С. Н. НИКИФОРОВ

# МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
## ЗАЩИЩЕННЫЕ СЕТИ

Учебное пособие

*Издание второе, стереотипное*

ЛАНЬ

САНКТ-ПЕТЕРБУРГ
МОСКВА · КРАСНОДАР
2021

УДК 004.056
ББК 32.973-018.2я723

**Н 62** **Никифоров С. Н.** Методы защиты информации. Защищенные сети : учебное пособие для СПО / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. : ил. — Текст : непосредственный.

**ISBN 978-5-8114-7907-8**

Учебное пособие предназначено для всех пользователей, стремящихся обеспечить защиту своей информации. Рассматриваются вопросы работы в безопасных сетях TOR, I2P и др.

Рекомендуется студентам, обучающимся по образовательной программе среднего профессионального образования по специальностям, входящим в укрупненные группы специальностей среднего профессионального образования «Информатика и вычислительная техника» и «Информационная безопасность».

УДК 004.056
ББК 32.973-018.2я723

**Рецензенты:**

*Б. Г. ВАГЕР* — доктор физико-математических наук, профессор Санкт-Петербургского государственного архитектурно-строительного университета;

*Е. Л. ГЕНИХОВИЧ* — доктор физико-математических наук, зав. лабораторией Главной геофизической обсерватории им. А. И. Воейкова.

**Обложка**
*П. И. ПОЛЯКОВА*

# ВВЕДЕНИЕ

Слово «информация» для современного человека встречается повсеместно. Причём, и прежде всего, это слово обозначает те сообщения, сведения, которые буквально обрушиваются на нас через телевидение, Интернет, прессу.

Что же такое информация?

Единого определения информации в настоящее время нет [11].

Существуют различные подходы к этому определению, связанные с решением конкретных научно-практических задач. Затруднения в едином и исчерпывающем определении информации естественны: понятие информации относится к числу первичных философских понятий, таких как материя, сознание, время, пространство и т. д.

Вот пример определения информации:

– *сообщение, осведомление о положении дел, сведения о чём-либо, передаваемые людьми*;

– *уменьшаемая неопределённость в результате получения сообщения.*

И несмотря на неопределённость даже определения самого объекта, в последние десятилетия XX века для значительной части трудящихся самых различных отраслей народного хозяйства основным предметом труда становится информация. Появляется понятие *национальные информационные ресурсы* [3]. О значимости этого понятия можно судить по популярной на Западе классификации стран по уровню их развития:

– на первом месте идут страны, способные производить и продавать информационные услуги;

– на втором — страны, не производящие информационных услуг (на продажу), но создающие и продающие товары — «вещи» (машины, холодильники, телевизоры, самолёты и т. д.);

– на третьем месте — страны, не производящие ни того, ни другого, и являющиеся поставщиками сырья и рабочей силы для стран более высоких категорий; они же являются покупателями соответствующей продукции ведущих стран [11].

Кстати, продажа информационных услуг в настоящее время обеспечивает в США более 50% доходов национального бюджета страны, а спецслужбы США на сбор и обработку информации расходуют более 2/3 своего бюджета.

В зависимости от целей понятие информации трактуется от философски обобщённого до бытового, т. е. можно сказать, что оно носит субъективный характер.

А что представляет собой понятие информации с научной точки зрения?

# 1. ФОРМУЛА ШЕННОНА

Пусть имеется $M$ равноправных и, следовательно, равновероятных возможностей. Например, при бросании игральной кости $M = 6$.

Тогда имеется априорная неопределённость, прямо связанная с $M$ (т. е. чем больше $M$, тем больше неопределённость). Измеренная её величина носит название *энтропии* и обозначается $H$ (*энтропия — мера неопределённости*):

$$H = f(M),$$

где $f()$ — некоторая возрастающая неотрицательная функция, определённая по меньшей мере для чисел натурального ряда.

При бросании кости и выяснении выпавшего числа приходит информация, количество которой обозначим $I$. После этого (т. е. апостериори) никакой неопределённости не остаётся: апостериорное $M = 1$, и этому значению должно соответствовать

$$H_{ps} = f(1) = 0.$$

Количество пришедшей информации естественно измерить величиной исчезнувшей неопределённости:

$$I = H_{pr} - H_{ps}.$$

Здесь индексы $pr$ — «априори», $ps$ — «апостериори».

Мы видим, что пришедшее количество информации совпадает с первоначальной энтропией.

Для определения вида функции $f()$ используем принцип аддитивности. В применении к игральной кости он гласит: энтропия двух бросаний кости в два раза больше, чем энтропия одного бросания, трех бросаний — в три раза больше и т. д. При двух бросаниях игральной кости число различных пар равно $36 = 6^2$. Вообще, в случае $n$ бросаний число равноправных возможностей равно $6^n$. Согласно принципу аддитивности находим

$$f(6^n) = nf(6),$$

при $m > 1$ эта формула имеет вид

$$f(m^n) = nf(m).$$

Обозначая $x = m^n$, имеем $\ln x = n \ln m$ и затем $n = \ln x / \ln m$ и

$$f(x) = \ln x / \ln m \cdot f(m),$$
$$f(x) = K \ln x,$$

где $K = f(m)/\ln x$ — положительная константа, не зависящая от $x$. Она связана с выбором единиц информации.

*Впервые логарифмическую меру информации ввёл Р. В. Л. Хартли, поэтому величину*

$$H = K \ln M$$

называют хартлиевским количеством информации.

Существуют несколько единиц измерения информации [9]:

1) если положить $K = 1$, то энтропия будет измеряться в натуральных единицах (naturaldigit) *натах*:

$$H_{нат} = \ln M;$$

2) если положить $K = 1/\ln 2$, то будем иметь энтропию, выраженную в двоичных единицах (binary digit) битах:

$$H_{бит} = 1/\ln 2 \cdot \ln M = \log_2 M;$$

3) если положить $K = 1/\ln 10$, то единицей измерения энтропии будет *хартли* (в честь Р. В. Л. Хартли):

$$H_{хартли} = 1/\ln 10 \cdot \ln M = \lg M;$$

4) если в качестве $K$ взять постоянную Больцмана $k = 1{,}38 \cdot 10^{-23}$ Дж/град, то будем иметь физическую шкалу измерения энтропии

$$H_{физ} = k \ln M.$$

Из сопоставления видно, что 1 нат крупнее 1 бита в $\log_2 e = 1/\ln 2 = 1{,}44$ раза.

Пусть, как и раньше, число возможностей равно $M$, можно рассматривать случайную величину $\xi$, принимающую одно из значений $M$, вероятности этих значений $P(\xi)$.

$$\text{Тогда } P(\xi) = 1/M, \text{ отсюда } M = 1/P(\xi).$$

Если в $H_{нат} = \ln M$ подставить $M$, то получим

$$H_{нат} = \ln 1/P(\xi) = \ln 1 - \ln P(\xi) = -\ln P(\xi).$$

Информация, полученная при выяснении реализации, численно равна первоначальной энтропии:

$$I(\xi) = -\ln P(\xi).$$

Из формулы видно, что информация и энтропия велики, когда априорная вероятность данной реализации мала, и наоборот.

Пусть известны вероятности того, сдал студент экзамен или нет:

$$P(\text{сдал}) = 7/8, \quad P(\text{не сдал}) = 1/8.$$

Количественно информация сообщения о том, что студент сдал экзамен, равна:

$$I(\text{сдал}) = -\ln P(\xi) = -\ln(7/8) = -\log_2 P(8/7) = 0{,}193 \text{ бита}.$$

Аналогично информация о том, что не сдал:

$$I(\text{не сдал}) = -\ln P(\xi) = -\ln(1/8) = -\log_2 P(8) = 3 \text{ бита}.$$

Таким образом, сообщение о том, что данный студент не сдал экзамен более информативно, так как это было маловероятно.

В своей работе по теории информации Клод Шеннон, используя энтропию как меру информации, формализует понятие количества информации. Приобретение информации сопровождается уменьшением неопределенности, поэтому количество информации можно измерить количеством исчезнувшей неопределенности.

Следовательно, теория информации имеет дело не со смыслом информации, а лишь с её количеством.

Поскольку речь идёт о таком носителе информации, как персональный компьютер, то все сведения, которые находятся, в том или ином виде в нём или на устройствах памяти будем считать информацией.

Таким образом, можем сформулировать «своё» определение информации: *все данные, находящиеся в компьютере*.

Стремление дать «своё» формализованное определение объясняется необходимостью указать предметную область, в которой будем работать. Так как вся информация в компьютере хранится в виде файлов системных, прикладных, пользовательских и других, то объектом нашей деятельности будет файл, совокупность файлов.

Дадим формализованное определение файлу: *именованная совокупность данных.*

Теперь о том, что значит защитить, и от чего защитить нашу информацию, т. е. какие-то файлы.

Защита — *предотвращение несанкционированного использования или искажения информации (файлов).*

# 2. ЗАЧЕМ ЗАЩИЩАТЬ?

Вопрос — зачем защищать? — неразрывно связан с другим вопросом — от кого защищать?

Надо сказать, что кодирование информации в связи с передачей её с помощью техники связи рассматривалось, прежде всего, как экономное, удобное и практически безошибочное средство.

Кодирование информации для средств связи появилось вместе с развитием этих средств в XIX веке [10].

Исторически первый код, предназначенный для передачи сообщений, связан с именем изобретателя телеграфного аппарата Сэмюэля Морзе и известен всем как азбука Морзе. В то время как шифровальное дело известно значительно дольше.

Геродот (V век до н. э.) приводит примеры писем, понятных лишь одному адресату. Спартанцы имели специальный механический прибор, при помощи которого важные сообщения можно было писать особым способом, обеспечивающим сохранение тайны. Собственная секретная азбука была у Юлия Цезаря.

В Средние века и эпоху Возрождения над изобретением тайных шифров трудились многое выдающиеся люди, в их числе философ Фрэнсис Бэкон, крупные математики Франсуа Виет, Джероламо Кардано, Джон Валлис.

Поэтому если кодирование — это технически необходимое действие для современной передачи информации, то шифрование имеет под собой совсем другие причины [1].

Возможно, это связано с социальными, даже физиологическими особенностями человеческого общества.

Владеть всей полнотой информации могут далеко не все слои общества, не все индивидуумы, так как для этого требуется не только определённый уровень подготовки, профессиональных знаний, но, что может быть важнее, психологические особенности личности, характера.

Нельзя забывать такой аспект, как частная, личная жизнь собственника некоторой информации, вторжение в которую преследуется по закону во многих государствах.

Исходя из изложенного, можно утверждать, что защита информации необходима.

## 2.1. Защита информации

Защита информации — важнейшая составная часть правил безопасной работы на компьютере. Что может угрожать данным на вашем компьютере?

1. Несанкционированный доступ. Для ваших недругов, заинтересованных в доступе к конфиденциальным данным, самый простой способ добраться до ваших секретов — тем или иным способом получить доступ к жесткому диску вашего компьютера. Защита информации от несанкционированного доступа должна включать такие меры, как:

– ограничение доступа посторонних к вашему компьютеру. Комната, где установлены компьютеры, должна закрываться на замок, неплохо бы оборудовать ее сигнализацией, решетками на окнах и другими средствами защиты. Но самое главное — не допускать обыкновенного разгильдяйства: не оставлять дверь открытой, когда «выходишь на минуточку», не разрешать посторонним бесконтрольно работать на вашем компьютере;

– установка паролей для входа на ваш компьютер и для доступа к отдельным разделам и папкам на диске;

– продуманная система разграничения доступа к информации на вашем компьютере и в вашей локальной сети;

– криптозащита (шифрование) наиболее важных данных.

2. Вирусы, троянские и другие зловредные программы, проникающие на компьютер без вашего ведома. Такие программы могут... Трудно придумать, чего же они сейчас не могут! Они могут удалить нужные файлы и запустить форматирование винчестера, передать своим хозяевам все ваши пароли и без вашего ведома превратить ваш компьютер в машину для рассылки спама... Защитите свой компьютер от вирусов!

3. Потеря информации при сбоях компьютера и собственных ошибочных действиях (случайное удаление нужных данных и т. п.). Чтобы избежать подобных неприятностей, регулярно сохраняйте вводимую информацию; каждый день в конце рабочего дня, а лучше два раза в день дублируйте все данные, в которых изменили хотя бы одну букву.

Выполнение вышеописанных мер по защите информации на вашем компьютере позволит обезопасить себя от потери данных, несанкционированного использования конфиденциальных сведений, избежать серьезных стрессов и связанных с ними проблем со здоровьем.

## 2.2. Исторические аспекты возникновения и развития информационной безопасности

Объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путём воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума.

Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов:

– I этап — до 1816 года — характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

– II этап — начиная с 1816 года — связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

– III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

– IV этап — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались в основном методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

– V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались в основном методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

– VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей-хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

– VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить, что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

# 3. ЦЕННОСТЬ ИНФОРМАЦИИ

Практически все виды деятельности предполагают:

– сбор;

– сортировку;

– хранение;

– передачу информации с целью управления чем-либо.

Так как теория информации имеет дело не со смыслом информации, а лишь с её количеством, то применять для определения ценности информации формулу Шеннона вряд ли целесообразно.

Для того чтобы убедиться, в чём это противоречит здравому смыслу, зададим следующий вопрос: «Какая книга содержит больше всего информации?» Вопрос, конечно, нужно стандартизировать, указав размер книги, страницы и тип шрифта, а также множество используемых знаков (алфавит).

После этого ответ, очевидно, будет таким: «*Больше всего информации содержит книга, текст которой является полностью случайным!*». Каждый новый символ должен быть абсолютно неожиданным [9].

Информация, необходимая для одних пользователей, для других — совершенно бесполезна, больше того, бесполезная сейчас информация (сведения) через какое-то время становится жизненно необходимой, поэтому понятие ценности информации носит *субъективный* характер.

Можно вспомнить известный афоризм Ницше: «Ценность — это точка зрения».

И всё же без информации нельзя!

Есть же понятие — национальные информационные ресурсы.

И, наверное, справедливо утверждение — *кто владеет информацией, тот владеет миром*!

# 4. ОСНОВНЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

Основными задачами защиты пользовательской информации являются [8]:

– обеспечение конфиденциальности информации;

– обеспечение целостности информации;

– обеспечение достоверности информации;

– обеспечение оперативного доступа к информации;

– обеспечение юридической значимости информации, представленной в виде электронного документа;

– обеспечение неотслеживаемости действий клиента.

*Конфиденциальность* — свойство информации быть доступной только ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.

*Целостность* — свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.

*Достоверность* — свойство информации, выражающееся в строгой принадлежности объекту, который является её источником, либо тому объекту, от которого эта информация получена.

*Оперативность* — способность информации или некоторого информационного ресурса быть доступным для конечного пользователя в соответствии с его временными потребностями.

*Юридическая значимость* — свойство информации, выражающееся в наличии атрибутов, означающих её способность быть юридически значимой.

*Неотслеживаемость* — способность совершать некоторые действия в информационной системе незаметно для других объектов [8].

# 5. РАБОТА В АНОНИМНЫХ СЕТЯХ

Стремление некоторых структур, коммерческих и не только, знать всё о каждом не всегда, мягко говоря, встречается с энтузиазмом. Более того, имея право на тайну переписки и личной жизни, по крайней мере юридически, хотелось бы хоть в какой-то степени его реализовать в смысле анонимности и безопасности (во всех значениях этого слова) при работе в Интернете.

Возможности скрыть свой **IP**-адрес[1], посетить сайт, заблокированный администратором сети, зашифровать, передаваемые по Сети сообщения, рассмотрены далее на примере двух систем: **TOR** и **I2P**.

## 5.1. Установка и использование TOR

**TOR** (аббревиатура ***T**he **O**nion **R**outer*) — свободное программное обеспечение для реализации второго поколения так называемой «луковой маршрутизации». Это система, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания (см. Википедия).

**TOR** следует скачивать только с официального сайта по адресу: **https://www.torproject.org/**, рис. 5.1.1.

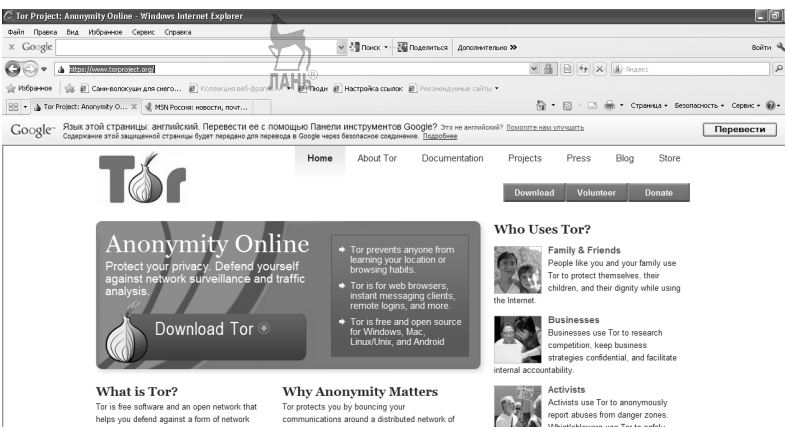


**Рис. 5.1.1**

Если стартовой страницей был, например, **Google**, то, нажав кнопку **Перевести**, можно русифицировать картинку, рис. 5.1.2.

[1] **IP-адрес** (*Internet Protocol Address*) — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети Интернет требуется глобальная уникальность адреса.

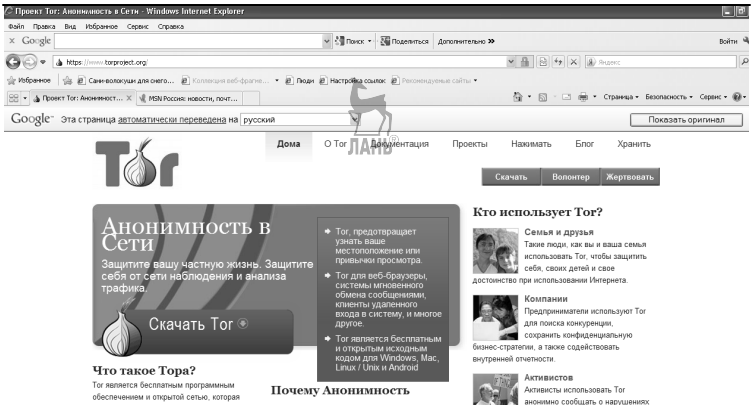


**Рис. 5.1.2**

Скачать пакет, нажав **Скачать Tor** или **Download Tor** и установив язык **Русский**, рис. 5.1.3.

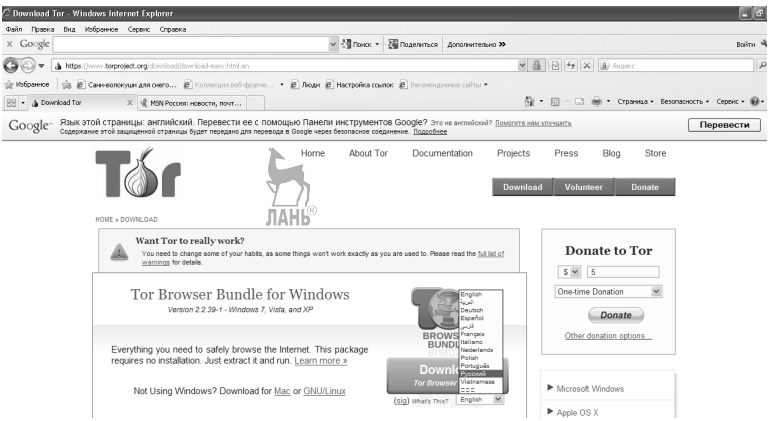


**Рис. 5.1.3**

Нажать кнопку **Download Tor Browser[2] Bundle** и в появившемся окне **Загрузка файла — предупреждение системы безопасности** нажать кнопку **Сохранить**, рис. 5.1.4.

[2] **Браузер** (*browser*) — программное обеспечение для просмотра веб-сайтов, т. е. для запроса веб-страниц (преимущественно из Сети), их обработки, вывода и перехода от одной страницы к другой.

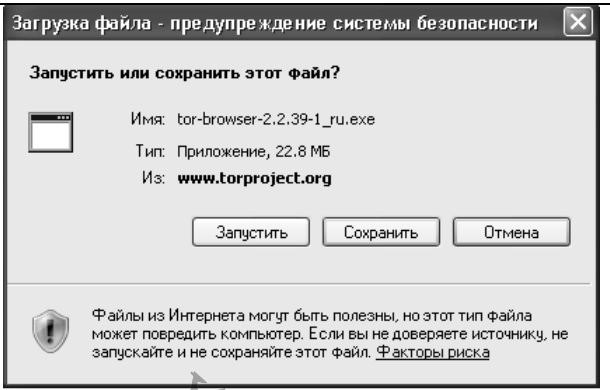


**Рис. 5.1.4**

Скачать пакет **Tor** целесообразно в специально подготовленную папку на флешке, тогда можно будет выходить в Интернет, если он есть, с любого компьютера, рис. 5.1.5.

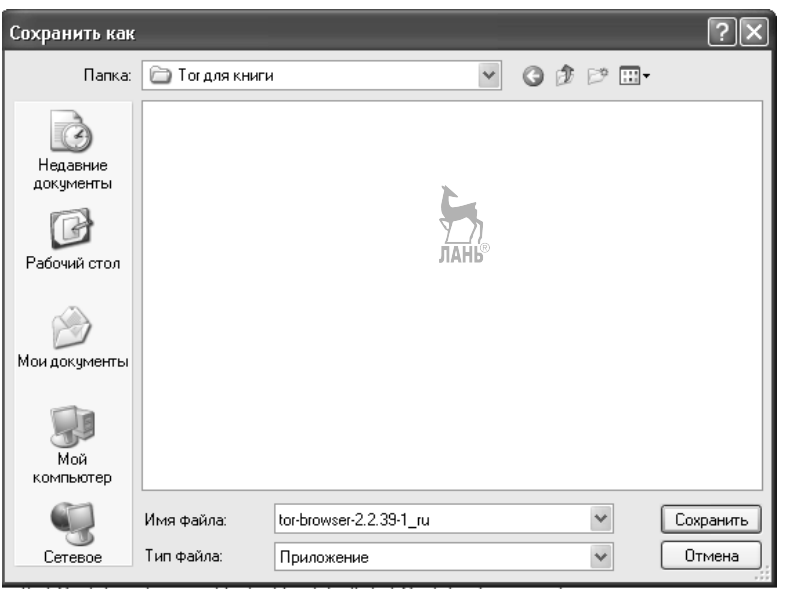


**Рис. 5.1.5**

Подождав некоторое время, в появившемся окне **Загрузка завершена** нажать кнопку **Открыть папку**, рис. 5.1.6.

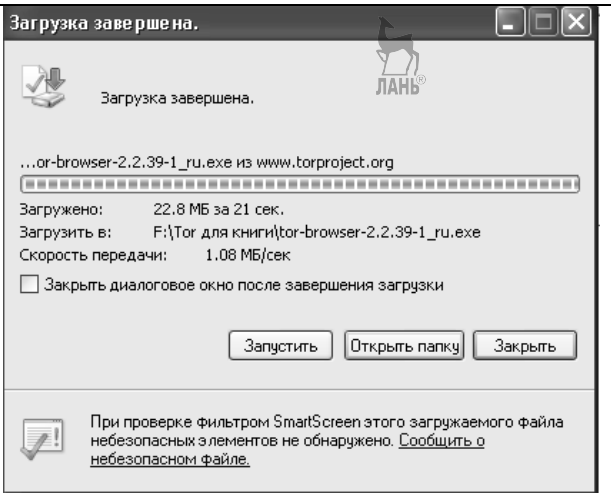


**Рис. 5.1.6**

В появившемся окне, в данном случае в специально созданной на флешке папке **Tor для книги**, отобразится архив **tor-browser-2.2.39-1_ru,** рис. 5.1.7.

