БЮРО
СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ

ОТДЕЛ «К»
(по борьбе с компьютерными преступлениями
и незаконным оборотом РЭС и СТС)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ТИПОВЫЕ АЛГОРИТМЫ ДЕЙСТВИЙ ПРИ ПОЛУЧЕНИИ ИНФОРМАЦИИ
ПО ЭЛЕКТРОННЫМ ИДЕНТИФИКАТОРАМ
В СЕТИ ИНТЕРНЕТ

Получение регистрационных данных по IP-адресу.

Интернет – всемирная система объединённых компьютерных сетей, построенная на базе протокола IP и маршрутизации IP-пакетов. Часто упоминается как «Всемирная сеть» и «Глобальная сеть», в обиходе иногда употребляют сокращённые наименования «инет», «нет».

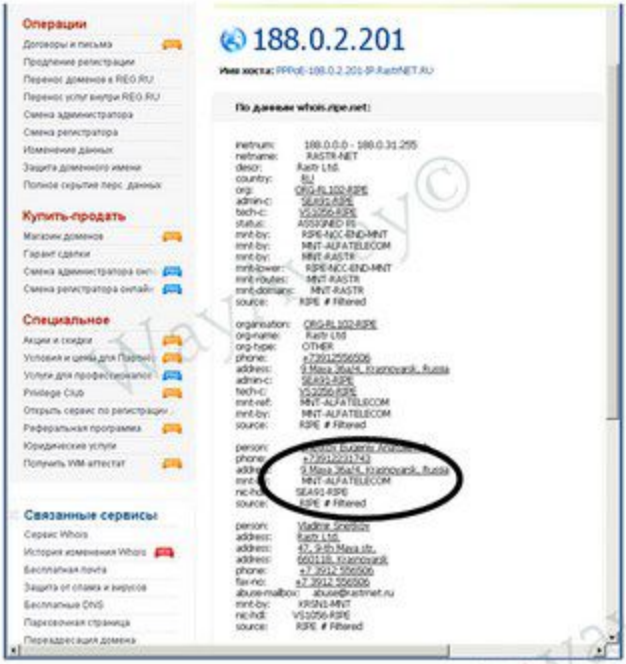
Интернет-провайдер (иногда просто провайдер) — организация (оператор связи), предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги.

IP-адрес (айпи-адрес, сокр. от англ. Internet Protocol Address) — уникальный сетевой адрес компьютера в сети, построенной по протоколу IP. Удобной формой записи IP-адреса (протокол IPv4) является запись в виде четырёх десятичных чисел значением от 0 до 255, разделённых точками, например, 192.168.0.1.

Порядок действий:

1. Используя глобальный справочный интернет-сервис WHOIS, предоставляющий информацию о регистрационных данных владельцев IP-адресов и доменных имен, устанавливаем оператора связи, которому принадлежит интересующий IP-адрес.

Пример: Используя сервис WHOIS по адресу http://reg.ru/whois устанавливаем оператора связи, которому принадлежит интересующий IP-адрес 188.0.2.201:



Примечание: С использованием глобальных сервисов WHOIS не может быть получена информация для следующих диапазонов IP-адресов:

10.0.0.1 – 10.255.255.254,
127.0.0.1 – 127.255.255.254,
169.254.0.1 – 169.254.255.254,
172.16.0.1 – 172.31.255.254,
192.168.0.1 – 192.168.255.254.

Указанные диапазоны IP-адресов используются для адресации внутри локальных и частных сетей передачи данных, так называемые «серые» IP-адреса. Подключение указанных IP-адресов к сети интернет осуществляется с использованием общего NAT-сервера. В результате, всем подключенным в сети Интернет абонентам назначается один внешний IP-адрес NAT-сервера. Как правило, с использованием одного IP-адреса к сети Интернет одновременно могут быть подключено несколько тысяч абонентов.

Примечание: Для установления в пределах г. Красноярска принадлежности IP-адресов из диапазона 172.16.0.1 – 172.31.255.254 необходимо воспользоваться сервисом WHOIS красноярской городской пиринговой сети, расположенным по сетевому адресу http://www.krs-ix.ru/tools/whois/.

2. Направить запрос установленному оператору о предоставлении регистрационных данных абонента. Предварительно, у оператора желательно узнать, является ли интересующий IP-адрес динамическим или статическим, а также выделен ли он NAT-серверу или конечному абоненту.