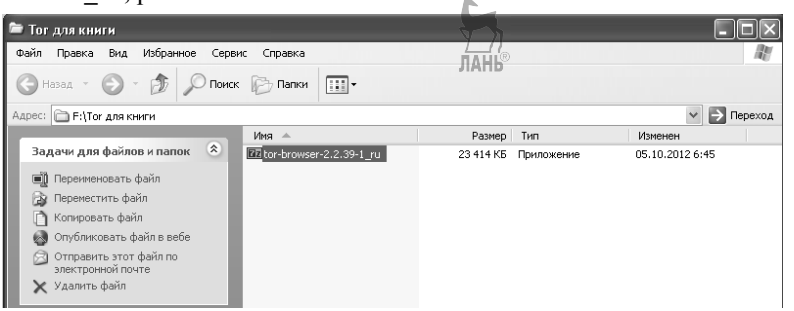


**Рис. 5.1.7**

Щёлкнув по архиву, приступим к распаковке, нажав кнопку **Extract**, рис. 5.1.8.

Через некоторое время увидим новую папку **TorBrowser**, рис. 5.1.9.

Раскрыв папку **Tor Browser**, выберем файл **Start Tor Browser** и запустим его, рис. 5.1.10.

Откроется окно **Панель управления Vidalia**, в котором будет сообщено о подключении к сети **Tor**, рис. 5.1.11.

В появившемся через некоторое время окне **Are you using Tor? — Mozilla Firefox**[3] отобразится ваш новый **IP**-адрес, в данном случае это **31.172.30.4**, рис. 5.1.12.

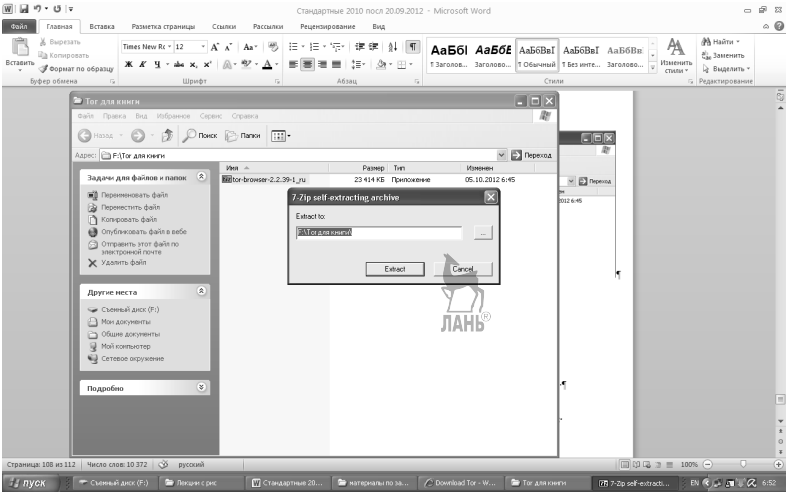


**Рис. 5.1.8**

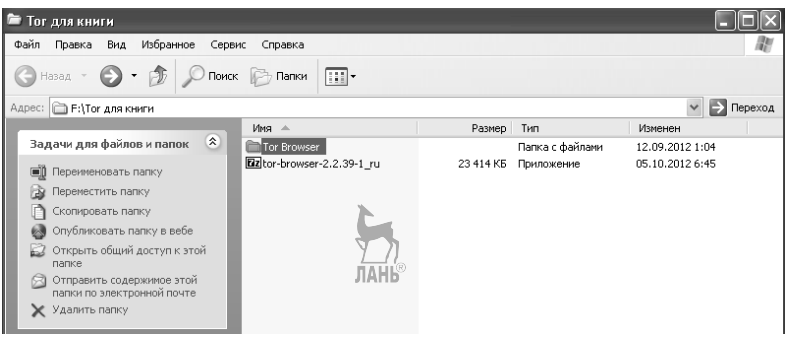


**Рис. 5.1.9**

[3] **Mozilla Firefox** [moʊˈzɪlə ˈfaɪ(ɹ)fɑks]) — свободно распространяемый браузер, входящий в набор программ Mozilla Application Suite, разработкой и распространением которого занимается Mozilla Corporation. Третий по популярности браузер в мире и второй среди свободного ПО.

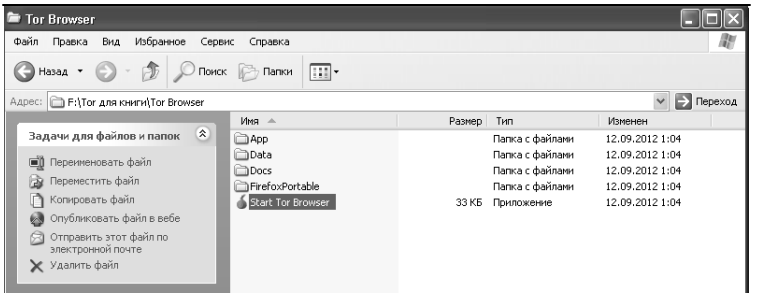


**Рис. 5.1.10**


**Рис. 5.1.11**

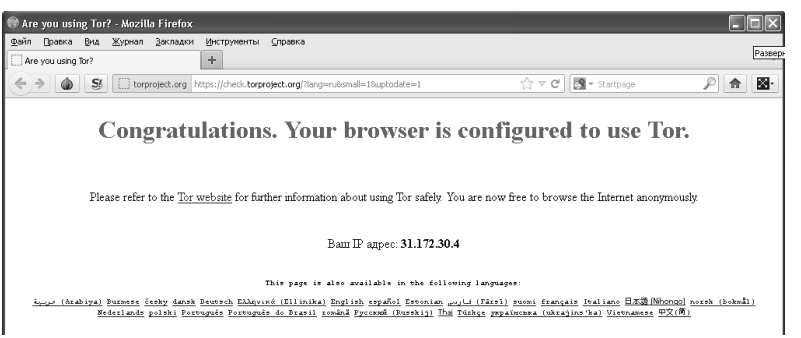


**Рис. 5.1.12**

Всё, соединение с сетью **Tor** установлено, и теперь вы анонимны.

Если щёлкнуть по пиктограмме **SP** (**Startpage,** Поиск с использованием **Startpage)**, то появится меню поисковых систем, рис. 5.1.13.

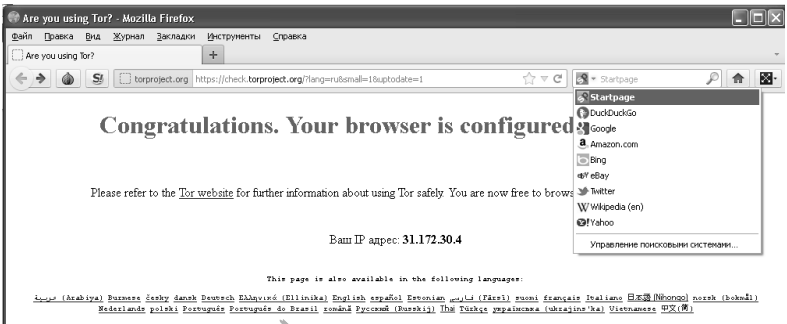


**Рис. 5.1.13**

Если в окне **Startpage** щёлкнуть два раза левой клавишей мышки по пиктограмме Поиск, то выполнится переход к окну **Startpage Search Engine — Mozilla Firefox**, где можно указать адрес конкретного узла, с которым необходимо установить соединение, рис. 5.1.14.

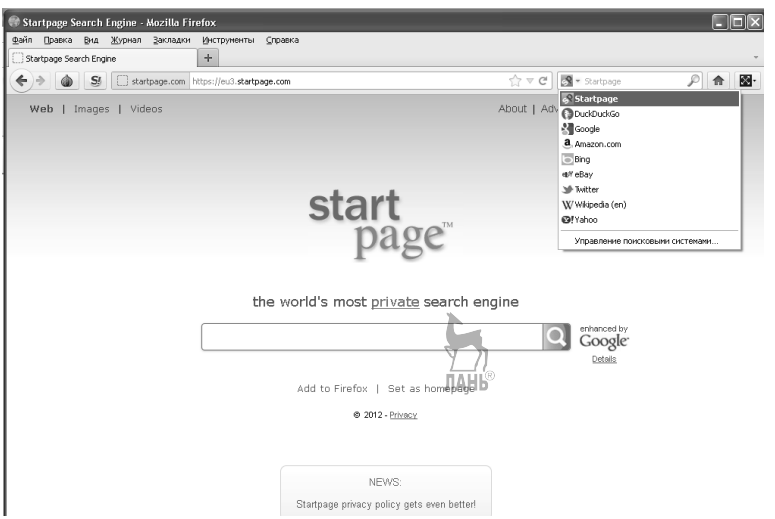


**Рис. 5.1.14**

## 5.2. Настройка почтового клиента Mozilla Thunderbird для работы в сети TOR

Запустить **Tor** и с помощью **Vidalia** убедиться, что подключены к сети **Tor**, рис. 5.1.14.

Запустить **Mozilla Thunderbird**:

– в появившемся окне <<**Thunderbird>> — <<Почта>>** выбрать **Создать новое сообщение** и щёлкнуть левой клавишей мышки, рис. 5.2.1;

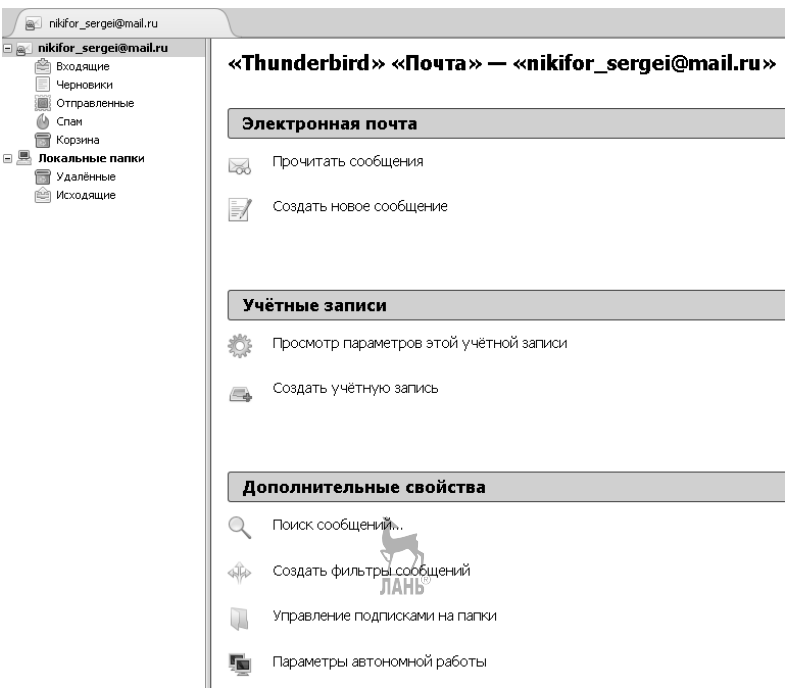


**Рис. 5.2.1**

– в появившемся окне **Создание сообщения (без темы)** выбрать **Инструменты**, затем в появившемся подменю выбрать **Настройки** и щёлкнуть левой клавишей мышки, рис. 5.2.2;

– в появившемся окне **Настройки** выбрать **Дополнительные**, затем на вкладке **Сеть и дисковое пространство**, рис. 5.2.3;

– в появившемся изменённом окне **Настройки** нажать кнопку **Настроить**, рис. 5.2.4;

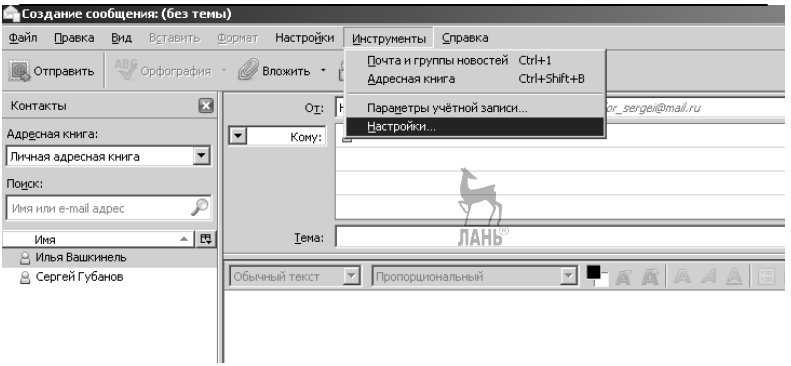


**Рис. 5.2.2**

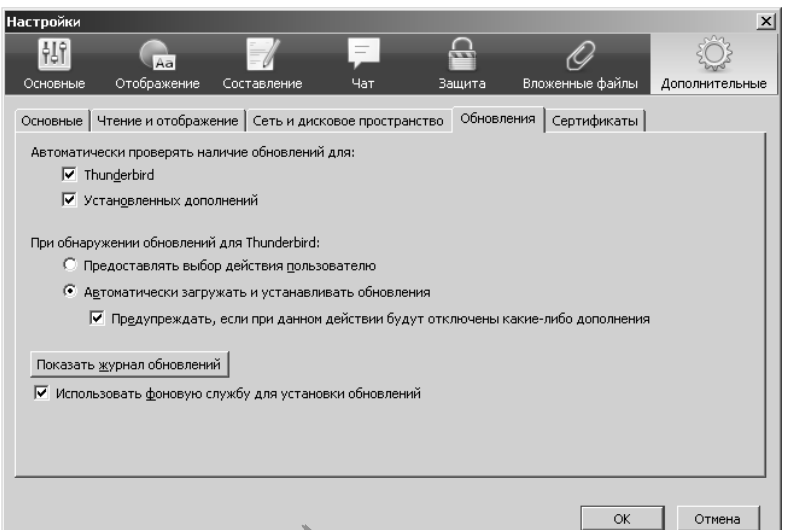


**Рис. 5.2.3**

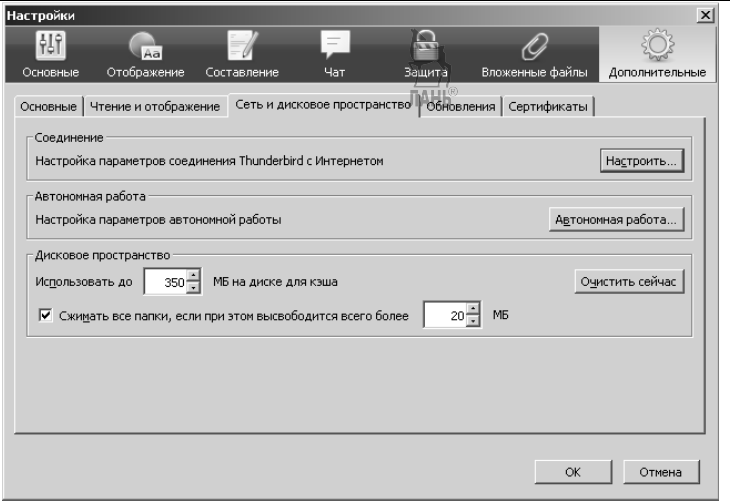


**Рис. 5.2.4**

– в появившемся окне **Параметры соединения** установить параметры, как показано на рис. 5.2.4 и нажать кнопку **ОК**;

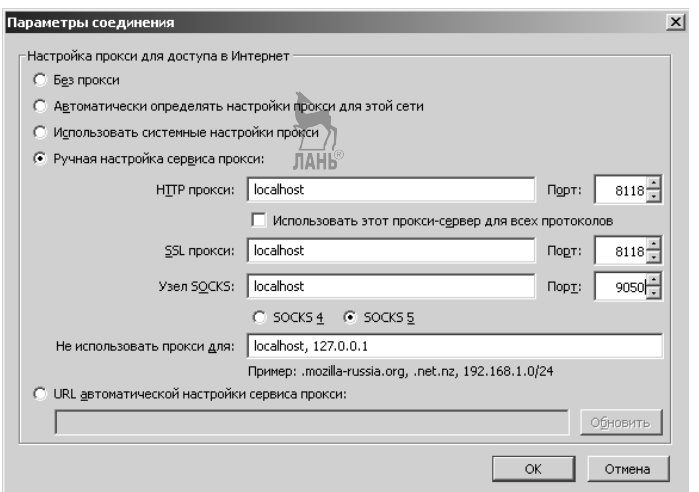


**Рис. 5.2.5**

– в появившемся окне **Настройки** нажать кнопку **ОК**, рис. 5.2.6;

– в появившемся окне **Создание сообщения** нажать пиктограмму **Отправить**, рис. 5.2.7;

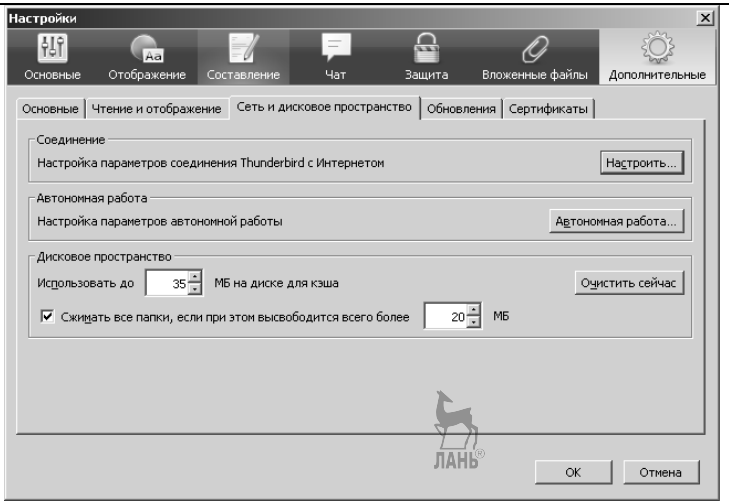


**Рис. 5.2.6**

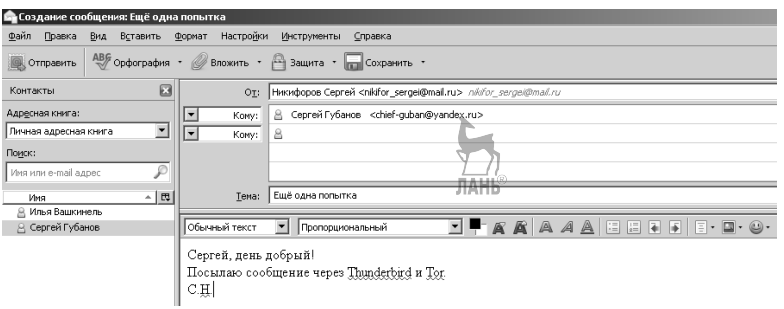


**Рис. 5.2.7**

– в появившемся окне **Отправка сообщения** увидеть процесс отправки, рис. 5.2.8;

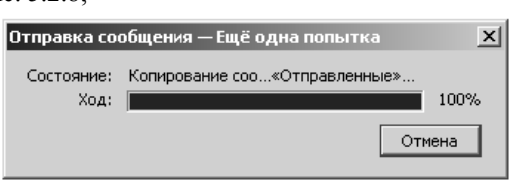


**Рис. 5.2.8**

– в разделе **Отправленные** можно убедиться, что сообщение отправлено адресату, рис. 5.2.9.

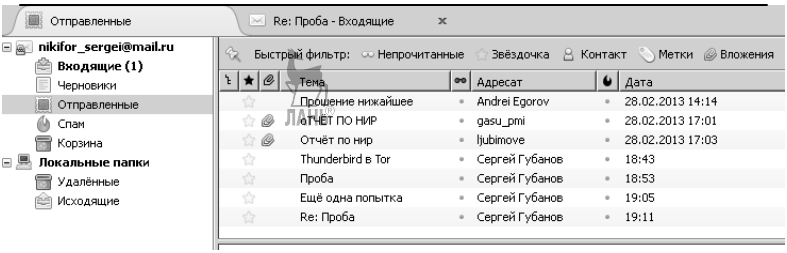


**Рис. 5.2.9**

## 5.3. Определение IP-адреса в mail.ru

Для того чтобы определить **IP-адрес**, необходимо, находясь в **Почте Mail.ru**:

– открыть соответствующее сообщение, например **Аня Головина**, рис. 5.3.1;

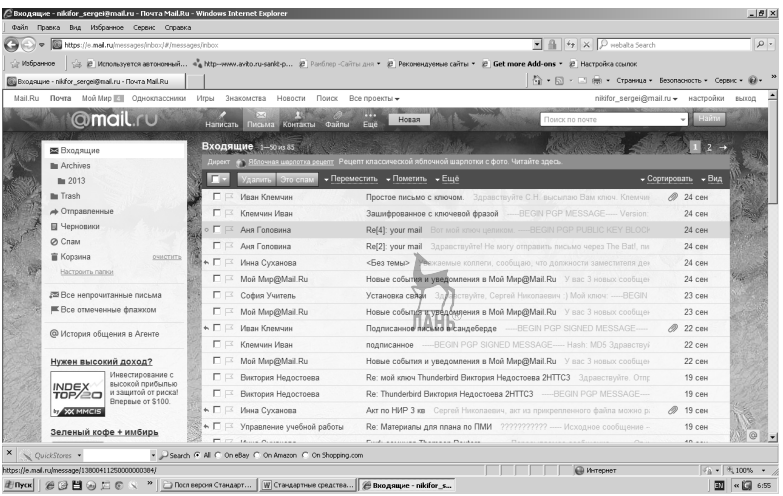


**Рис. 5.3.1**

– в появившемся окне выбранного сообщения в горизонтальном меню выбрать раздел **Ещё**, рис. 5.3.2, и щёлкнуть левой клавишей мышки;

– в появившемся подменю выбрать раздел **Служебные заголовки**, рис. 5.3.3, и щёлкнуть левой клавишей мышки;

– в появившемся окне с информацией выделить **Received: from [37.145.55.66]**, рис. 5.3.4.