Типовыми запросами для получения регистрационных данных являются запросы к оператору связи, сетевому адресному пространству которого принадлежат интересующие IP-адреса.

Примечание: Для установления в пределах г. Красноярска принадлежности IP-адресов из диапазона 172.16.0.1 – 172.31.255.254 необходимо воспользоваться сервисом WHOIS красноярской городской пиринговой сети, расположенным по сетевому адресу http://www.krs-ix.ru/tools/whois/.

2. Направить запрос установленному оператору о предоставлении регистрационных данных абонента. Предварительно, у оператора желательно узнать, является ли интересующий IP-адрес динамическим или статическим, а также выделен ли он NAT-серверу или конечному абоненту.

Типовыми запросами для получения регистрационных данных являются запросы к оператору связи, сетевому адресному пространству которого принадлежат интересующие IP-адреса.

Пример: Запрос регистрационных данных динамического «белого» IP-адреса:

> … прошу предоставить регистрационные данные абонента, которому был выделен IP-адрес … (*например, 87.23.123.32*) в следующие периоды времени …

Пример: Запрос регистрационных данных статического «белого» IP-адреса:

> … прошу предоставить регистрационные данные абонента, которому выделен IP-адрес … (*например, 87.23.123.32*) …

Пример: Запрос регистрационных данных «серого» IP-адреса при наличии IP-адреса NAT-сервера, через который он подключен:

… прошу предоставить регистрационные данные абонента и информацию о соединениях *(если требуется)*, который посредством IP-адреса … (*указывается IP-адрес NAT-сервера, например, 87.23.123.32*) осуществлял соединения с интернет-ресурсами* … (*например, mail.ru или 94.100.191.205*) в следующие периоды времени … (*желательно указать несколько периодов*)

* *Необходимо указывать названия (или IP-адреса) конкретных интернет-ресурсов, к которым интересующий абонент мог подключаться, так как в один и тот же период времени одновременно через NAT-сервер могут быть подключено до нескольких тысяч абонентов.*

Примечание: Для получения информации о соединениях некоторым операторам связи требуется предоставить постановление суда.

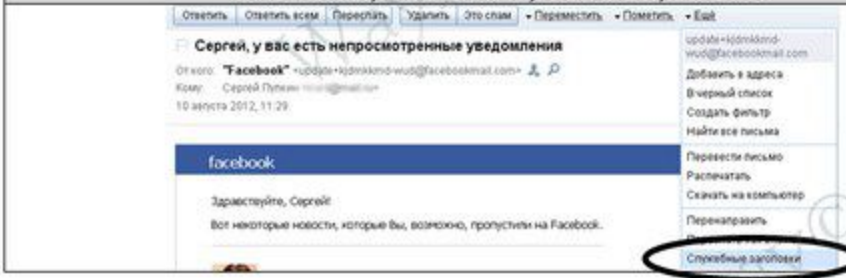
Установление отправителя электронного письма.

Каждое электронное письмо содержит информацию о маршруте следования в процессе отправки-получения (RFC-заголовок, свойства письма). При этом, как правило, по умолчанию данная информация, получателю не отображается. Анализ информации о движении электронного письма позволит получить сведения об IP-адресе ЭВМ, с которого письмо было отправлено и реальный электронный почтовый ящик. В ряде случаев при получении письма в поле «От кого» может быть указан произвольный, в том числе не принадлежащий злоумышленнику электронный почтовый ящик.

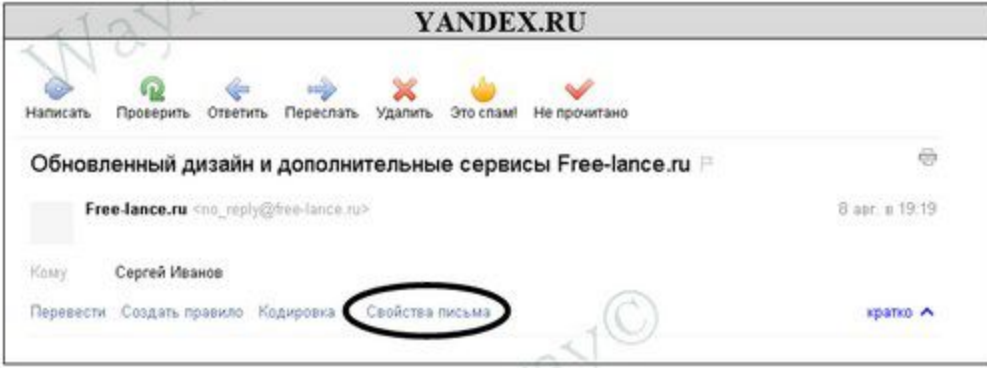
Порядок действий:

1. Установить IP-адрес, с которого было отправлено письмо. В зависимости от используемой программы-почтового клиента ознакомиться со свойствами электронного письма можно следующим образом: необходимо открыть электронное письмо и в командной панели выбрать команду отображения свойств письма. Ниже указано расположение пунктов меню для некоторых почтовых клиентов:

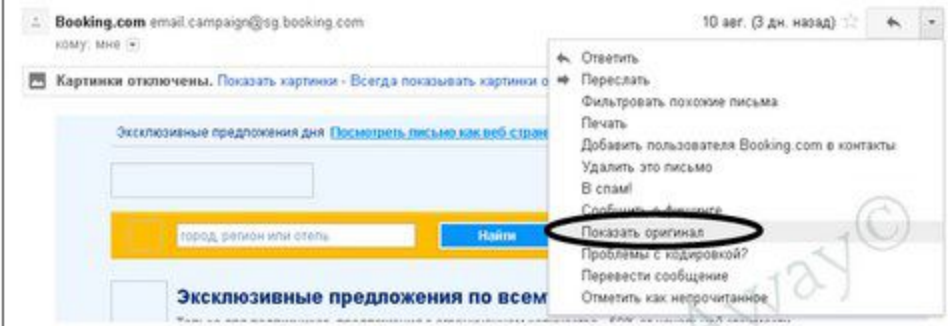
MAIL.RU, INBOX.RU, LIST.RU, BK.RU



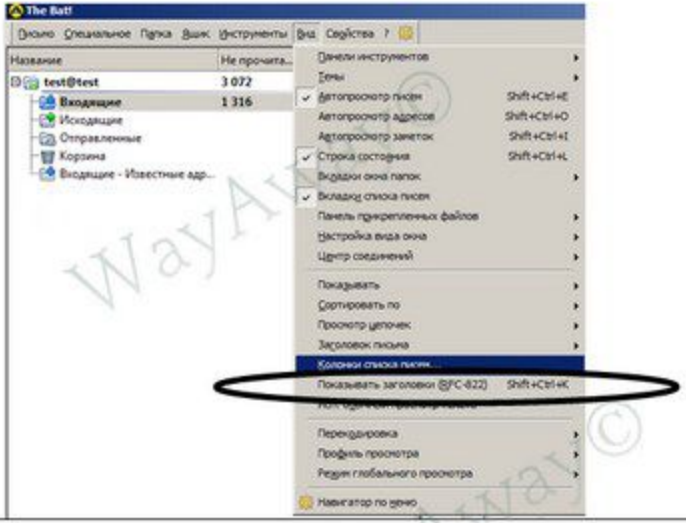
YANDEX.RU



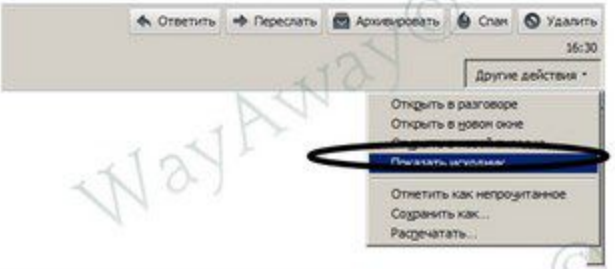
GMAIL.COM



THE BAT



MOZILLA THUNDERBIRD



В результате, отобразится текст, примерно, следующего содержания:

```
From ivanova@mail.ru Mon Nov 21 08:14:29 2011
Return-path: <ivanova@mail.ru>
Received: from mail by f287.mail.ru with local
        id 1RSLH3-00052b-00
        for petrov@mail.ru; Mon, 21 Nov 2011 08:14:29 +0400
Received: from [213.87.121.85] by e.mail.ru with HTTP;
        Mon, 21 Nov 2011 08:14:29 +0400
From:=?UTF-8?B?0J7Qu9C10YHRjyDQktC70LDQtNC40LzQuNGA0L7QstC90LAg0KjQuNC90Lo=?=
 =?UTF-8?B?0LXQstC40Yc=?= <ivanova@mail.ru>
To: =?UTF-8?B?0JLQtFddhCIC0=?= <petrov@mail.ru>
Subject: =?UTF-8?B?UmU6IHlvdXIgbWFpbA==?=
Mime-Version: 1.0
X-Mailer: mPOP Web-Mail 2.19
X-Originating-IP: [213.87.121.85]
Date: Mon, 21 Nov 2011 08:14:29 +0400
References: <E1RSKyW-0002fF-00.petrov-mail-ru@f57.mail.ru>
In-Reply-To: <E1RSKyW-0002fF-00.petrov-mail-ru@f57.mail.ru>
Reply-To:=?UTF-8?B?0J7Qu9C10YHRjyDQktC70LDQtNC40LzQuNGA0L7QstC90LAg0KjQuNC90Lo=?=
 =?UTF-8?B?0LXQstC40Yc=?= <ivanova@mail.ru>
X-Priority:
Content-Type: multipart/alternative;
        boundary="--ALT--YTDCOxOX1321848869"
Message-Id: <E1RSLH3-00052b-00.ivanova-mail-ru@f287.mail.ru>
X-Spam: Not detected
X-Mras: Ok
```

Как правило, IP-адрес отправителя содержится в полях «X-Originating-IP» или «Received: from» (см. рисунок выше). Необходимо определить первый снизу IP-адрес (самый последний в тексте, наиболее ранний по сопутствующему времени, с учетом часового пояса). Дата и время отправления письма указаны в поле «Date» или «Received: from», значение +0400 указывает, на часовой пояс относительно нулевого меридиана (в данном примере +0400 – указывает на московский часовой пояс).

Если полученный IP-адрес принадлежит диапазонам:

10.0.0.1 – 10.255.255.254,

127.0.0.1 – 127.255.255.254,