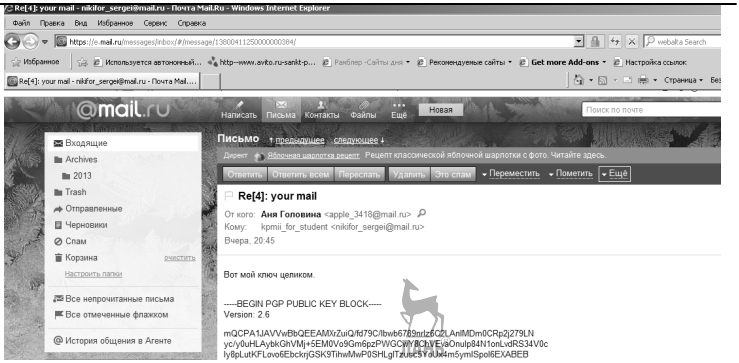


**Рис. 5.3.2**

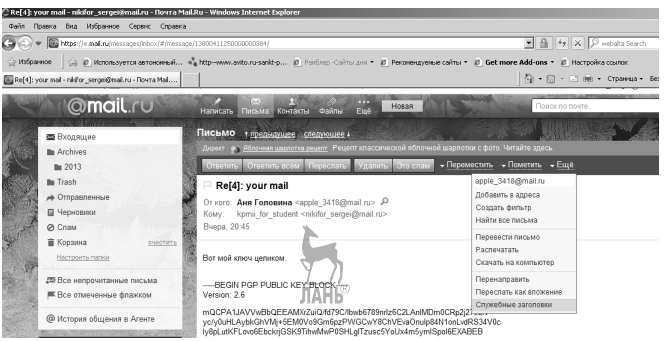


**Рис. 5.3.3**

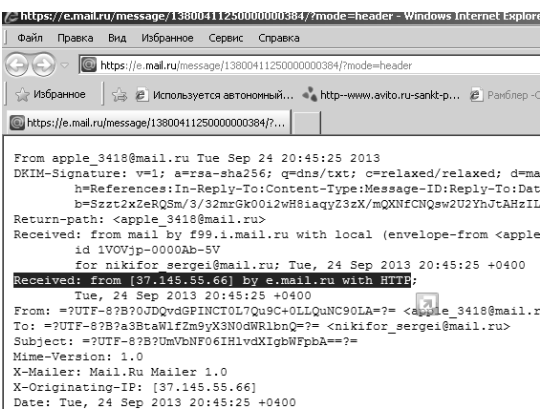


**Рис. 5.3.4**

Таким образом, **IP**-адрес автора данного сообщения **37.145.55.66**.

## 5.4. Определение IP-адреса в THE BAT!

Для того чтобы определить **IP-адрес**, необходимо, находясь в программе почтовый клиент **THE BAT!**:

– открыть соответствующее сообщение, например **Аня Головина**, рис. 5.4.1;

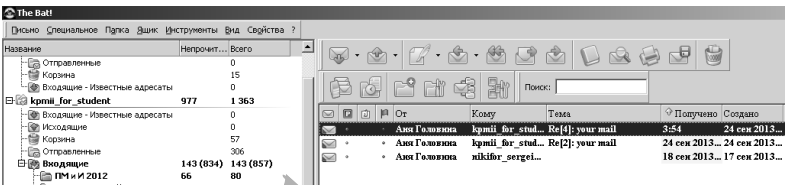


**Рис. 5.4.1**

– в появившемся окне выбранного сообщения в горизонтальном меню выбрать раздел **Вид**, рис. 5.4.2, и щёлкнуть левой клавишей мышки;

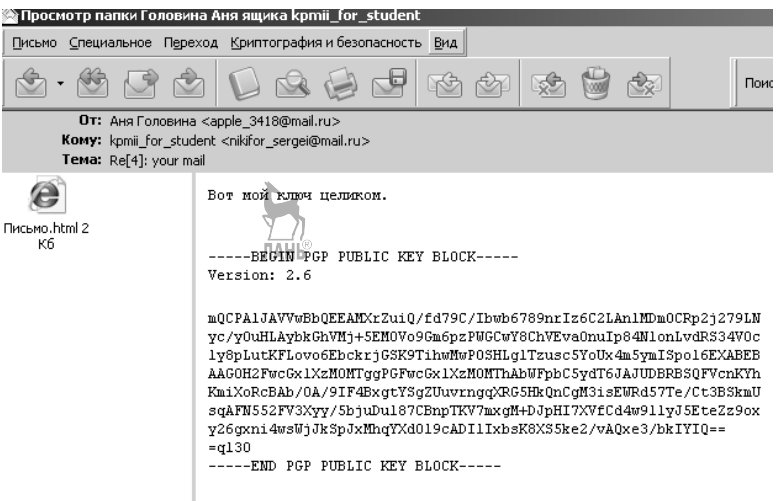


**Рис. 5.4.2**

– в появившемся подменю выбрать раздел **Показывать заголовки (RFC-822)**, рис. 5.4.3, и щёлкнуть левой клавишей мышки;

– в появившемся окне с информацией выделить **X-Originating-IP [37.145.55.66]**, рис. 5.4.4.

Таким образом, **IP**-адрес автора данного сообщения **37.145.55.66**.

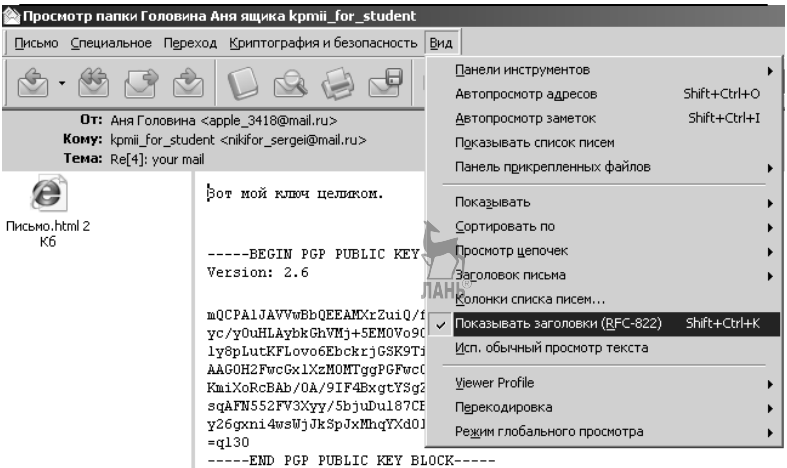


**Рис. 5.4.3**

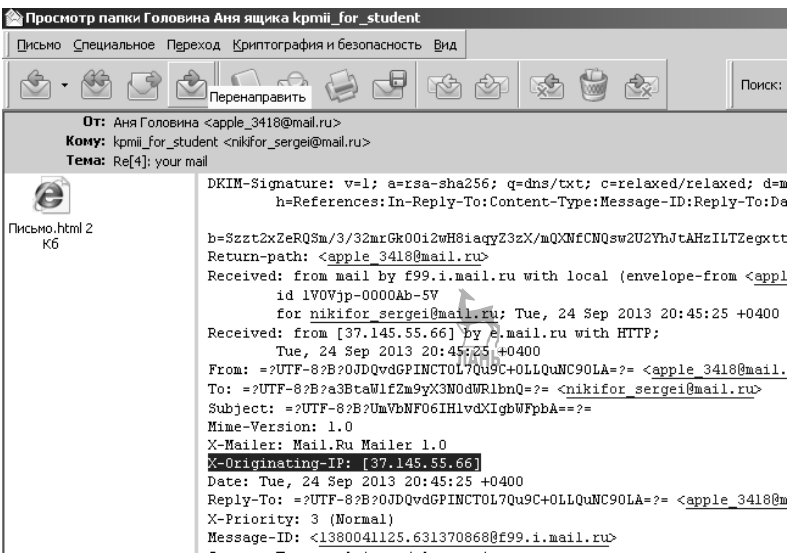


**Рис. 5.4.4**

## 5.5. Определение IP-адреса в Thunderbird

Для того чтобы определить **IP-адрес**, необходимо, находясь в программе почтовый клиент **Thunderbird**:

– выбрать соответствующее сообщение, например **Аня Головина**, рис. 5.5.1;

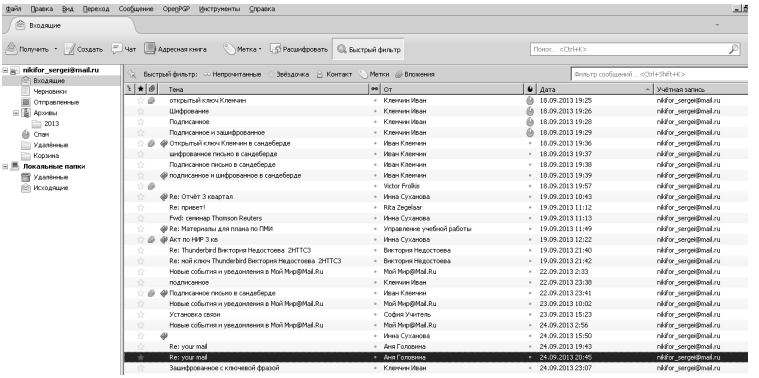

**Рис. 5.5.1**

– в горизонтальном меню выбрать раздел **Вид**, в появившемся подменю выбрать раздел **Заголовки**, а в нём выбрать **Все**, рис. 5.5.2, и щёлкнуть левой клавишей мышки;

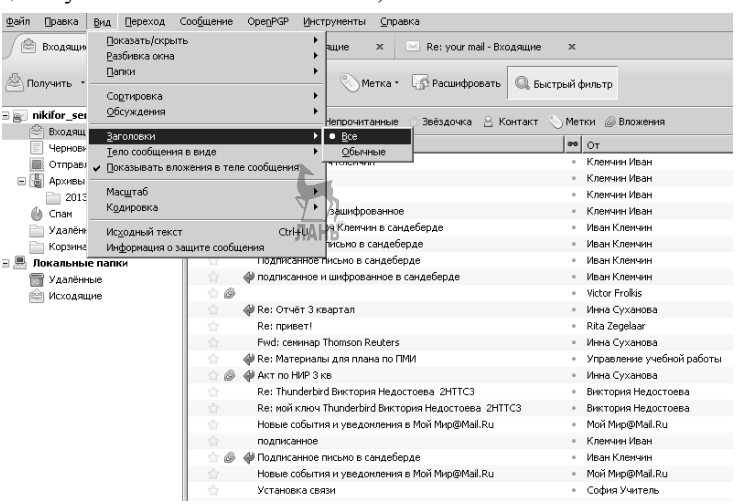


**Рис. 5.5.2**

– после этого щёлкнуть два раза левой клавишей мышки по выбранному сообщению, в данном случая **Аня Головина**, и в появившемся окне выбранного сообщения выделить **X-Originating-IP [37.145.55.66]**, рис. 5.5.3.

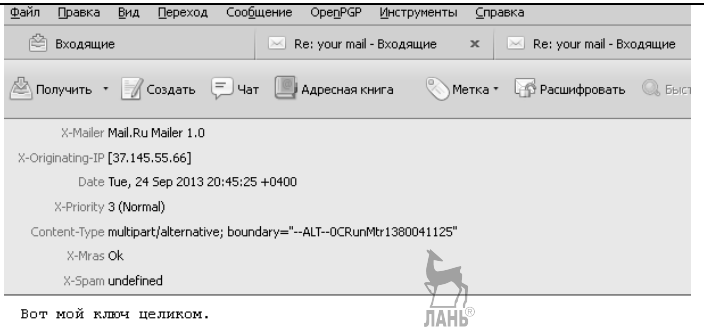


**Рис. 5.5.3**

Таким образом, **IP**-адрес автора данного сообщения **37.145.55.66**.

## 5.6. Программа для анонимной отправки e-mail Anmase

Программа **Anmase** — простейшая утилита для отправки анонимных сообщений по электронной почте с возможностью подмены имени и адреса отправителя. Программа не рассчитана на пакетную отправку писем и не может использоваться спамерами, создана скорее для развлечения.

Для того чтобы скачать программу **Anmase**, необходимо обратиться по адресу: **http://anmase.ru/Soft**:

– в появившемся окне выбрать **Скачать Anmase 5.0 (1,4 МБ)**, рис. 5.6.1;

– в появившемся окне **Загрузка файла — предупреждение системы безопасности** выбрать кнопку **Сохранить** и щёлкнуть левой клавишей мышки, рис. 5.6.2;

– в появившемся окне **Сохранить как** выбрать место установки программы, например в папке **2013**, имя файла **Anmase** и щёлкнуть левой клавишей мышки по кнопке **Сохранить**, рис. 5.6.3;

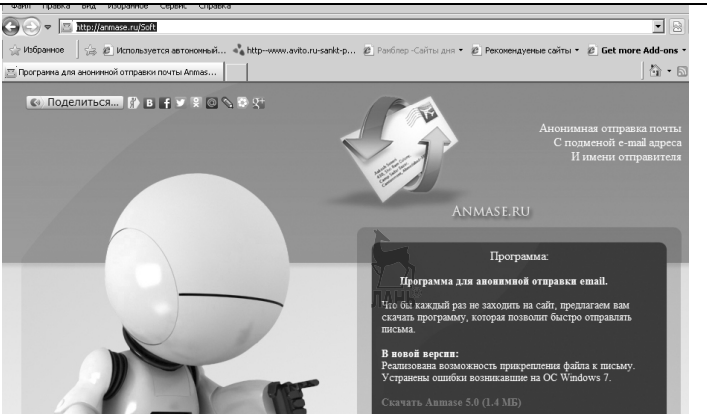


**Рис. 5.6.1**

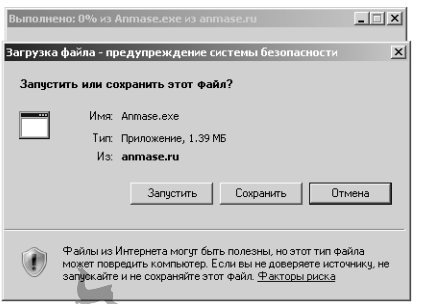


**Рис. 5.6.2**

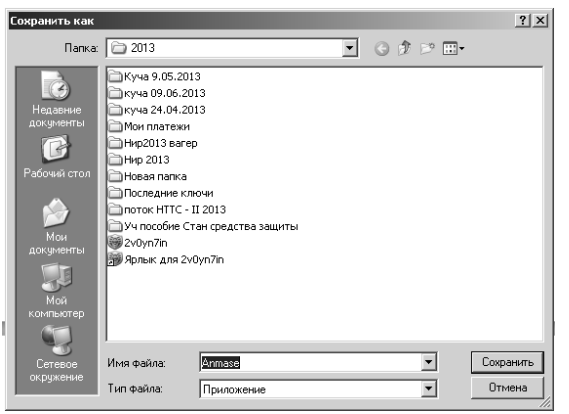


**Рис. 5.6.3**

– в появившемся окне **Загрузка завершена** выбрать кнопку **Открыть папку** и щёлкнуть левой клавишей мышки по кнопке **Сохранить**, рис. 5.6.4;

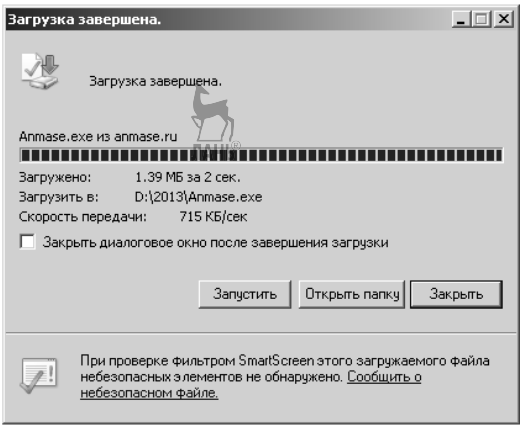


**Рис. 5.6.4**

– в появившейся папке **2013** выбрать кнопку убедиться в наличии программы **Anmase**, рис. 5.6.5.

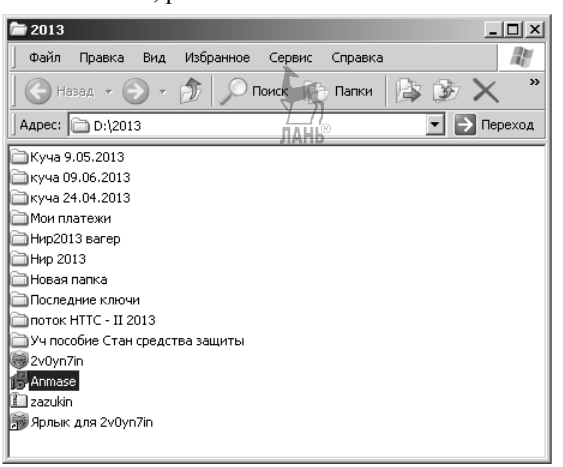


**Рис. 5.6.5**

### 5.6.1. Установка программы Anmase

Для установки программы **Anmase** необходимо выполнить следующие действия:

– выбрать, в данном случае в папке **2013**, **Anmase** и щёлкнуть два раза левой клавишей мышки, рис. 5.6.5;

– в появившемся окне **Установка Anmase** выбрать **Russian (Русский)** и нажать кнопку **ОК**, рис. 5.6.1.1;

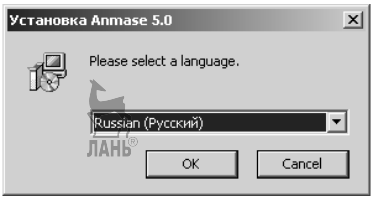


**Рис. 5.6.1.1**

– в появившемся окне **Установка Anmase 5.0** нажать кнопку **Далее**, рис. 5.6.1.2;

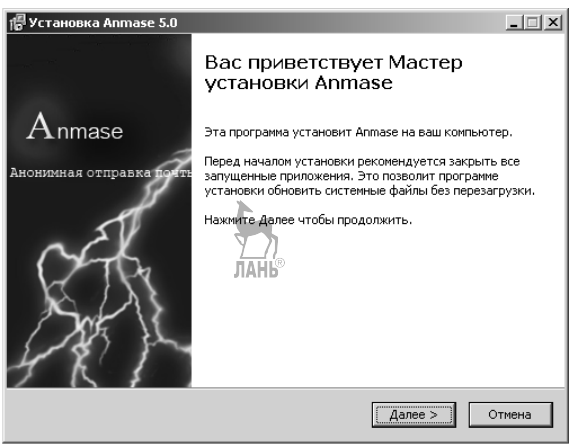


**Рис. 5.6.1.2**

– в появившемся изменённом окне **Установка Anmase 5.0** нажать кнопку **Далее**, рис. 5.6.1.3;

– в появившемся изменённом окне **Установка Anmase 5.0** нажать кнопку **Далее**, рис. 5.6.1.4;

– в появившемся изменённом окне **Установка Anmase 5.0** нажать кнопку **Установить**, рис. 5.6.1.5;

– в появившемся изменённом окне **Установка Anmase 5.0** нажать кнопку **Готово**, рис. 5.6.1.6;

– убедиться в появлении на **Рабочем столе** ярлыка программы **Anmase 5.0**, рис. 5.6.1.7.

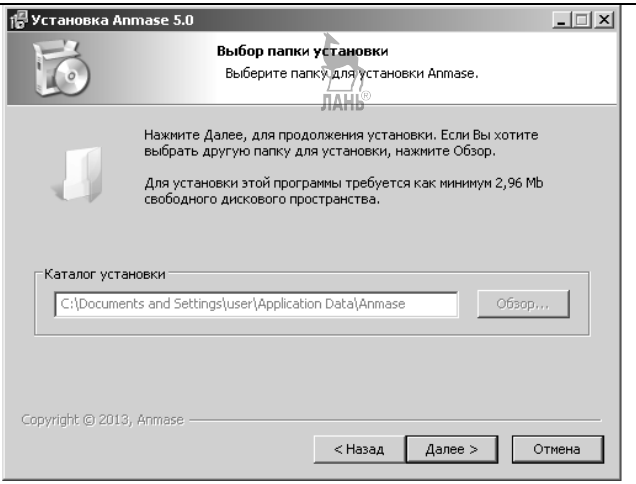


**Рис. 5.6.1.3**

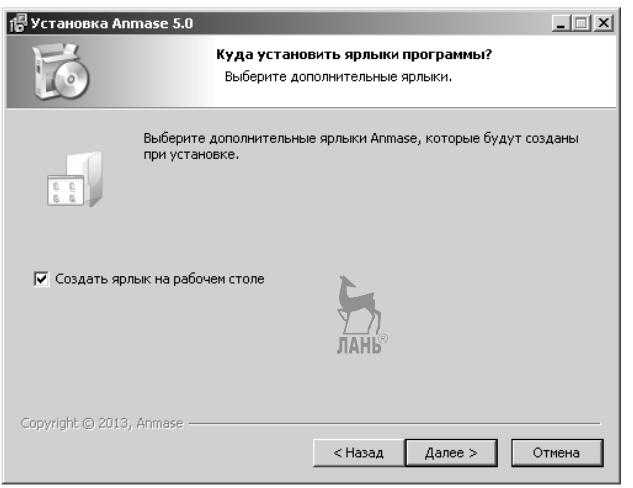


**Рис. 5.6.1.4**

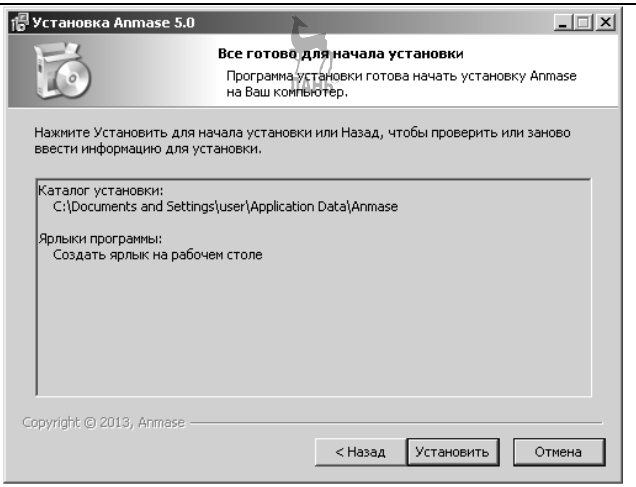


**Рис. 5.6.1.5**

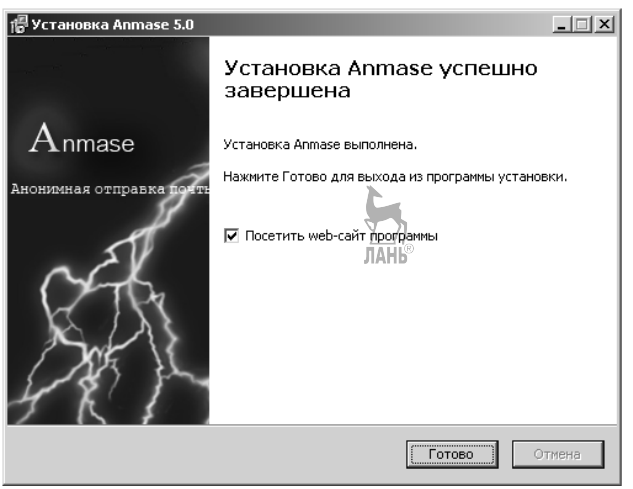


**Рис. 5.6.1.6**


**Рис. 5.6.1.7**

### 5.6.2. Использование программы Anmase

Для запуска программы **Anmase** необходимо щёлкнуть по значку, рис. 5.6.1.7:

– в результате появится окно **Anmase.ru — анонимная отпра…**, рис. 5.6.2.1;

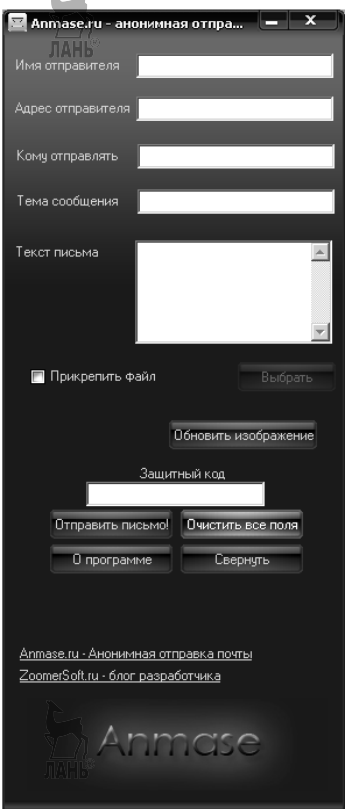


**Рис. 5.6.2.1**

– выбрать ссылку **Anmase.ru — Анонимная отправка почты** и щёлкнуть левой клавишей мышки, рис. 5.6.2.1;