169.254.0.1 – 169.254.255.254,

172.16.0.1 – 172.31.255.254,

192.168.0.1 – 192.168.255.254,

то необходимо выбрать следующий находящийся выше IP-адрес, а полученный использовать для идентификации абонента во внутренней сети установленного интернет-провайдера.

2. Получить регистрационные данные и информацию о соединениях по установленному IP-адресу (описано выше).

Установление владельца электронного почтового ящика (e-mail)

Название электронного почтового ящика (ЭПЯ) имеет вид zzz@yyy.ru, где zzz – имя пользователя (логина), yyy – адрес сервиса электронной почты (*например, mail.ru*).

Порядок действий:

1. Установить принадлежность электронного почтового ящика к сервису электронной почты.

Наиболее популярные сервисы электронной почты:

E-mail	Компания	Адрес, телефон
@mail.ru, @inbox.ru, @list.ru, @bk.ru	ООО «Мэйл.Ру»	125167, Россия, Москва, Ленинградский проспект, д. 47, стр. 2, БЦ «Авион», 5 этаж
@yandex.ru	ООО «Яндекс»	119021, Москва, ул. Льва Толстого, 16, тел: +7 495 739-70-00
@rambler.ru, @lenta.ru, @myrambler.ru, @autorambler.ru, @ro.ru, @r0.ru	ООО «Рамблер Интернет Холдинг»	115280, Москва, Ленинская слобода, д. 19, тел: +7 (495) 785-17-00
@qip.ru, @pochta.ru, @fromru.com, @front.ru, @hotbox.ru, @Hotmail.ru, @krovatka.su, @land.ru, @mail15.com, @mail333c.com, @newmail.ru, @nightmail.ru,	ООО «Медиа Мир»	117485, Москва, Профсоюзная 84/32, тел: +7 (495) 363-11-11
@5ballov.ru, @aeterna.ru, @ziza.ru, @memori.ru, @photofile.ru, @fotoplenka.ru, @pochta.com, @nm.ru		

Примечание: Электронные почтовые ящики вида @gmail.com (@google.com), @hotmail.com, @yahoo.com принадлежат сервисам электронной почты, находящимся в США.

2. Направить запрос о предоставлении регистрационных данных и активности электронного почтового ящика.

Перед направлением запроса необходимо проверить существование такого ЭПЯ. Для этого необходимо попытаться зарегистрировать ящик, указав в соответствующем поле интересующий адрес, если он будет занят, то ЭПЯ существует.

Пример: Запрос регистрационных данных владельца электронного почтового ящика:

> …прошу предоставить регистрационные данные, IP-адреса авторизации, абонентский номер активации и восстановления пароля владельца электронного почтового ящика...

В полученном ответе будет информация об IP-адресах, с которых владелец управлял ЭПЯ.