– появится окно **Отправить e-mail письмо с чужого адреса**, рис. 5.6.2.2;

– заполнить **Форму отправки письма**, указав произвольное **Имя отправителя** и **Адрес отправителя**, а также введя предлагаемый код, рис. 5.6.2.3;

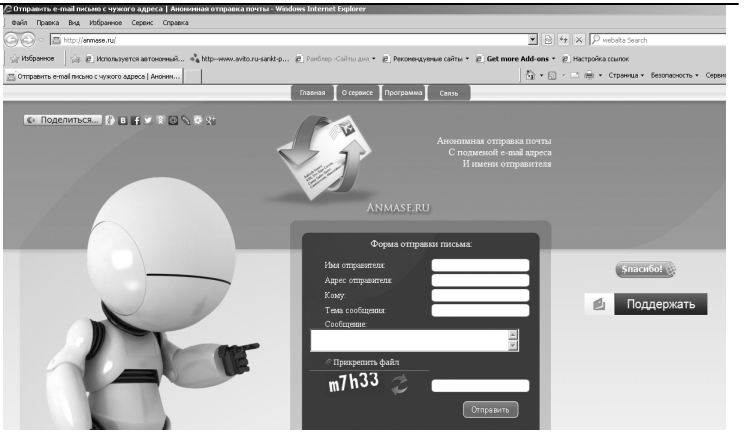


**Рис. 5.6.2.2**

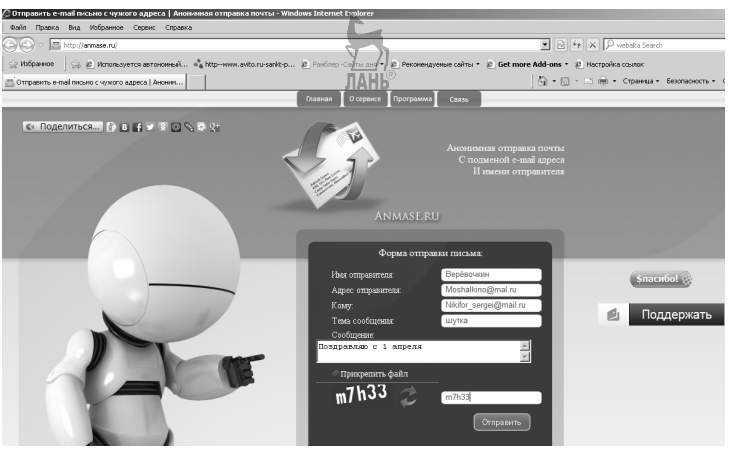


**Рис. 5.6.2.3**

– в данном случае отправил сообщение самому себе от анонимного адресата **Верёвочкин** с анонимным адресом **Moshalkino@mail.ru.**

## 5.7. Настройка программы Skype на использование сети TOR

Для настройки программы интернет-телефонии **Skype** на использование сети **TOR** необходимо включить программу **Skype**, щёлкнув два раза левой клавишей мышки по пиктограмме, рис. 5.7.1:


**Рис. 5.7.1**

– в появившемся окне **Skype** выбрать команду **Инструменты**, рис. 5.7.2;

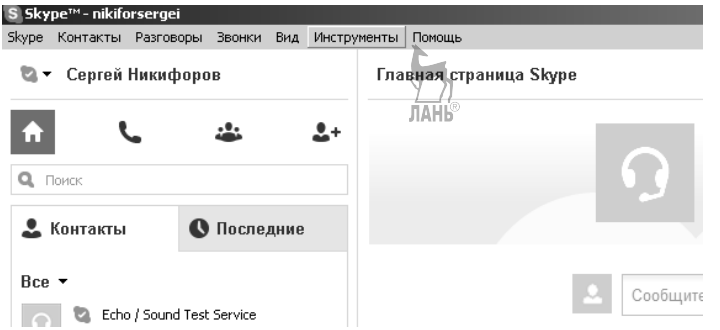


**Рис. 5.7.2**

– в появившемся меню выбрать команду **Настройки**, рис. 5.7.3;

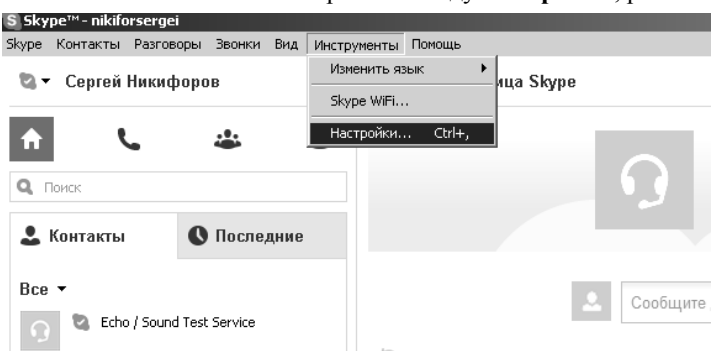


**Рис. 5.7.3**

– в появившемся окне **Skype — Настройки** перейти в раздел **Дополнительно**, рис. 5.7.4;

– в появившемся изменённом окне **Skype — Настройки** перейти в раздел **Соединение**, рис. 5.7.5;

– в появившемся изменённом окне **Skype — Настройки** установить параметры так, как показано на рис. 5.7.6.

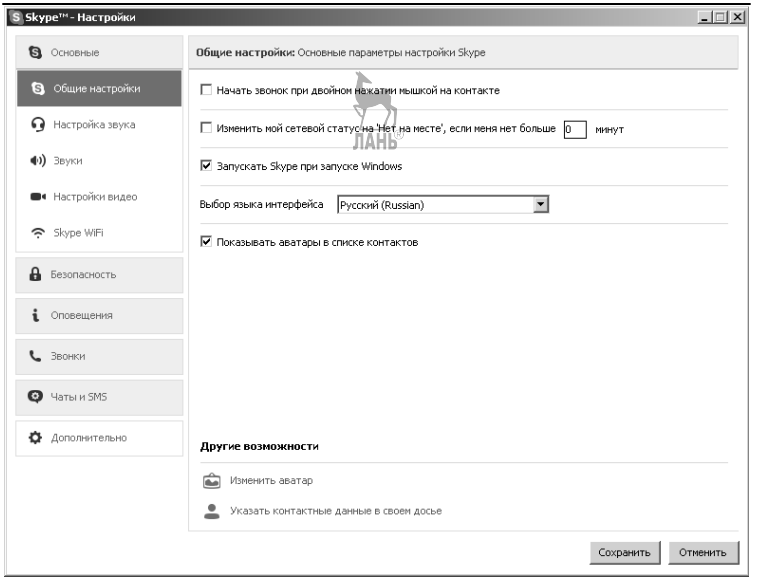


**Рис. 5.7.4**

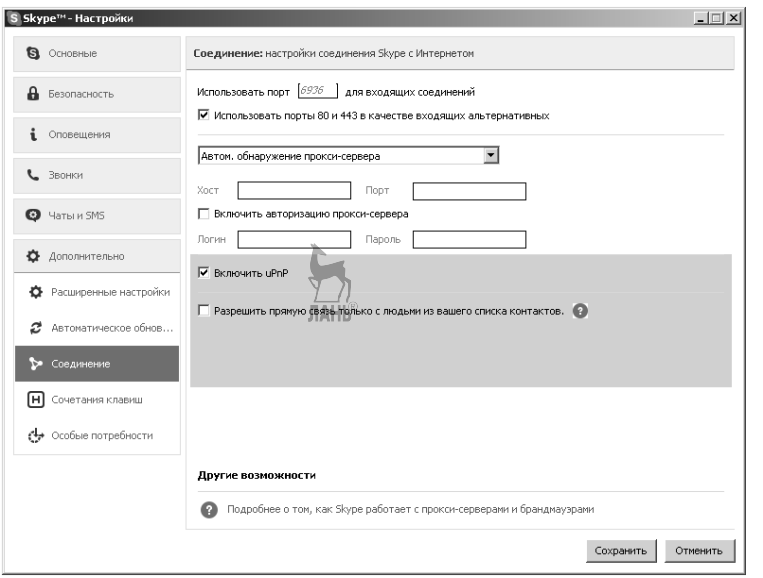


**Рис. 5.7.5**

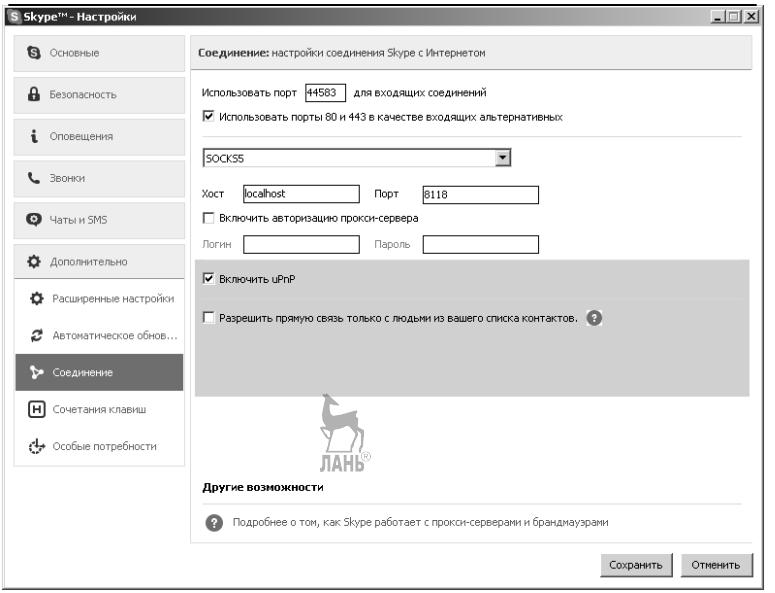


**Рис. 5.7.6**

## 5.8. Установка и использование сети I2P

**I2P** (аббревиатура *Invisible Internet Project*) — оверлейная сеть, т. е. работающая поверх обычного Интернета.

Получить информацию о сети можно по адресу: **http://i2prus.wordpress.com/tag/i2p/.**

### 5.8.1. Установка Java-машины

Программное обеспечение для работы с **I2P** написано на **Java**, поэтому сначала необходимо установить виртуальную **Java**-машину.

Для загрузки виртуальной **Java**-машины необходимо выполнить следующие действия:

– перейти по адресу **http://java.com/ru/**;

– в появившемся окне **Java.com: Java и вы — Windows Internet Explorer** нажать кнопку **Загрузить Java бесплатно**, рис. 5.8.1.1;

– в появившемся изменённом окне **Загрузить Java для Windows — Windows Internet Explorer** нажать кнопку **Согласиться и начать бесплатную загрузку**, рис. 5.8.1.2;

– в появившемся окне **Загрузка файла — предупреждение системы безопасности** нажать кнопку **Запустить**, рис. 5.8.1.3;


**Рис. 5.8.1.1**


**Рис. 5.8.1.2**

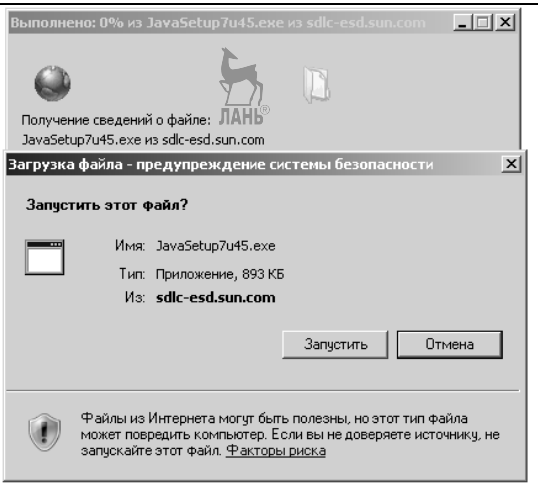


**Рис. 5.8.1.3**

– в появившемся окне **Internet Explorer — предупреждение системы безопасности** нажать кнопку **Выполнить**, рис. 5.8.1.4;

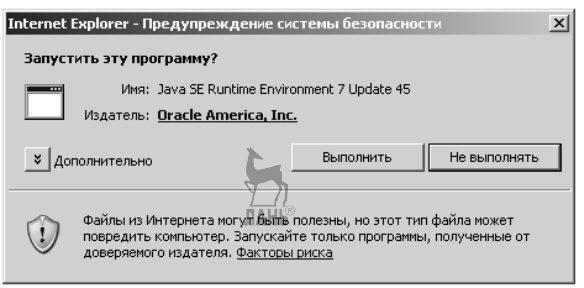


**Рис.5.8.1.4**

– в появившемся окне **Java Setup — Welcome** нажать кнопку **Install**, рис. 5.8.1.5;

– в появившемся окне **Java Setup — Progress** наблюдать процесс инсталляции, рис. 5.8.1.6;

– в появившемся окне **Java Setup — Complete** нажать кнопку **Close**, рис. 5.8.1.7;

– в появившемся окне **Verify Java Version — Windows Internet Explorer** нажать кнопку **Verify Java Version**, рис. 5.8.1.8;

– процесс инсталляции отобразится в окне **Downloading Java Installer**, рис. 5.8.1.9;


**Рис. 5.8.1.5**


**Рис. 5.8.1.6**


**Рис. 5.8.1.7**


**Рис. 5.8.1.8**


**Рис. 5.8.1.9**

– в появившемся окне **Do you want run this application** нажать кнопку **Run**, рис. 5.8.1.10;


**Рис. 5.8.1.10**

– в появившемся окне **Java Setup — Close Browsers** нажать кнопку **Close Browsers and Continue**, рис. 5.8.1.11;


**Рис. 5.8.1.11**

– в появившемся изменённом окне **Java Setup — Close Browsers** нажать кнопку **ОК**, рис. 5.8.1.12;

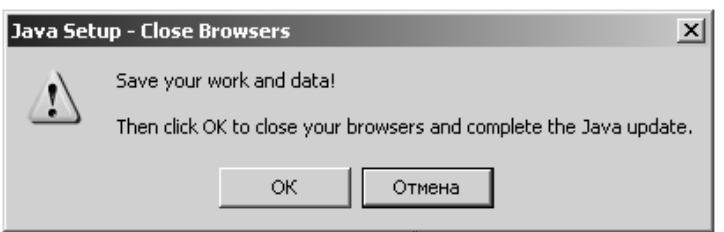


**Рис. 5.8.1.12**

– перезагрузить компьютер и в разделе **Установка и удаление программ** убедиться в появлении **Java 7 Update 45**, рис. 5.8.1.13.

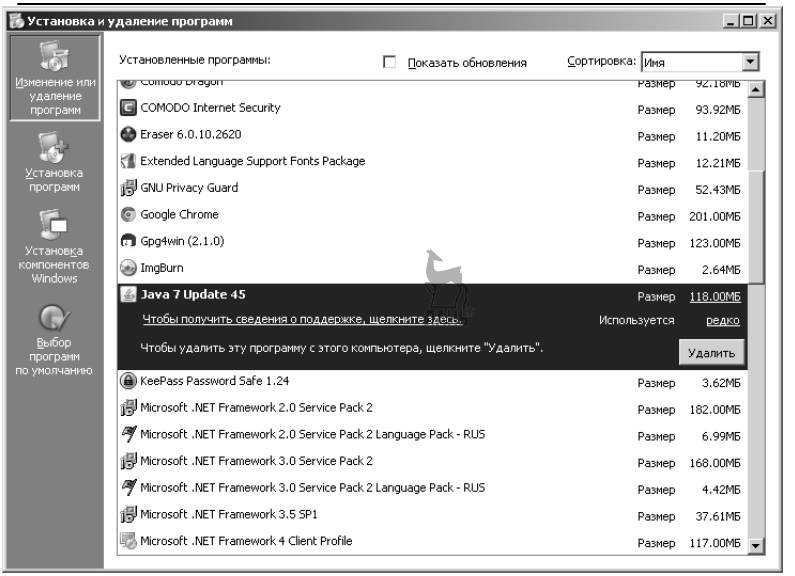


**Рис. 5.8.1.13**

## 5.8.2. Установка I2P

После установки **Java**-машины необходимо перейти на сайт **http://www.i2p2.de/download_ru** и скачать графический инсталлятор — программу **i2p install**:

– в появившемся окне **Скачать — I2P — Windows Internet Explorer** выбрать **i2pinstall_0.9.8.1_windows.exe**, рис. 5.8.2.1;

– в появившемся окне **Загрузка файла — предупреждение системы безопасности** нажать кнопку **Запустить**, рис. 5.8.2.2;

– можно в появившемся окне **Загрузка файла — предупреждение системы безопасности** нажать кнопку **Сохранить**, рис. 5.8.2.2;

– тогда выполнить сохранение, например как показано на рис. 5.8.2.3;

– в появившемся окне **Загрузка завершена** нажать кнопку **Запустить**, рис. 5.8.2.4;

– в появившемся окне **Internet Explorer — предупреждение системы безопасности** нажать кнопку **Выполнить**, рис. 5.8.2.5;

– в появившемся окне **Language Selection** выбрать язык и нажать кнопку **ОК**, рис. 5.8.2.6;

– в появившемся окне **IzPack — Установка i2p** нажать кнопку **Далее**, рис. 5.8.2.7;

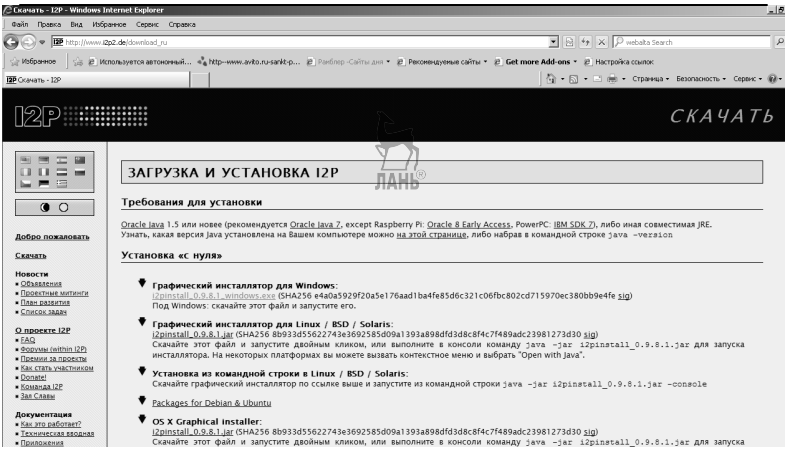


**Рис. 5.8.2.1**

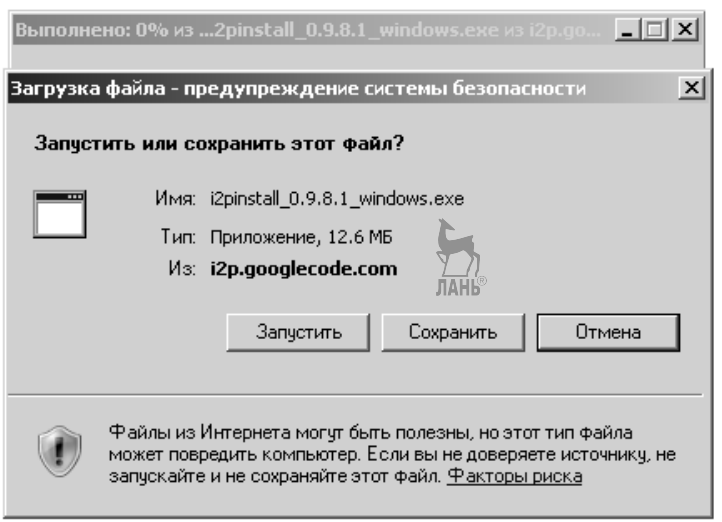


**Рис. 5.8.2.2**

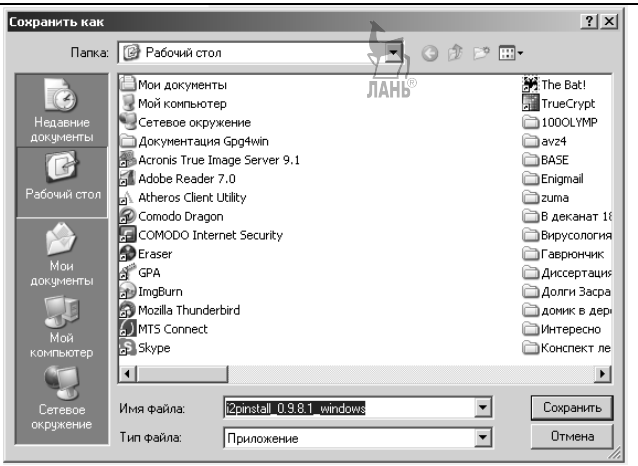


**Рис. 5.8.2.3**

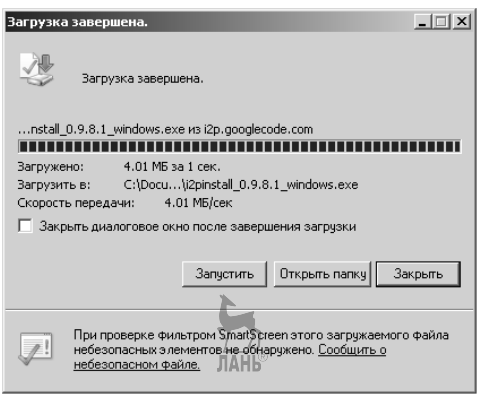


**Рис. 5.8.2.4**

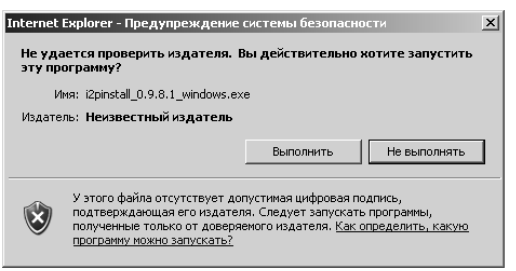


**Рис. 5.8.2.5**


**Рис. 5.8.2.6**

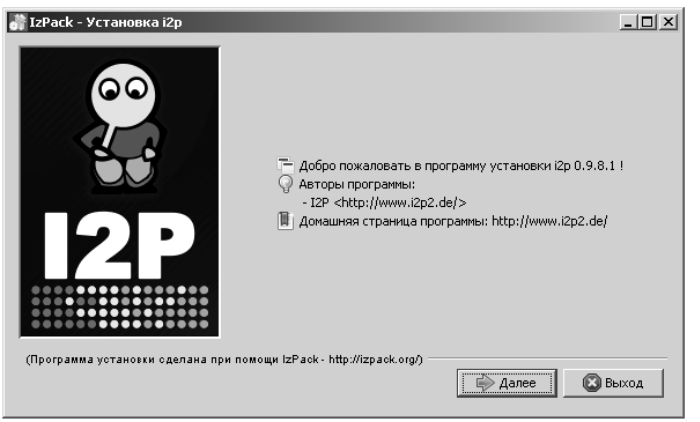


**Рис. 5.8.2.7**

– в появившемся изменённом окне **IzPack — Установка i2p** ознакомиться с информацией и нажать кнопку **Далее**, рис. 5.8.2.8;

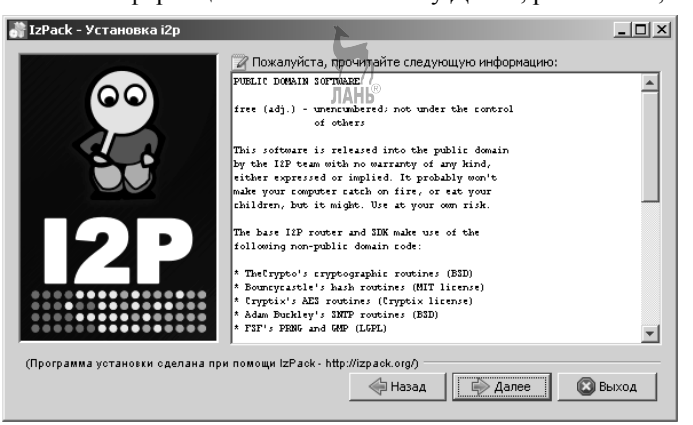


**Рис. 5.8.2.8**

– в появившемся изменённом окне **IzPack — Установка i2p** установить «флажок» на **Windows Service** и нажать кнопку **Далее**, рис. 5.8.2.9;

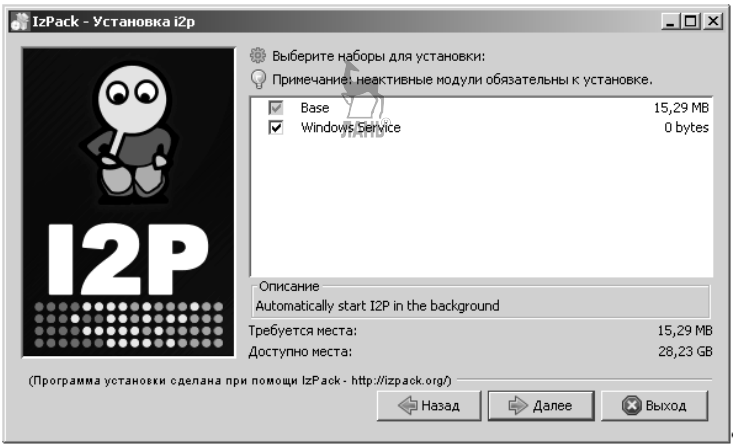


**Рис. 5.8.2.9**

– в появившемся изменённом окне **IzPack — Установка i2p** выбрать каталог установки и нажать кнопку **Далее**, рис. 5.8.2.10;

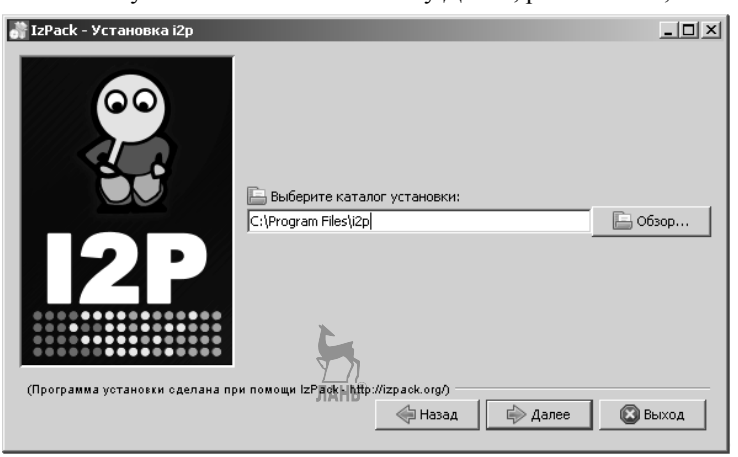


**Рис. 5.8.2.10**

– в появившемся окне **installer.Message** нажать кнопку **ОК**, рис. 5.8.2.11;

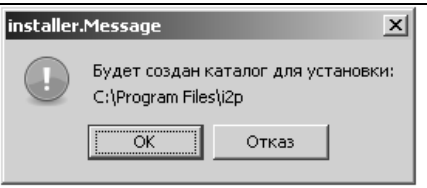


**Рис. 5.8.2.11**

– в появившемся изменённом окне **IzPack — Установка i2p** указать места создания ярлыков и нажать кнопку **Далее**, рис. 5.8.2.12;

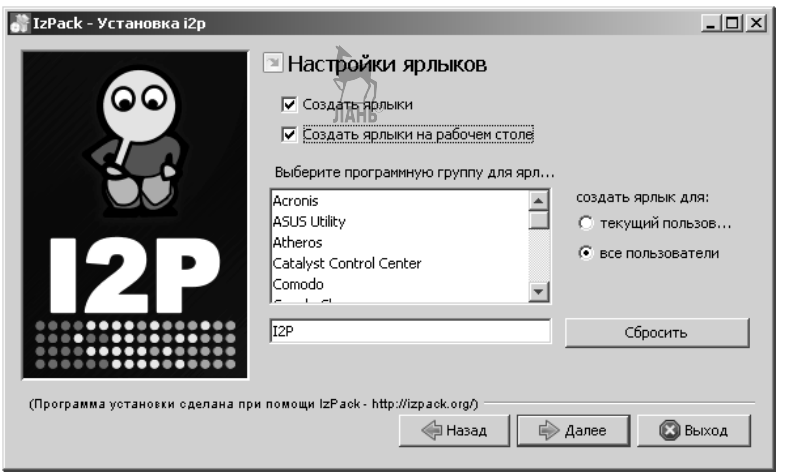


**Рис. 5.8.2.12**

– в появившемся изменённом окне **IzPack — Установка i2p** увидеть ход установки и нажать кнопку **Далее**, рис. 5.8.2.13;

– в появившемся изменённом окне **IzPack — Установка i2p** увидеть информацию об успешной установке и нажать кнопку **Завершено**, рис. 5.8.2.14;

– убедиться в появлении ярлыков **I2P** на **Рабочем столе**, рис. 5.8.2.15;

– запустив программу **services**, можно убедиться, что служба **I2P Service** установлена и работает, рис. 5.8.2.16.


**Рис. 5.8.2.13**

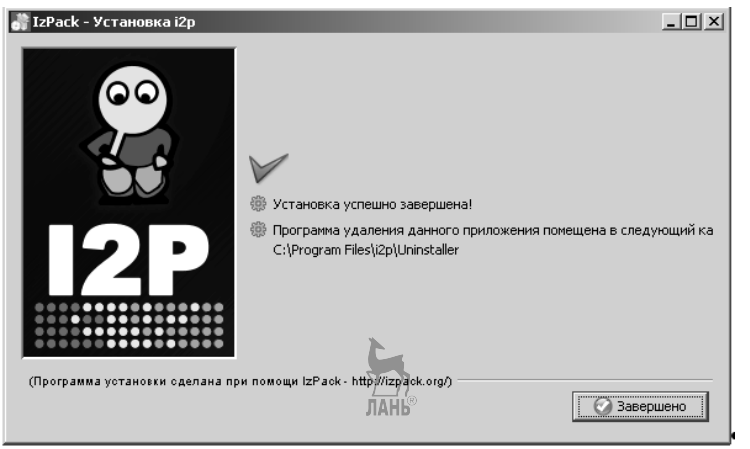


**Рис. 5.8.2.14**

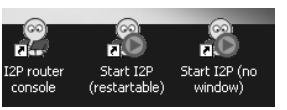


**Рис. 5.8.2.15**

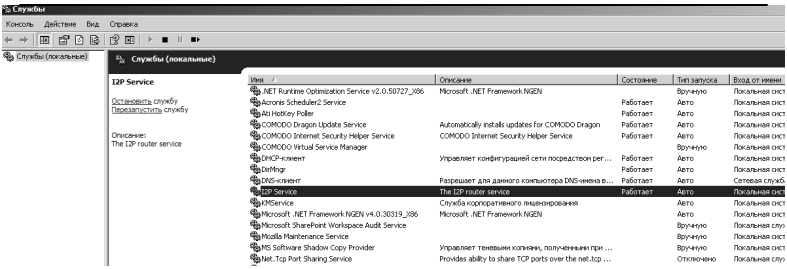


**Рис. 5.8.2.16**

## 5.8.3. Выбор и установка браузера для работы в сети I2P

После установки **I2P** целесообразно выбрать и, если надо, установить и настроить браузер. В принципе можно использовать любой, но с **Firefox** будет проще. Чтобы скачать браузер **Firefox** необходимо перейти, например, по адресу: **http://fx.yandex.ru/?from=direct_serp__6|:**

– в появившемся окне **Firefox 26** нажать кнопку **Скачать бесплатно**, рис. 5.8.3.1;

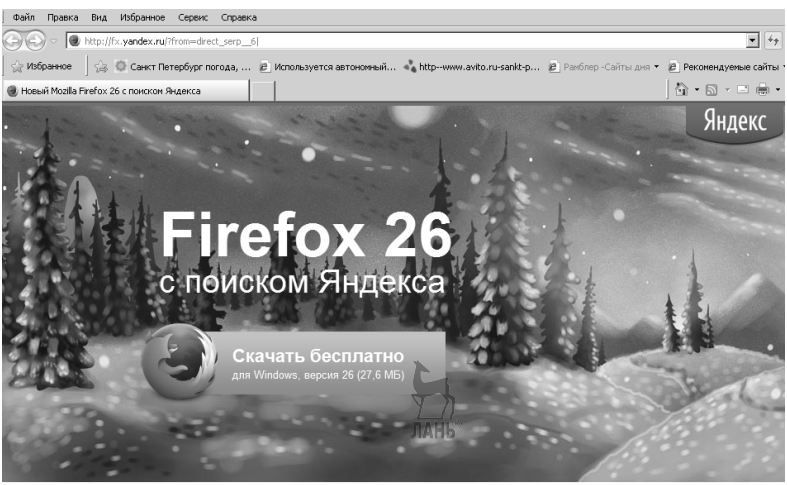


**Рис. 5.8.3.1**

– в появившемся окне **Загрузка файла — предупреждение системы безопасности** нажать кнопку **Сохранить**, рис. 5.8.3.2;

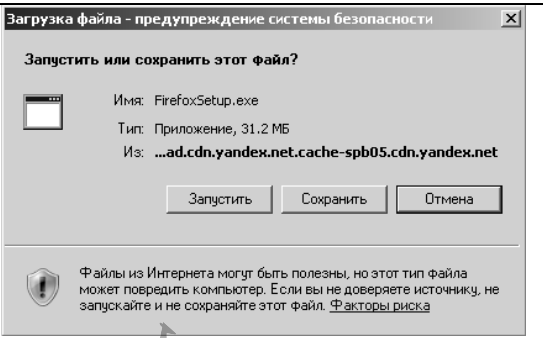


**Рис. 5.8.3.2**

– в появившемся окне **Сохранить как** выбрать место для размещения файла **FirefoxSetup**, например папка Мои документы, и нажать кнопку **Сохранить**, рис. 5.8.3.3;

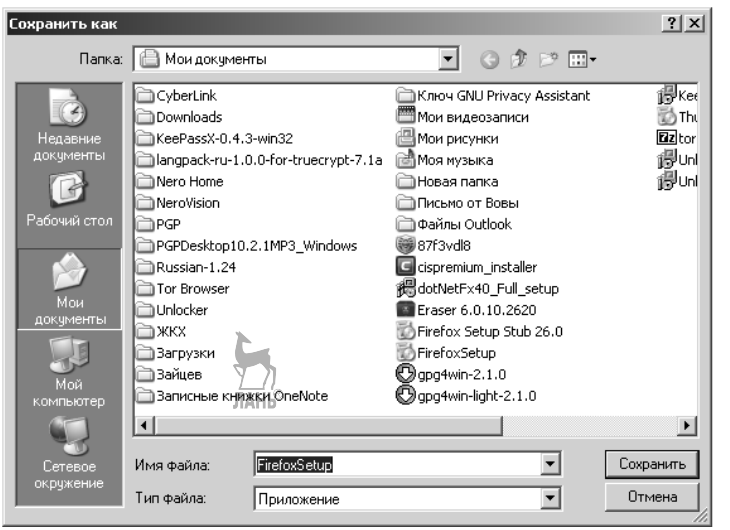


**Рис. 5.8.3.3**

– после чего щёлкнуть мышкой по файлу **FirefoxSetup** и в появившемся окне **Открыть файл — предупреждение системы безопасности** нажать кнопку **Выполнить**, рис. 5.8.3.4;

– в появившемся окне увидеть процесс установки, рис. 5.8.3.5;

– затем в появившемся окне **Установка Mozilla Firefox** нажать кнопку **Далее**, рис. 5.8.3.6;

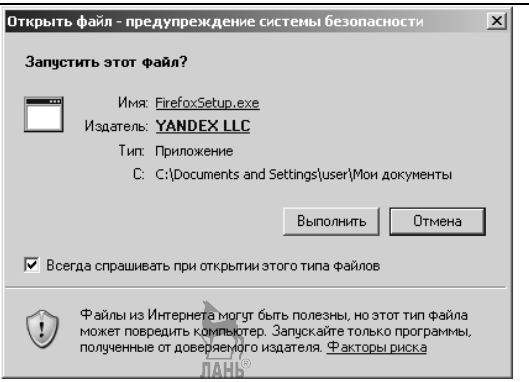


**Рис. 5.8.3.4**

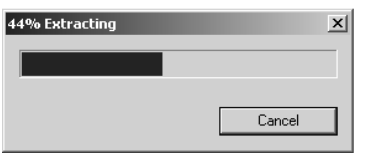


**Рис. 5.8.3.5**

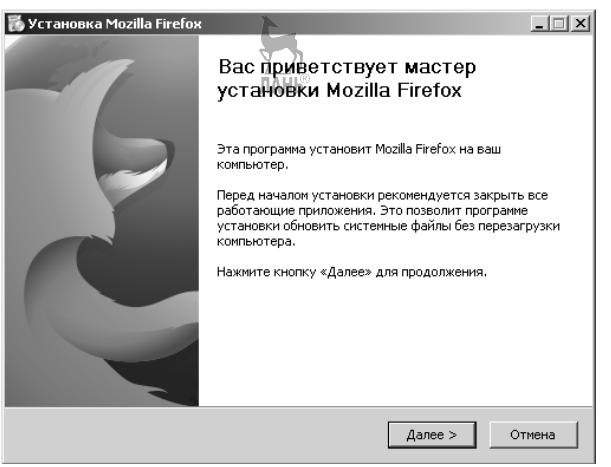


**Рис. 5.8.3.6**

– в появившемся изменённом окне **Установка Mozilla Firefox** выбрать **Обычная** и нажать кнопку **Далее**, рис. 5.8.3.7;

– в появившемся изменённом окне **Установка Mozilla Firefox** нажать кнопку **Обновить**, рис. 5.8.3.8;

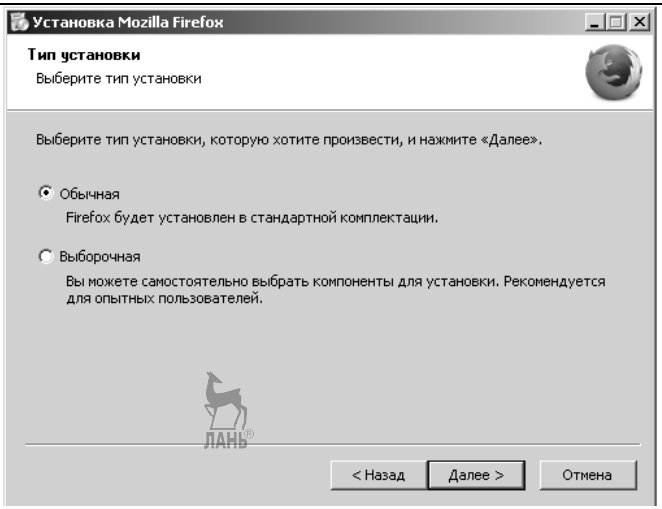


**Рис. 5.8.3.7**

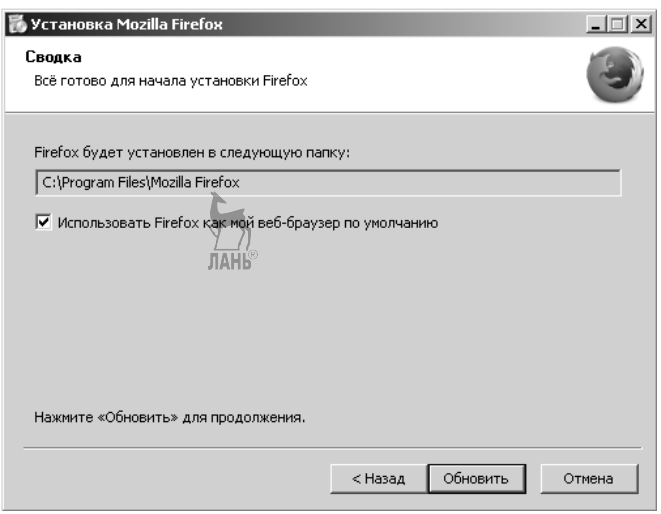


**Рис.5.8.3.8**

– в появившемся изменённом окне **Установка Mozilla Firefox** увидеть процесс копирования, рис. 5.8.3.9;

– в появившемся изменённом окне **Установка Mozilla Firefox** нажать кнопку **Готово**, рис. 5.8.3.10.

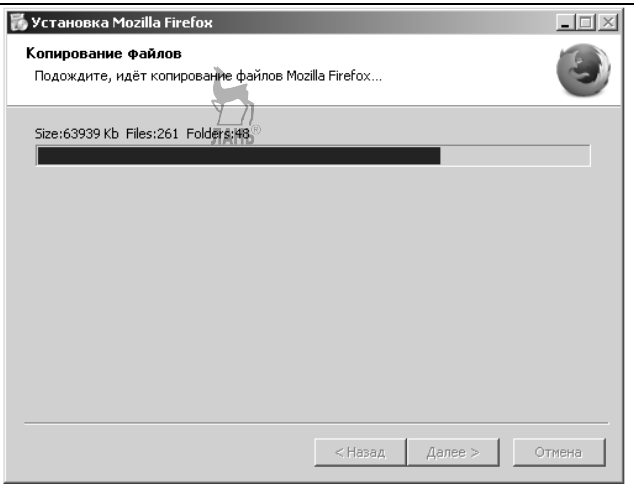


**Рис. 5.8.3.9**

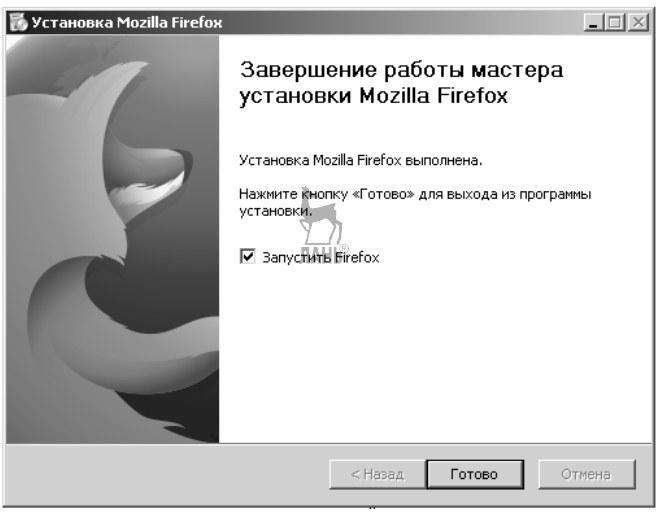


**Рис. 5.8.3.10**

## 5.8.4. Настройка сети I2P

Для настройки можно воспользоваться информацией, представленной по адресу: **http://alexeev.pro/?page_id=1489**.

Щёлкнуть мышкой по ярлыку **I2P router console** или по **ярлыку Start I2P (restartable)**, рис. 5.8.4.1:


**Рис. 5.8.4.1**

– в появившемся окне **Консоль маршрутизатора I2P** убедиться, что в разделе **Локальные туннели** есть надпись **Коллективные клиенты**. Если такая надпись есть и горит зеленая звезда, то это значит, что мы успешно подключились к **I2P** Интернету, щёлкнуть мышкой по кнопке **I2P,** рис. 5.8.4.2;

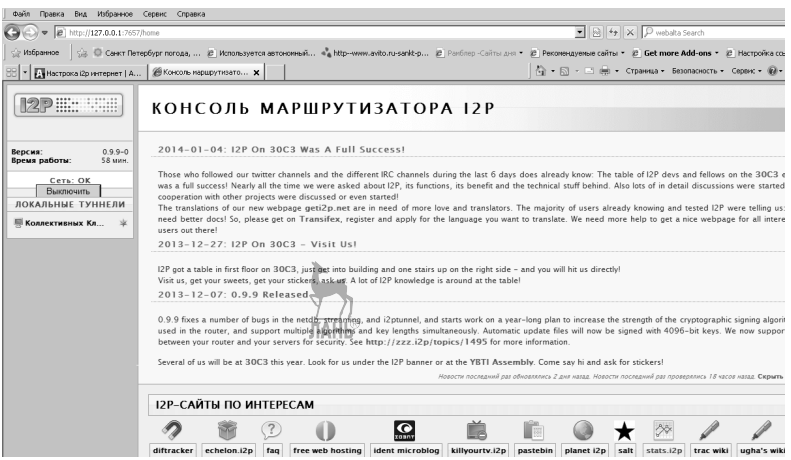


**Рис. 5.8.4.2**

– в появившемся изменённом окне **Консоль маршрутизатора I2P** выбрать **Настройки I2P** и приступить к первоначальной настройке **I2P-маршрутизатора**, рис. 5.8.4.3;

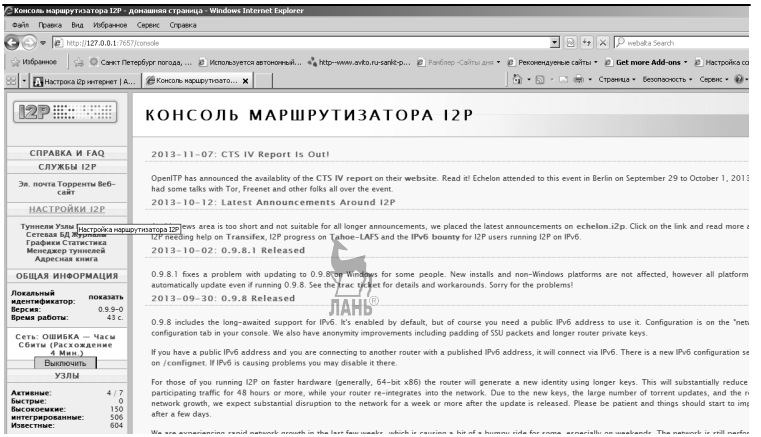


**Рис. 5.8.4.3**

– в появившемся окне **Настройка полосы пропускания для I2P** можно ничего не менять, можно вписать значения **256** и **512** килобайт/секунду на приём и отдачу соответственно, так как при этом повышается трафик, и нажать кнопку **Сохранить изменения**, рис. 5.8.4.4;

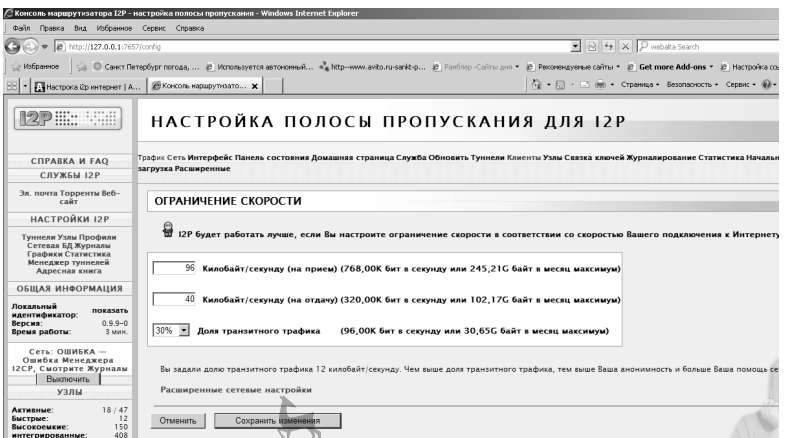


**Рис. 5.8.4.4**

– чтобы появилась возможность открыть **I2P**-сайт, необходимо добавить в **адресную книгу** адреса подписок, для чего щёлкаем по ссылке **Адресная книга** и в появившемся разделе **Адресные Книги** выбираем **Подписки**, рис. 5.8.4.5;

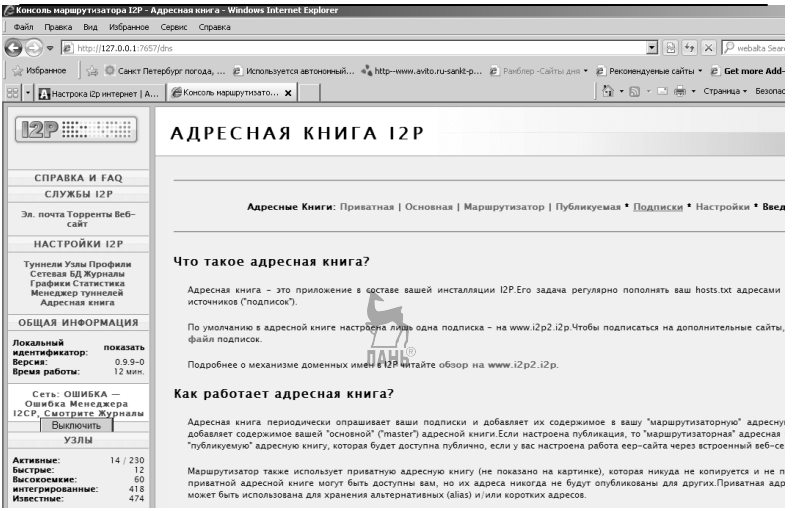


**Рис. 5.8.4.5**

– в появившемся изменённом окне **Адресная книга I2P** в окно **C:\DocumentsandSettings\user\ApplicationData\I2P\addressbook\subscriptions.txt** добавляем список

**http://www.i2p2.i2p/hosts.txt**
**http://i2host.i2p/cgi-bin/i2hostetag**
**http://stats.i2p/cgi-bin/newhosts.txt**
**http://tino.i2p/hosts.txt**
**http://dream.i2p/hosts.txt**
**http://hosts.i2p/**
**http://trevorreznik.i2p/hosts.txt**
**http://cipherspace.i2p/addressbook.txt**
**http://hosts.i2p/hosts.cgi?filter=all**
**http://bl.i2p/hosts2.txt**
**http://rus.i2p/hosts.txt**,

рис. 5.8.4.6;

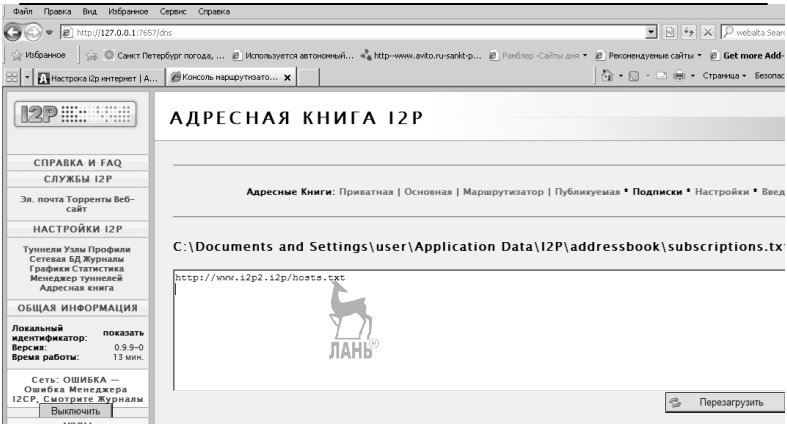


**Рис. 5.8.4.6**

– чтобы получилось, как показано на рисунке, и нажать кнопку **Сохранить**, рис. 5.8.4.7.

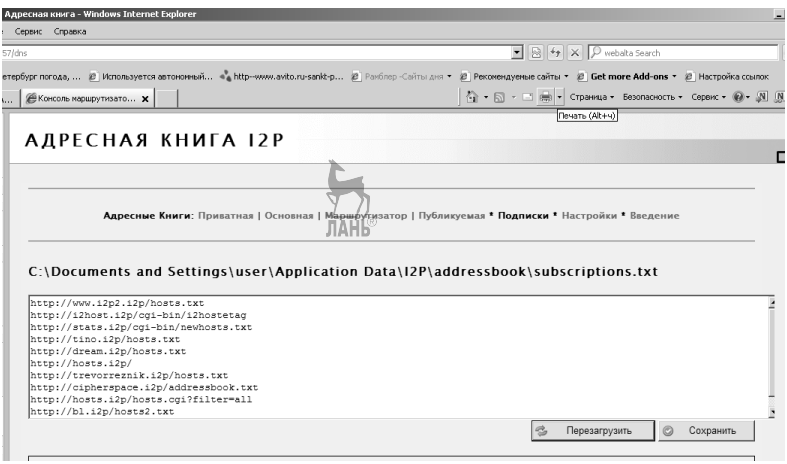


**Рис. 5.8.4.7**

Первоначальные настройки **I2P** можно считать законченными, для более или менее комфортного пребывания в сети этого достаточно.

## 5.8.5. Создание учётной записи в сети I2P

Перед созданием учёной записи необходимо пройти по цепочке **Пуск, Панель управления, Свойства обозревателя**:

– в появившемся окне **Свойства: Интернет** выбрать **Подключения,** рис. 5.8.5.1;

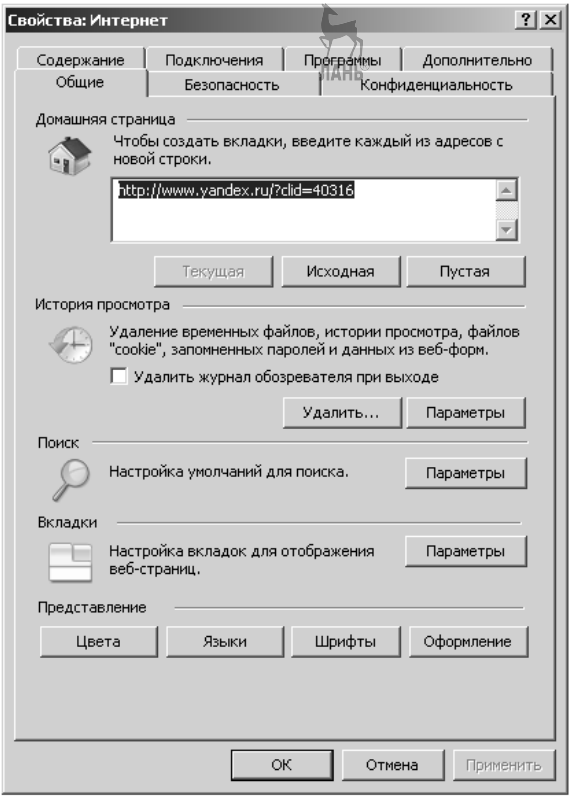


**Рис. 5.8.5.1**

– в появившемся изменённом окне **Свойства: Интернет** нажать кнопку **Настройка сети**, рис. 5.8.5.2;

– в появившемся изменённом окне **Свойства: Интернет** установить «флажки» как показано на рис. 5.8.5.3 и нажать кнопку **Дополнительно**;

– в появившемся окне **Параметры прокси-сервера** прописать адрес и порт, как показано на рис. 5.8.5.4.

Последовательно три раза нажать кнопку **ОК** и закрыть окно **Панель управления**.

Комментарии: *после установки параметров прокси-сервера, необходимых для работы сети* ***I2P****, простой Интернет перестаёт работать.*

*Сеть* ***TOR*** *и почтовый клиент* ***Thunderbird работают*** *нормально.*

*Чтобы обеспечить работу простого Интернета, необходимо вернуться к первоначальным настройкам, т. е. отключить прокси-сервер.*

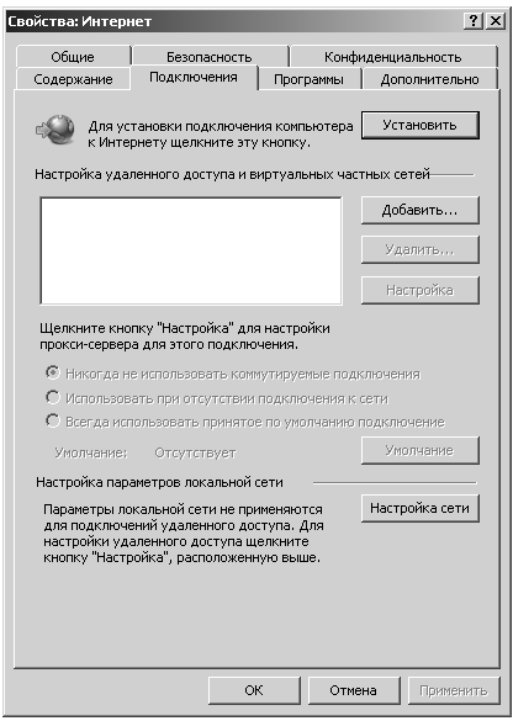


**Рис. 5.8.5.2**

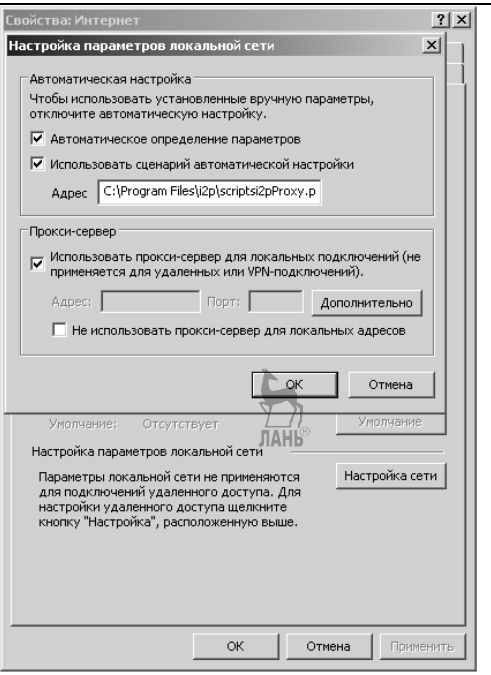


**Рис. 5.8.5.3**

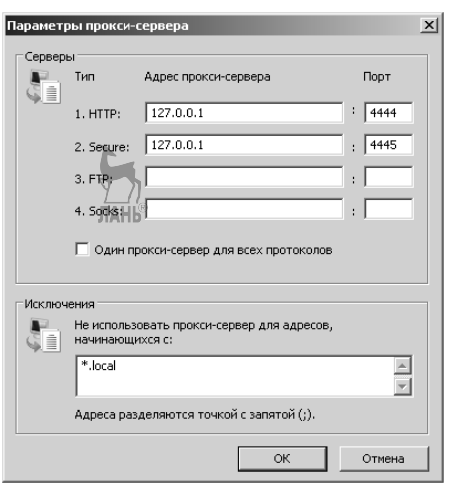


**Рис. 5.8.5.4**

Для создания учётной записи необходимо, находясь на **Консоли маршрутизатора I2P**, выбрать раздел **Эл. Почта** и щёлкнуть мышкой, рис. 5.8.5.5:

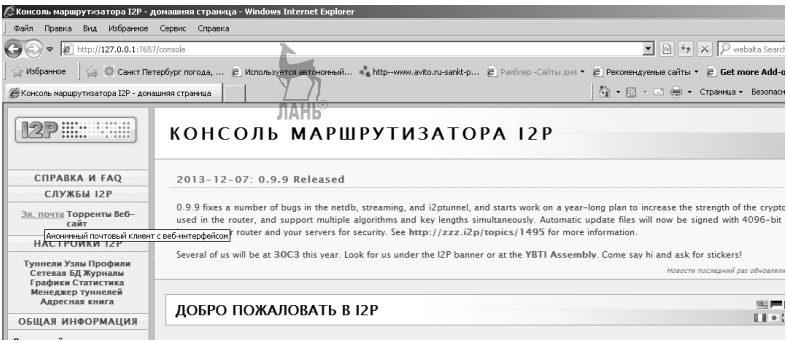


**Рис. 5.8.5.5**

– в появившемся окне **susimail — Логин — Windows Internet Explorer** щёлкнуть по ссылке **Создать учётную запись**, рис. 5.8.5.6;

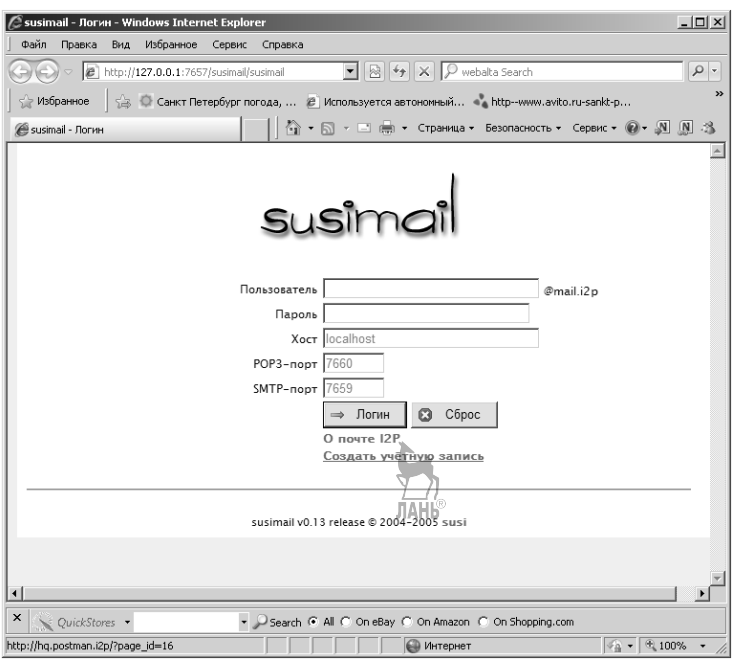


**Рис. 5.8.5.6**

– в появившемся окне **PostmanHQ>>1. Creating a mailbox — Windows Internet Explorer** заполнить форму, предлагаемую **Postman HQ**, указав имя ящика и пароль, и щёлкнуть по кнопке **Proceed**, рис. 5.8.5.7;

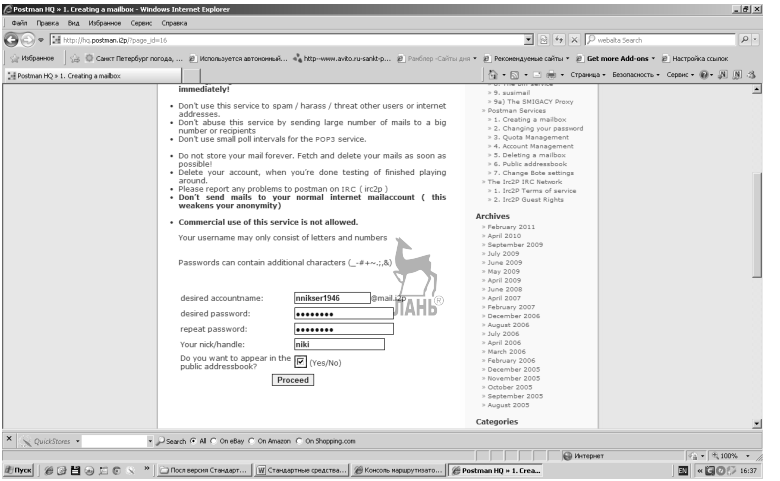


**Рис. 5.8.5.7**

– в появившемся изменённом окне **PostmanHQ>>1. Creatinga-mailbox — Windows Internet Explorer** увидеть сообщение **Postman HQ** (имя ящика и пароль) и подтвердить своё согласие, щёлкнув по кнопке **Confirm and Create Mailbox**, рис. 5.8.5.8;

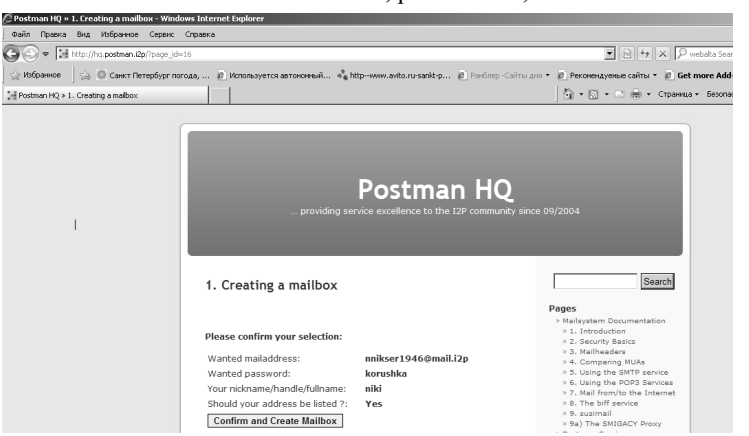


**Рис. 5.8.5.8**

– в появившемся изменённом окне **Postman HQ>>1. Creating a mailbox —- Windows Internet Explorer** увидеть данные о созданном ящике, рис. 5.8.5.9.

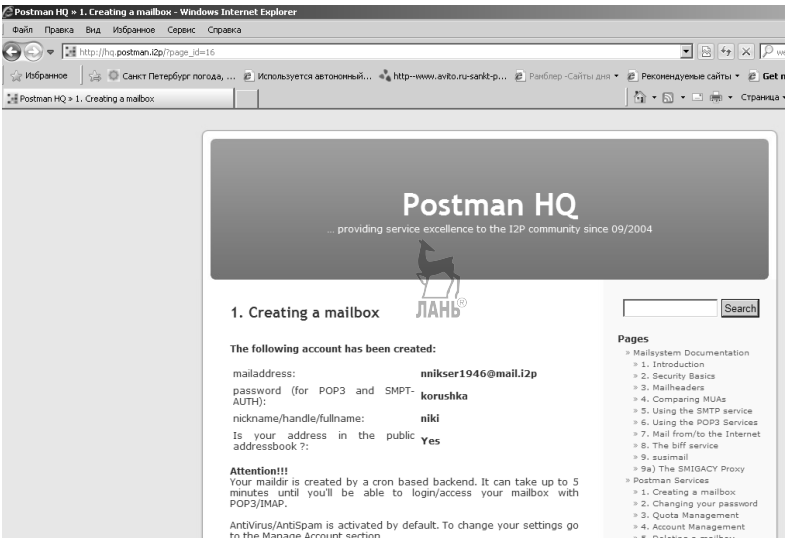


**Рис. 5.8.5.9**

Ящик **nnikser@mail.i2p** создан.

## 5.8.6. Почта в сети I2P

**http://hq.postman.i2p/** является почтовым сервером сети **I2P**. Для того чтобы там зарегистрироваться, можно создать учётную запись, как было сделано в разделе 5.8.5, а можно пройти по ссылке **http://hq.postman.i2p/?page_id=16**. После регистрации вы получите ящик вида username@mail.i2p, в данном случае **nnikser@mail.i2p**. Есть, правда, одно ограничение. Если вы не будете пользоваться заведенным ящиком 100 дней (в течение этого периода ни разу в него не зайдете), то он будет удален.

Чтобы войти в электронную почту сети **I2P** можно, находясь на **Консоли маршрутизатора I2P**, выбрать раздел **Эл. Почта** и щёлкнуть мышкой, рис. 5.8.6.1.

А можно щёлкнуть мышкой по пиктограмме **Эл. почта**, находясь на **Консоли маршрутизатора I2P,** рис. 5.8.6.1:

– в появившемся окне **susimal — Логин — Windows Internet Explorer** ввести имя своего почтового ящика (**Пользователь**), пароль и нажать **Логин** или **Enter**, рис. 5.8.6.3;

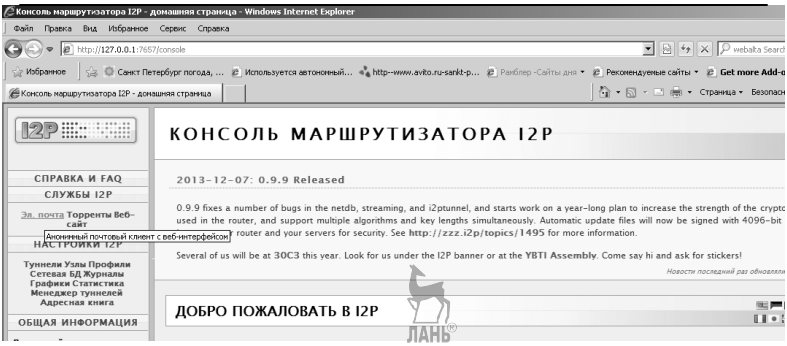


**Рис. 5.8.6.1**

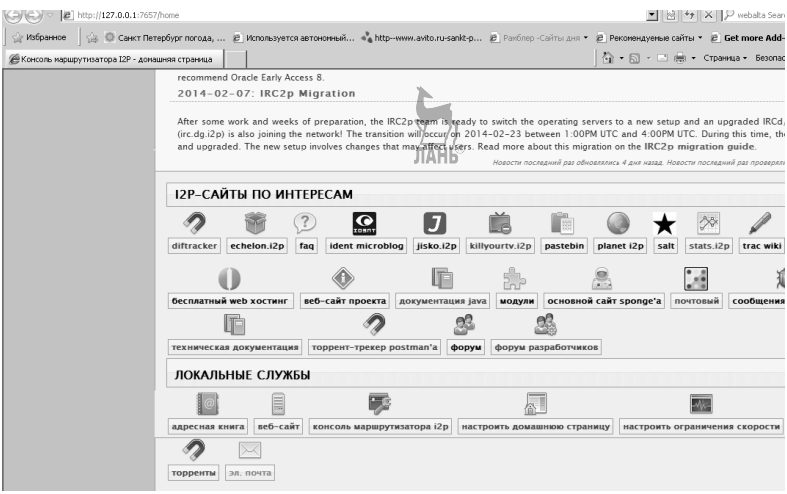


**Рис. 5.8.6.2**

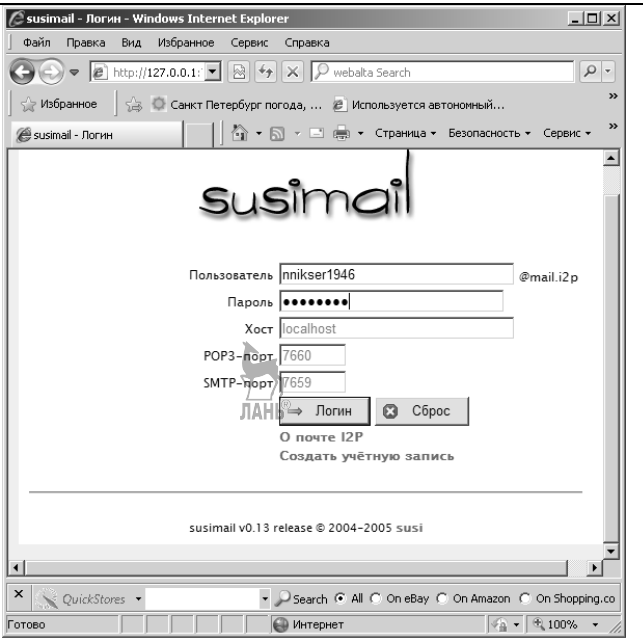


**Рис. 5.8.6.3**

– в появившемся окне откроется панель почты **Susimal,** рис. 5.8.6.4.


**Рис. 5.8.6.4**

## 5.8.7. Настройка почтового клиента Mozilla Thunderbird для работы в сети I2P

Сначала необходимо запустить сеть **i2p**, щёлкнув по пиктограмме **StartI2P** (по **Window**), рис. 5.8.4.1.

Затем создать учётную запись, как описано в разделе 5.8.5.

В данном случае создан ящик **nnikser1946@mail.i2p**.

Далее запустить почтовый клиент **Mozilla Thunderbird**, щёлкнув по пиктограмме, рис. 5.8.7.1:

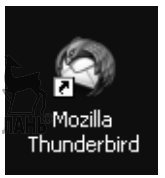


**Рис. 5.8.7.1**

– в появившемся окне **«Thunderbird» «Почта» — Nikiforov_sergei@mail.ru** (в конкретном случае), пройдя по цепочке **Учётные записи**, **Создать учётную запись**, **Электронная почта**, создать учётную запись с тем же именем, что и в **Susimail** сети **i2p**, т. е. **nnikser1946@mail.i2p,** рис. 5.8.7.2.

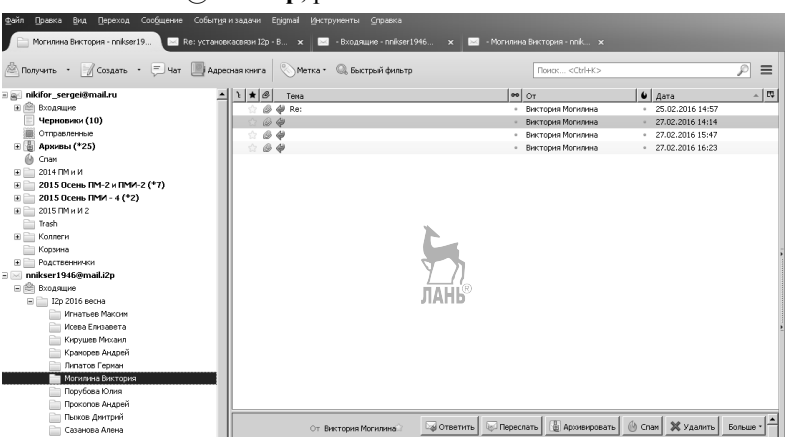


**Рис. 5.8.7.2**

Выбрав учётную запись **nnikser1946@mail.i2p, Просмотр параметров этой учёной записи**, установить в окне **Параметры учётной записи** (в данном случае для **nnikser1946@mail.i2p**) параметры, как показано на рис. 5.8.7.3.

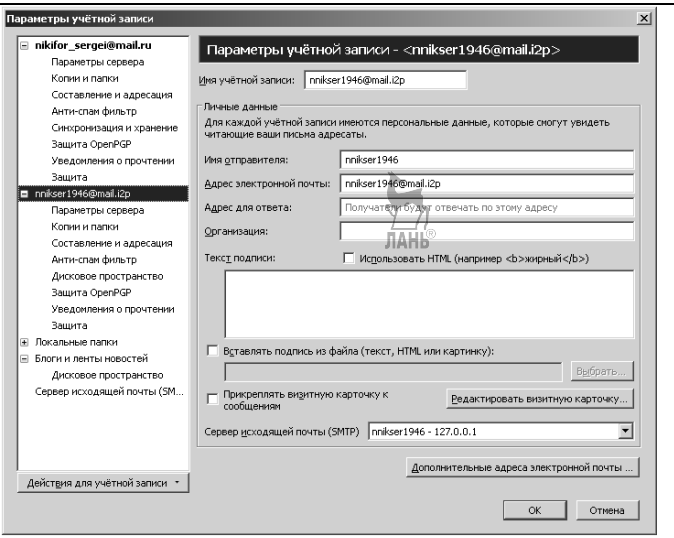


**Рис. 5.8.7.3**

Выбрав в окне **Параметры учётной записи** раздел **Параметры сервера**, установить их, как показано на рис. 5.8.7.4.

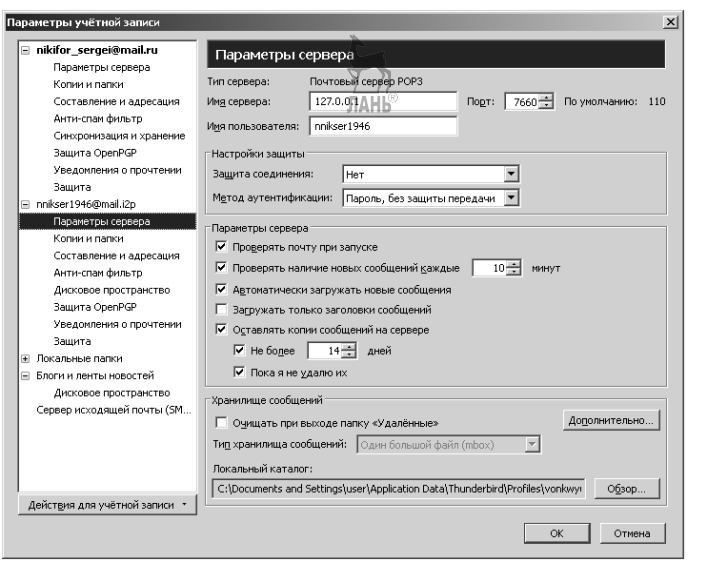


**Рис. 5.8.7.4**

Выбрав в окне **Параметры учётной записи,** раздел **Сервер исходящей почты (SMTP)**, установить параметры, как показано на рис. 5.8.7.5.

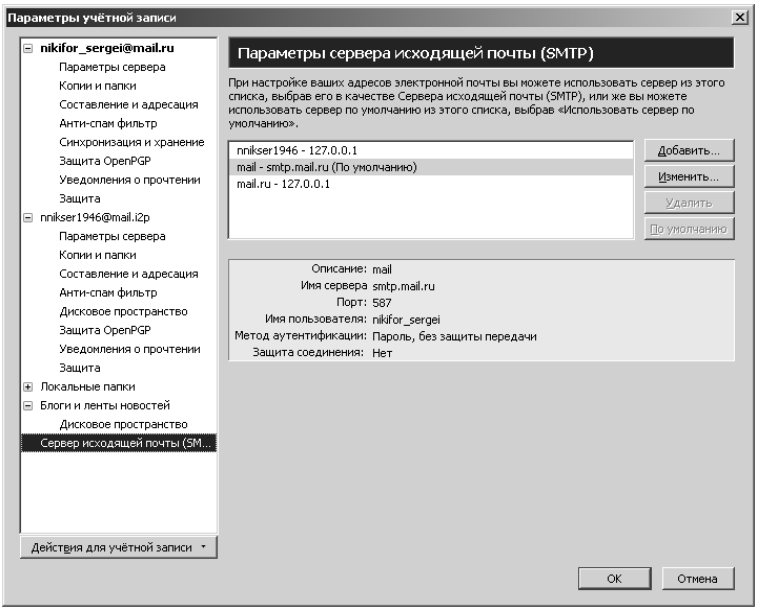


**Рис. 5.8.7.5**

Собственно, всё. В результате почтовый клиент **Thunderbird** будет работать с почтой **I2P**, как с обычным ящиком. Остаётся ждать писем и писать самому.

## 5.9. Установка и использование сети Hamachi

**Hamachi —** программное обеспечение, предназначенное для построения **VPN**[4]. **Hamachi** позволяет создать собственную защищён-

[4] *Virtual Private Network* — виртуальная частная сеть — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

ную сеть из компьютеров, соединённых через Интернет, как будто они соединены одной физической локальной сетью.

**Hamachi** позволяет создать локальную сеть (**LAN**[5]) поверх Интернета. Чаще всего **Hamachi-**сети используются для соединения серверов с серым **IP**[6] и клиентских компьютеров. Кстати, такой метод значительно усложняет дешифрацию клиентского трафика.

Любые приложения, которые работают через локальную сеть, могут работать через сети **Hamachi**, при этом передаваемые данные будут защищены, и обмен между ними осуществляется в стиле **peer-to-peer**[7].

**Hamachi** — система организации виртуальных защищённых сетей на основе протокола **UDP**[8]. В такой сети узлы для установления соединения между собой используют третий узел, который помогает им лишь обнаружить друг друга, а передача информации производится непосредственно между узлами. При этом взаимодействующие узлы могут находиться за **NAT**[9] или фаерволом.

Получить информацию о сети можно по адресу **http://i2prus.wordpress.com/tag/i2p/.**

### 5.9.1. Установка сети Hamachi

Скачать программу можно с официального сайта **https://secure.logmein.com›hamachi.msi:**

– в появившемся окне **Загрузка файла — предупреждение системы безопасности** нажать кнопку **Сохранить**, рис. 5.9.1.1;

[5] Local Area Network, LAN — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

[6] Частный IP-адрес (от англ. *Private IP address*), также называемый *внутренним*, *внутрисетевым*, *локальным* или *«серым»*, — IP-адрес, принадлежащий к специальному диапазону, не используемому в сети Интернет.

[7] Одноранговая, децентрализованная или пиринговая (от англ. *peer-to-peer*, *P2P* — равный к равному) сеть — это оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.

[8] UDP (от англ. *User Datagram Protocol* — протокол пользовательских датаграмм) — один из ключевых элементов Transmission Control Protocol/Internet Protocol, набора сетевых протоколов для Интернета.

[9] NAT (от англ. *Network Address Translation* — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

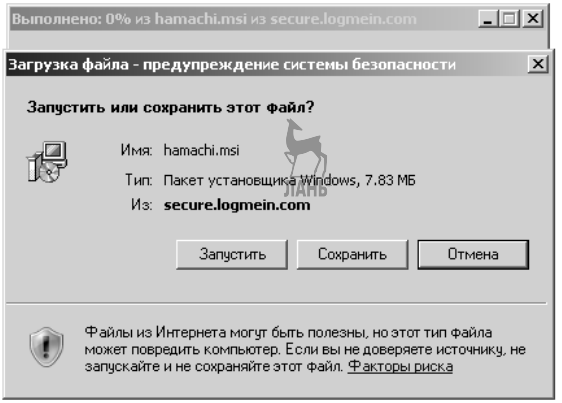


**Рис. 5.9.1.1**

– в появившемся окне **Сохранить как** выбрать раздел для сохранения, например **Мои документы**, и нажать кнопку **Сохранить**, рис. 5.9.1.2;

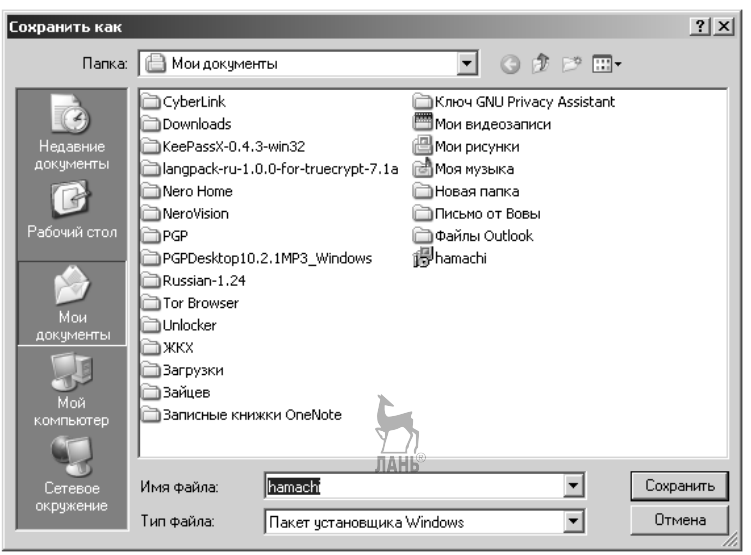


**Рис. 5.9.1.2**

– в появившемся окне **Загрузка завершена** нажать кнопку **Запустить**, рис. 5.9.1.3;

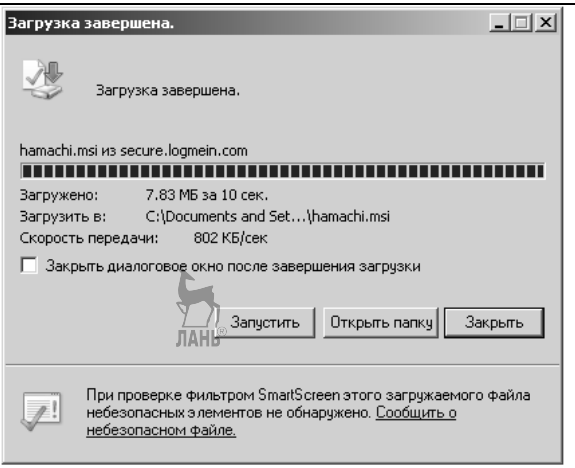


**Рис. 5.9.1.3**

– в появившемся окне **Internet Explorer — Предупреждение системы безопасности** нажать кнопку **Выполнить**, рис. 5.9.1.4;

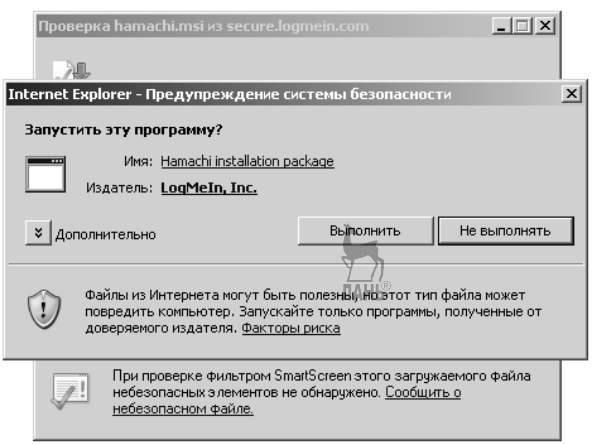


**Рис. 5.9.1.4**

– в появившемся окне **LogMeIn Hamachi Setup** выбрать язык и нажать кнопку **Next**, рис. 5.9.1.5;

– в появившемся окне **Установка LogMeIn Hamachi** нажать кнопку **Далее**, рис. 5.9.1.6;

– в появившемся изменённом окне окне **Установка LogMeIn Hamachi** нажать кнопку **Принимаю**, рис. 5.9.1.7;

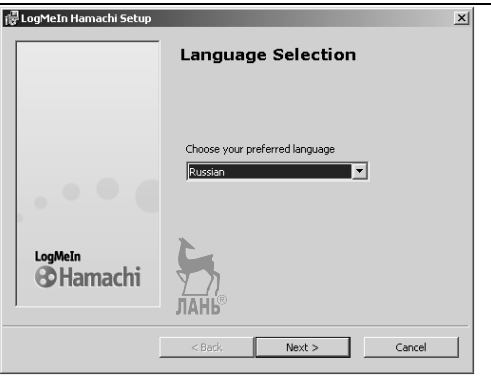


**Рис. 5.9.1.5**


**Рис. 5.9.1.6**

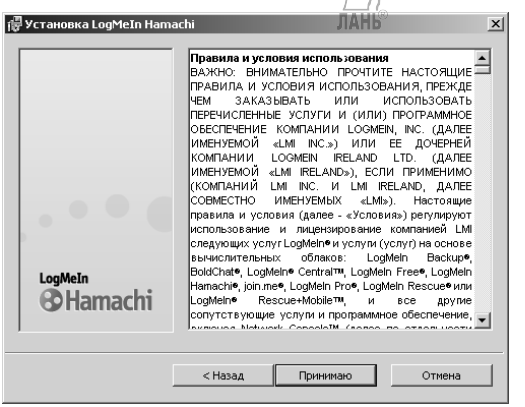


**Рис. 5.9.1.7**

– в появившемся изменённом окне окне **Установка LogMeIn Hamachi** нажать кнопку **Установить**, рис. 5.9.1.8;

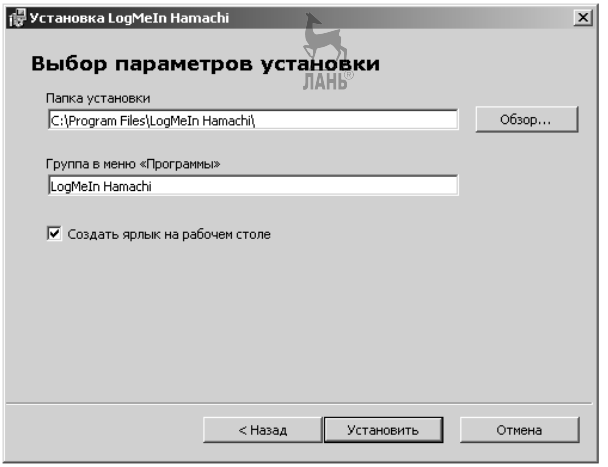


**Рис. 5.9.1.8**

– в появившемся изменённом окне **Установка LogMeIn Hamachi** нажать кнопку **Готово**, рис. 5.9.1.9;


**Рис. 5.9.1.9**

– в появившемся окне **LogMeIn Hamachi** нажать кнопку **Включить**, рис. 5.9.1.10;

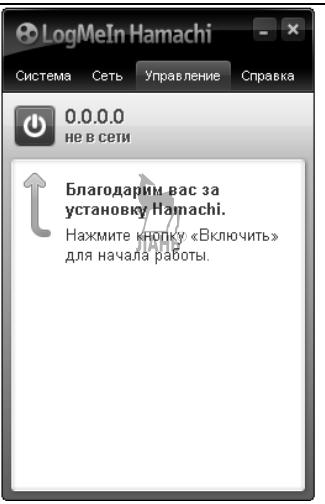


**Рис. 5.9.1.10**

– в появившемся окне **Зарегистрировать этот клиент** выбрать имя клиента, например **nicif1**, и нажать кнопку **Create**, рис. 5.9.1.11;

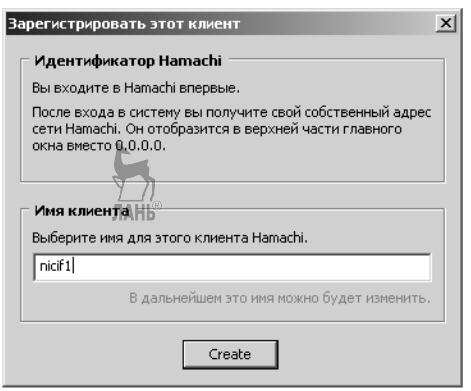


**Рис. 5.9.1.11**

– в появившемся изменённом окне **LogMeIn Hamachi** выбрать **Создать новую сеть**, рис. 5.9.1.12;

– в появившемся окне **Создание сети** выбрать идентификатор сети и пароль и нажать кнопку **Создать**, рис. 5.9.1.13;

– в появившемся окне **LogMeIn Hamachi** отобразится информация о созданной сети **nicif_pmi1**, рис. 5.9.1.14.

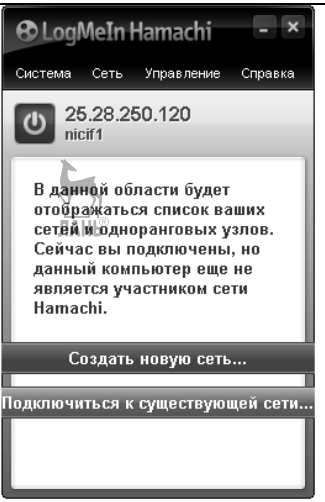


**Рис. 5.9.1.12**

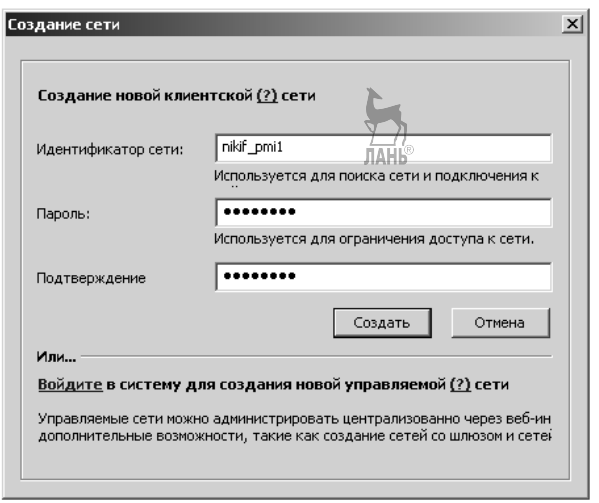


**Рис. 5.9.1.13**

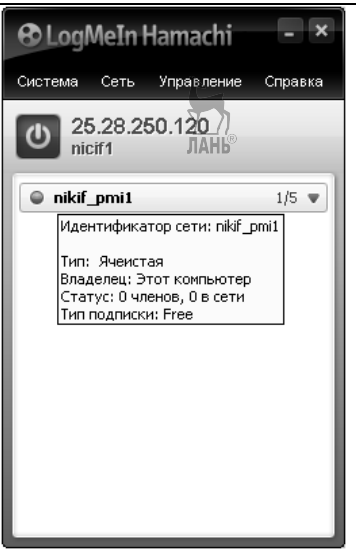


**Рис. 5.9.1.14**

## 5.9.2. Подключение к сети Hamachi

Для подключения к существующей сети **Hamachi** можно было выбрать **Подключиться к существующей сети**, рис. 5.9.1.12.

А можно, если у вас установлена своя сеть **Hamachi**, щёлкнуть по пиктограмме **LogMeIn Hamachi**, рис. 5.9.2.1:


**Рис. 5.9.2.1**

– в появившемся окне **LogMeIn Hamachi** в разделе **Сеть** выбрать **Подключиться к существующей сети** и увидеть подключение, рис. 5.9.2.2;

– в появившемся окне **Подключение к сети** указать заранее известный идентификатор сети, к которой осуществляется подключение, в данном случае **Alena_Esaulova**, и пароль и нажать кнопку **Подключиться**, рис. 5.9.2.3;

– в появившемся окне **LogMeIn Hamachi** увидеть подключение клиента **nicif1**, рис. 5.9.2.4.

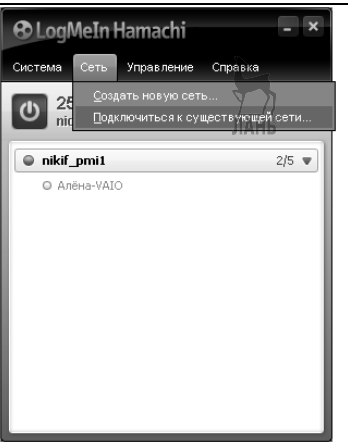


**Рис. 5.9.2.2**

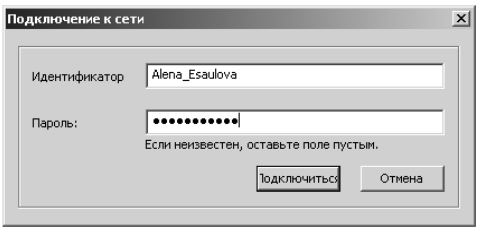


**Рис. 5.9.2.3**

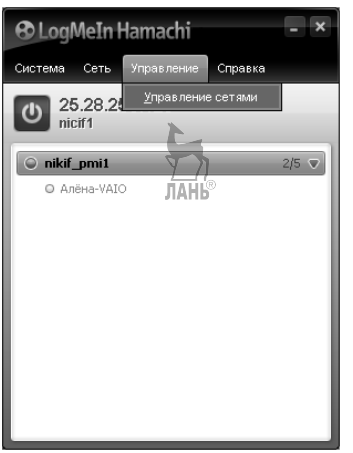


**Рис. 5.9.2.4**

# ПРИЛОЖЕНИЕ. КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ (ИНТЕРНЕТ-МАГАЗИНЫ)[10]

Развитие Интернета приводит к тому, что появляется все больше магазинов, торгующих товарами через Интернет. С одной стороны, у этой технологии есть ряд несомненных и значительных плюсов.

1. Потребитель может ознакомиться с имеющимся в наличии товаром, причем, как правило, всегда есть возможность просмотреть фотографии товара в различном ракурсе, ознакомиться с его техническими характеристиками. Нередко интерфейс интернет-магазина предоставляет набор «мастеров-помощников», осуществляющих подбор товара по различным задаваемым покупателями характеристикам или выполняющих сравнение нескольких родственных товаров.

2. Затраты на создание и содержание интернет-магазина значительно меньше, чем на содержание больших торговых площадей — причина в том, что не требуется оплачивать аренду помещений, их освещение/отопление/охрану, отсутствует воровство товара, покупателем может быть человек из любой точки страны. Следовательно, это выгодно и владельцу магазина, и покупателю (так как цена на любой товар должна покрывать издержки на его продажу, меньше издержки — меньше наценка).

3. Доставка товара транспортными или курьерскими компаниями вполне доступна по цене, происходит быстро и, как правило, качественно — следовательно, товар может быть доставлен покупателю быстро и удобным ему способом.

Однако, как известно, где белое — там обязательно будет и черное, и за любым плюсом обязательно кроется и ряд минусов. Главные минусы состоят в том, что:

1. Интернет-магазин может создать любой школьник, это не сложно. Следовательно, никакого магазина может в реальности не существовать — и проверить это непросто.

2. Покупатель «приходит» в магазин «виртуально» — т. е. работает с магазином на уровне сайта. Следовательно, реального товара он не видит, и неизвестно, есть ли указанный товар в реальности и в наличии, в каком он техническом состоянии, а главное — насколько заявленные характеристики и фотографии соответствуют реальности.

[10] Перепечатка с сайта О. Зайцева «Информационная безопасность» http://z-oleg.com/secur/avz/download.php.

3. Покупка товара через Интернет предполагает его полную или частичную предоплату — в данной ситуации все упирается в честность владельца магазина, который, получив деньги, может попросту не выслать товар или выслать товар ненадлежащего качества или другого типа. И дальше начинается самое интересное — никакого письменного договора между магазином и покупателем нет, равно как нет кассового чека или иного подтверждения покупки — и в случае чего отстоять свои права в суде будет весьма непросто (или невозможно).

Рассмотрим основные моменты, которые позволяют избежать обмана и вовремя опознать мошенников.

## Репутация магазина

Разноцветный сайт, на котором представлены красивые меню и картинки, а также заверения в исключительной порядочности данного сайта и магазина — не более чем изображение на экране. Такой сайт может сделать любой студент, хостинг сейчас стоит весьма дешево, и, как следствие, сайт — совершенно не показатель. Однако кое-что по сайту определить можно:

1. С помощью сервисов типа http://leader.ru/secure/ несложно определить все данные о домене магазина — в частности, когда он зарегистрирован и на кого. И если домен зарегистрирован недавно на Васю Пупкина или размещается у непонятного малоизвестного хостера где-то за границей, то это повод задуматься.

2. Стоит внимательно присмотреться к сайту — нет ли там ошибок (грамматических ошибок, нерабочих ссылок, разделов со статусами «на реконструкции»). Наличие множества подобных ошибок, равно как, скажем, неработоспособность поиска или половины ссылок вглубь сайта, должно заставить серьезно задуматься.

3. Несложно узнать индекс цитируемости любого ресурса. Например, с помощью Яндекс http://help.yandex.ru/catalogue/?id=1111360 можно определить «цитируемость» любого ресурса, равно как можно поискать ресурс в каталоге поисковика (в случае Яндекса http://help.yandex.ru/catalogue/?id=1111360). Например, магазин Chip-Dip имеет «цитируемость» = 750, магазин «Озон» = 10000, тогда как индекс цитирования поддельного сайта будет около нуля.

3. Проверить сайт магазина по базам фишинговых сайтов (например, Kaspersky Internet Security делает это автоматически, равно как аналогичные антивирусные продукты с функцией «антифишинг» или ее аналогами).

4. Следует «пробить» URL магазина через крупные поисковые машины, в частности: Яндекс, Рамблер, Google. Анализируя результат, несложно сделать выводы о репутации сайта — нередко в первых 3–5 результатах встречается описание проблем с данным магазином или жалобы обманутых клиентов. Причем следует понимать, что отзывы могут быть и фальшивыми — но крайне сложно заполонить весь Интернет фальшивыми отзывами по некоему магазину. Кроме того, многие поисковики (я, например, часто пользуюсь Яндекс-Маркет, но это на любителя) ведут свои рейтинги магазинов, аккумулируя положительные и отрицательные отзывы.

5. Одним из факторов оценки является наличие на сайте множества сторонних баннеров, всевозможной рекламы, кучи кнопок счетчиков и рейтингов — крупные ресурсы таким вещами не занимаются, так как интернет-торговля приносит им доход, несопоставимо больший дохода от подобной рекламы.

## Отзывы о магазине и товаре

Для начала очень важно отметить, что воспринимать всерьез отзывы о самом магазине, качестве его работы и отзывы о товарах на сайте магазина необходимо воспринимать крайне скептически. Это в особенности ярко видно на сайтах, продающих разные медицинские чудо-приборы, которые лечат все болезни, начиная от глистов и вплоть до плоскостопия завихрением искривленных торсионно-хренотронных полей и тому подобными псевдонаучными чудесами — там отзывы охватывают все ходовые заболевания и возрастные категории, и что важно — все восторженно-положительные. Поэтому для получения полной картины о товаре перед его приобретением через Интернет стоит не полениться и изучить отзывы по нему на различных форумах и сайтах. Посетить сайт производителя и помнить, что он тоже может быть лохотроном, или, что лучше, поискать реального человека среди знакомых, разбирающегося в искомой категории товаров или имеющего такой товар. Кроме того, нередко можно встретить обзоры товара (и помнить при этом, что обзоры бывают заказными). И обязательно стоит помнить, что приврать (или случайно умолчать о каких-либо ограничениях или особенностях товара) любят все, так как задача любого магазина — продать.

## Наличие офиса, торговых площадей и региональных представительств

Самое главное в фирме — это офис. С нормальным юридическим адресом (причем которым не является квартира!), телефоном, факсом, банковскими реквизитами. Причем это совершенно однозначный критерий — у любой реальной фирмы они есть, и эту информацию реальная фирма не скрывает. И наоборот — если офиса нет, и предлагается связь по ICQ, почте или скайпу (т. е. нет даже телефонов) — то это крайне настораживающий фактор. Еще более настораживающим является использование в качестве контактов магазина почтовых адресов на бесплатных сервисах типа mail.ru. Один мой знакомый, связанный по долгу работы с закупкой разной комплектации, иной раз экзотической, выработал интересную стратегию — он сначала пытается дозвониться до менеджера интернет-магазина и уточнить у него что-либо (причем неважно, что именно). Если это не удается (нет контактов, хронически не отвечают телефоны, или отвечает и там сидит «девочка-попугай» с ответом на все вопросы: «Смотрите на сайте, там все есть, ничего больше не скажу») — интернет-магазин снимается с рассмотрения как неблагонадежный. Если связь есть — то далее идет второй вопрос: «А к вам можно подъехать?» (причина любая: оплатить товар по месту, уточнить что-то из его характеристик, подписать договор). И тут нередко выясняется, что ему отвечает работающий по найму оператор, который не знает координат офиса и иной раз, нередко, не видел в глаза своего работодателя. Это второй настораживающий фактор (причем у лохотронщиков есть на это готовый сценарий — «приезжайте, конечно, наш офис в д. Малое Гадюкино, 150 км вертолетом на северо-запад от Нижнего Тагила» — т. е. расчет идет на то, что никто и никогда туда не поедет).

Итак, общий вывод: перед покупкой любого товара в интернет-магазине однозначно стоит узнать, **есть ли у магазина реальный офис**, и существует ли он в природе (так как липовый адрес на сайте указать несложно). Еще лучше, если кроме интернет-магазина у фирмы-продавца есть реальные торговые площади, так как их наличие и факт существования несложно проверить, и это очень хороший показатель благосостояния фирмы (реальные характерные примеры — сеть магазинов «Чип-Дип» или, к примеру, «Никс» и «Ф-Центр»).

## Методика оплаты и доставки

Данный вопрос является одним из самых важных — так как мошенничество начинается именно на стадии цепочки «деньги» — «товар» — «деньги+». На этом этапе как минимум необходимо проанализировать два момента:

**1. Как производится оплата?** Если есть варианты оплаты через банк и даны реквизиты, или с помощью электронных платежных средств через уважаемого посредника типа Assist — то это одно дело. Если речь идет о прямом зачислении денег на некий кошелек типа Yandex, WebMoney и т. п., то это крайне подозрительно, если никакого другого пути оплаты нет, а купить уж очень хочется, то по меньшей мере можно проверить аттестат кошелька получателя и посмотреть, нет ли по данному кошельку жалоб в арбитраж, но, повторюсь, прямой перевод является аналогом отправки письма «на деревню дедушке» — его можно использовать только в полной уверенности в надежности магазина. Причина проста — если после банковского перевода остается хотя бы подтверждение платежа (это не панацея — но хоть что-то), прямой же перевод можно считать подаренными деньгами (конечно, можно потом жаловаться в арбитраж соответствующей платежной системы и т. п.). Еще интереснее ситуация, если на сайте магазина просят ввести номер и код подтверждения кредитной карточки — это должен быть или невероятно уважаемый и давно существующий магазин (а соединение с ним должно идти по SSL-протоколу), или оттуда нужно бежать. Дело в том, что предоставляя номер своей кредитной карты и код подтверждения (цифры на обратной стороне) покупатель, по сути, дает возможность списать любую сумму денег с его карты!

**2. Может ли интернет-магазин работать с юридическим лицом** (т. е. выставить счет, принять деньги безналом и выдать комплект документов с подписями и печатями)? Если может — это отлично, а вот если не может — то это подозрительно. Дело в том, что для выдачи необходимого комплекта бумаг и получения безналичных платежей необходимо зарегистрировать фирму, иметь счет в банке, печать — это слишком сложно и накладно для лохотронщиков.

Еще один момент — это **предоплата**. Момент самый интересный — так как, внося предоплату, покупатель, по сути, передает деньги «под честное слово». Если магазин предлагает несколько видов (оплата и получение товара в офисе в случае самовывоза, оплата курьеру, оплата при получении наложенным платежём, полная пред-

оплата перед отправкой курьерской компанией и т. п.) — то это нормальная практика. Если предлагается только один метод, в особенности с полной предоплатой — то это очень подозрительно.

## Наложенный платёж — что он гарантирует?

Отдельно можно сказать про отправку наложенным платежом — с одной стороны, визуально это гарантия того, что деньги не похитят мошенники и что оплата будет произведена на почте при получении товара. Это, естественно, не так (но это мало кому известно) — и этим пользуются мошенники: в случае наложенного платежа оплачивается не товар, а полученная посылка! И это, по сути, оплата кота в мешке, с последующей возможностью вскрыть его в присутствии почтовых работников для сверки содержимого посылки с описью. При этом есть интересная особенность — если в описи написано «телефон мобильный — 1 шт.», то совершенно любой лежащий в посылке мобильник таковым и будет считаться — и бесполезно доказывать на почте, что где-то на сайте был заказан другой телефон, другой модели и т. п. Аналогично в случае, если присланный товар бракованный или нерабочий — почта не уполномочена вести техническую экспертизу и проверять исправность товара, его качество и его комплектность... — цитата с сайта почты: «Почтовые отправления с наложенным платежом выдаются адресатам после получения полной суммы наложенного платежа, и только потом клиент может проверить наличие пересылаемого вложения (но не качество)». Наиболее показательным моментом является то, что заказав, к примеру, мобильник, получив посылку с правильной стоимостью и оплатив ее на почте можно вскрыть посылку и обнаружить там опись вида «Свисток для отпугивания акул — 1 шт.» — и, собственно, сам свисток. Доказывать сотрудникам почты тот факт, что на сайте заказывался мобильник, а не свисток, а также то, что акулы не боятся свиста и т. п., — совершенно бесполезно, так как почта проверяет именно факт наличия того, что указано в описи — и никаких более претензий не принимает! Это необходимо четко представлять, делая заказ с оплатной наложенным платежом в малоизвестном и сомнительном интернет-магазине (особенно видя раз десять на сайте уверения в том, что совершенно никакого риска, так как оплата только при получении и т. п.).

## Цена

Как известно, вся торговля работает по алгоритму «деньги — товар — деньги+», т. е., покупая что-то дешево, продавец накручивает некий «коэффициент жадности» и продает товар, получая прибыль за счет разницы в цене. Следовательно, если предлагается купить товар по цене, значительно меньшей его средней цены (а среднюю цену несложно узнать в Интернете), то где-то есть обязательно подвох — не может же продавец работать себе в убыток!

## Законность сделки

Законность — это немаловажный момент, нередко применяемый мошенниками. Предлагая всевозможный «таможенный конфискат», «прошедший в обход таможни товар» и т. п., они создают правдоподобное объяснение низкой заманчивой цене и барьер на пути пострадавшего в милицию — совершая сомнительную сделку, пострадавший оказывается в интересной ситуации — не идти же ему в полицию с заявлением типа «Я купил ворованный телефон, ввезенный в обход таможни, а мне вместо него прислали свисток от акул».

## Гарантия и правила возврата товара

Гарантия и правила возврата — одна из важнейших составляющих торговли, в особенности удаленной. Дело в том, что:

1. Даже самый уважаемый и надежный магазин может прислать пересортицу (т. е. отличный от заказанного товар) или что-то нечаянно не прислать (или прислать лишнее). Делается это обычно без злого умысла, по причине компьютерных сбоев или элементарной халатности комплектующего заказ персонала.

2. Присланный товар может оказаться неисправным или (и это самое сложное и туманное) не отвечающим ожидаемым и заявленным на сайте характеристикам.

3. Товар может оказаться бракованным или сломаться в ходе эксплуатации.

В подобных ситуациях понадобится выполнение операции возврата товара для замены, возврата денег или гарантийного ремонта. У честных магазинов на этот случай детально описана процедура возврата товара, процедура его экспертизы и замены, имеются образы заявлений, расписана процедура отправки товара для обмена и ремонта, с товаром соответственно поставляются гарантийные талоны

и иные документы, указывающие на комплектность заказа. В случае лохотрона все это или не описано вообще, или открыто говорится что-то вроде того, что «мы торгуем таможенным конфискатом, дешево, без обмена и гарантии» — в таком случае связываться с подобным «магазином» неразумно.

## Общие выводы

Итак, резюмируя все вышесказанное, можно сформулировать ряд советов и конкретных рекомендаций.

1. Перед покупкой стоит потратить 15 минут и заняться небольшим детективным расследованием — выяснить, как давно существует магазин, есть ли у него офис и реальные контактные данные, какие отзывы у магазина существуют в Интернете. Если магазин принимает деньги через электронные платежные системы типа WebMoney — обязательно проверить, есть ли отрицательные данные в арбитраже платежных систем, и что дает поиск по номеру кошельков (нередко сразу находятся отзывы типа «Отправил деньги на кошелек xxx, и меня кинули»). Важно отметить, что нет единого показателя.

2. Никогда не вводите на сайте магазина параметры своей кредитной карточки. Исключением может быть или очень хорошо известный и давно существующий интернет-магазин, или оплата через посредника типа Assist (при этом необходимо обязательно убедиться, что обмен идет по защищенному протоколу SSL, и номер кредитной карточки передается именно системе Assist, а не фишинговому ресурсу).

3. Внося предоплату, следует четко понимать, что деньги переводятся «под честное слово» (причина проста — нет подписанного двухстороннего договора между продавцом и покупателем). При этом наиболее опасны прямые переводы с кошелька на кошелек. Если в случае крупного и уважаемого магазина риск невелик (так как обманывать покупателя владельцам магазина нет резона — репутация дороже).

4. Если оплата ведется путем расчета кредитной картой — стоит завести отдельную кредитную карту специально для покупок через Интернет и не держать на ней значительных сумм денег. В такой ситуации риск потерять деньги в результате кражи параметров кредитной карты минимален.

5. Следует помнить, что отправка товаров наложенным платежом является гарантией получения посылки, но не гарантией получе-

ния заказанных товаров надлежащего качества (что, естественно, не исключает факт мошенничества).

6. Следует помнить, что задача любого магазина — продать товар. Поэтому обязательно следует перепроверить все характеристики заказываемого товара, уточнить его среднюю цену и внешний вид из различных источников. Радикальные расхождения в описании товара являются тревожным признаком.

7. Не следует верить отзывам о магазине и товаре на самом сайте магазина. Однозначно следует поискать более или менее независимые отзывы в Интернете и изучить их.

8. Перед заказом следует очень внимательно изучить правила обмена, возврата, гарантийного ремонта товара. Если таковые операции не описаны и (или) не предусматриваются интернет-магазином, то однозначно лучше не рисковать.

9. Работая с малоизвестным магазином, постарайтесь хотя бы найти знакомых, которые уже работали с ним, — и спросите их мнение. Мнение знакомого незаинтересованного человека и его реальный опыт ценнее десятков отзывов в Интернете.

10. Если на сайте интернет-магазина открыто сказано, что товар добыт неким не совсем незаконным путем — остерегайтесь, так как легальный магазин никогда такого не напишет (так как это, по сути, публичная явка с повинной — компетентные органы, естественно, заинтересуются, откуда левый товар и т. п.). Аналогичное можно сказать об аномально низких ценах, радикально отличающихся от рыночных, — в случае легальной торговли подобное невозможно.

# ЛИТЕРАТУРА

1. *Аршинов*, *М. Н.* Коды и математика (рассказы о кодировании) / М. Н. Аршинов, Л. Е. Садовский. — М. : Наука, Главная редакция физико-математической литературы, 1983. — 144 с. — (Библиотечка «Квант», Вып. 30).

2. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

3. *Громов*, *Г. Р.* Национальные информационные ресурсы: проблемы промышленной эксплуатации. — М. : Наука, 1984. — 240 с.

4. *Касперский*, *Е.* Компьютерное зловредство. — СПб. : Питер, 2007. — 202 с.

5. *Колисниченко*, *Д. Н.* Анонимность и безопасность в интернете. От чайника к пользователю. — СПб. : БХВ-Петербург, 2012. — 24 с.

6. *Михайлов*, *А. В.* Компьютерные вирусы и борьба с ними. — М. : ДИАЛОГ-МИФИ, 2012. — 148 с.

7. *Михаэль*, *А. Бэнкс*, Информационная защита ПК. — Киев : ВЕК+ ; М. : Энергия ; СПб. : Корона-Принт, 2001. — 272 с.

8. *Петров*, *А. А.* Компьютерная безопасность. Криптографические методы защиты. — М. : ДМК, 2000. — 448 с.

9. *Стратонович*, *Р. Л.* Теория информации. — М. : Сов. Радио, 1975. — 424 с.

10. *Хэмминг*, *Р. В.* Теория кодирования и теория информации. — М. : Радио и связь, 1983. — 176 с.

11. *Шанкин*, *Г. П.* Ценность информации. Вопросы теории и приложений. — М. : Филоматис, 2004. — 128 с.

### Список интернет-ресурсов, которые использовались в разделах книги

1. http://www.comodo.com/home/internet-security/free-internet-security.php — программа-антивирус Comodo Internet Security.

2. http://z-oleg.com/secur/avz/download.php — программа-антивирус Зайцева (AVZ).

3. http://www.freedrweb.com/cureit — антивирусный сканер от Dr.Web.

4. http://www.pcflank.com/scanner1.htm?from=menu — программа проверки эффективности установленного брандмауэра.

5. http://www.truecrypt.org/ — сайт разработчика программы шифрования TrueCrypt.

6. http://www.truecrypt.org/localizations — русская локализация программы шифрования TrueCrypt.

7. https://www.torproject.org/ — официальный сайт программного обеспечения Tor.

8. https://www.torproject.org/dist/torbrowser/tor-browser-2.2.32-3_ru.exe — прямая ссылка на загрузку последней версии Tor Browser.

9. https://www.torproject.org/download/download.html.ru — два настроенных комплекта программного обеспечения: пакет Tor Browser; пакет Tor Browse Instant Messaging Bundle, который содержит не только браузер, но и клиент мгновенного обмена сообщениями.

10. https://bridges.torproject.org — программа для получения списка мостов для доступа к сети Tor.

11. http://www.pgpi.com — криптографическая (шифровальная) программа PGP.

12. http://www.ritlabs.com/ru/products/thebat/ — почтовый клиент The Bat!.

13. http://help.mail.ru/mail-help/mailer/tb — руководство по настройке The Bat!.

14. http://allbat.info/settings/ — настройка The Bat! для других почтовых сервисов.

15. http://biblprog.org.ua/ru/unlocker/ — программа-разблокировщик.

16. http://genpas.narod.ru/ — генератор паролей.

17. http://keepass.info/download.html — программа хранения паролей KeePassPasswordSafe.

18. http://www.eraser.heidi.ie/ — программа Eraser для удаления данных без возможности восстановления.

19. http://www.microsoft.com/downloads/ru/details.aspx?familyid=9cfb2d51-5ff4-4491-b0e5-b386f32c0992 — платформа NETFramework, необходимая для работы программы Eraser.

**Дополнительно**

1. https://nordrus.info/security/ — руководство по защите информации.

2. http://malpaso.ru/gpg-keysigning-party/ — правила обмена ключами для зашифрованного обмена информацией.

3. https://pgpru.com/ — сайт проекта OpenPGP в России.

4. http://www.antivirus.ru/AvFirm.html — коллекция из нескольких десятков ссылок на сайты производителей антивирусов.

5. http://www.virustotal.com/ — сайт, на котором удобно анализировать подозрительные файлы.

# ОГЛАВЛЕНИЕ

*Сергей Николаевич НИКИФОРОВ*

**МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**
ЗАЩИЩЕННЫЕ СЕТИ

*Учебное пособие*

Издание второе, стереотипное

Зав. редакцией литературы
по информационным технологиям
и системам связи *О. Е. Гайнутдинова*

ЛР № 065466 от 21.10.97
Гигиенический сертификат 78.01.10.953.П.1028
от 14.04.2016 г., выдан ЦГСЭН в СПб

**Издательство «ЛАНЬ»**
lan@lanbook.ru; www.lanbook.com
196105, Санкт-Петербург, пр. Юрия Гагарина, д. 1, лит. А
Тел./факс: (812) 336-25-09, 412-92-72
Бесплатный звонок по России: 8-800-700-40-71

Подписано в печать 19.03.21.
Бумага офсетная. Гарнитура Школьная. Формат 84×108 $^{1}/_{32}$.
Печать офсетная. Усл. п. л. 5,04. Тираж 50 экз.

Заказ № 330-21.

Отпечатано в полном соответствии
с качеством предоставленного оригинал-макета
в АО «Т8 Издательские Технологии».
109316, г. Москва, Волгоградский пр., д. 42, к. 5.