3. Направить необходимые запросы для получения информации по IP-адресу.

Установление владельца интернет-сайта

Интернет-сайт / Веб-сайт (от англ. website: web — «паутина, сеть» и site — «место», буквально «место, сегмент, часть в сети») — совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединённых под одним адресом (доменным именем или IP-адресом).

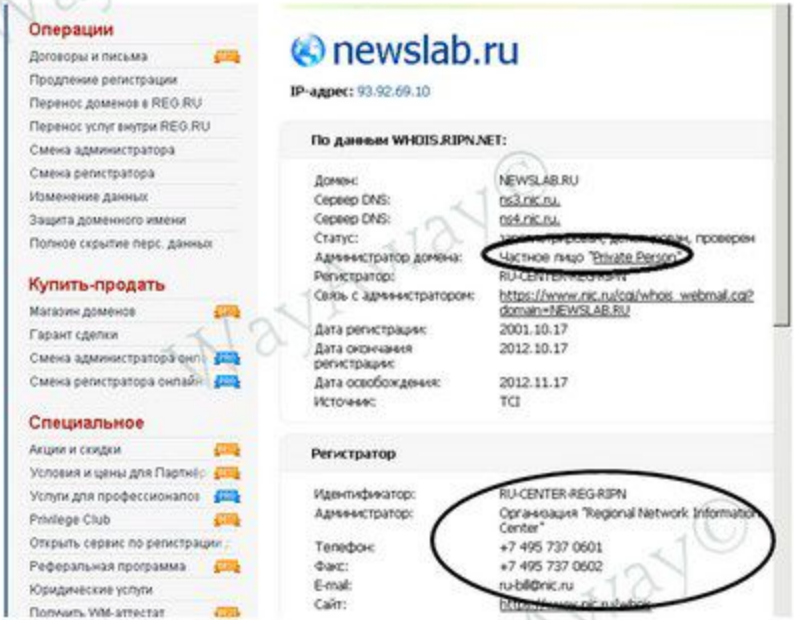
Доменное имя — символьное имя, служащее для идентификации сетевых-ресурсов. Доменные имена дают возможность адресации компьютеров и расположенных на них сетевых ресурсов (веб-сайтов, серверов электронной почты, других служб) в удобной для человека форме.

Хостинг-провайдер — компания, занимающаяся предоставлением услуг по размещению интернет-сайтов на своих технических площадках.

Порядок действий:

1. Используя глобальный справочный интернет-сервис WHOIS, предоставляющий информацию о регистрационных данных владельцев IP-адресов и доменных имен, получаем открытую информацию о регистранте доменного имени и организации, на ресурсах которой размещается интернет-сайт с интересующим доменным именем.

Пример: Используя сервис WHOIS по адресу http://reg.ru/whois устанавливаем оператора связи, которому принадлежит интересующий интернет-сайт newslab.ru:



Если в качестве владельца сайта указано Private Person (частное лицо), то необходимо направить запрос в компанию регистратор домена (в нашем примере – «Regional Network Information Center», сайт, где можно узнать справочную информацию – NIC.RU).

В большинстве случаев регистрационные данные, которые предоставляет владелец домена, администрацией не проверяются и могут не соответствовать действительности. Кроме того, сервисом whois предоставляется информация только для доменов второго уровня - вида xxx.ru (*например, newslab.ru*), информацию для доменов вида yyy.xxx.ru (*например, crime.newslab.ru*) необходимо получать у владельцев домена второго уровня.

2. В полученной информации в поле nserver указан владелец хостинга (технической площадки) сайта (*в данном случае компания «Regional Network Information Center»*), который может предоставить регистрационные данные. (могут быть недостоверными), а также, ip-адреса авторизации, контактные данные, платежные реквизиты, которые являются достоверными.

Пример: Запрос регистрационных данных владельца доменного имени или сайта:

> … прошу предоставить регистрационные данные владельца доменного имени (сайта), а также предоставить информацию об IP-адресах и времени его авторизации (с указанием часового пояса), контактные данные (телефон, e-mail), номера электронных кошельков, с которых производилась оплата услуг. …

3. Направить необходимые запросы для получения информации по IP-адресу и электронной почте.

Установление пользователя социальной сети

Социальная сеть – интернет-портал, предназначенный для общения пользователей, создания групп по интересам, обмена музыкой и фотографиями. Пользователи, как правило, идентифицируются либо по уникальным номерам (ID), либо по электронным почтовым ящикам.

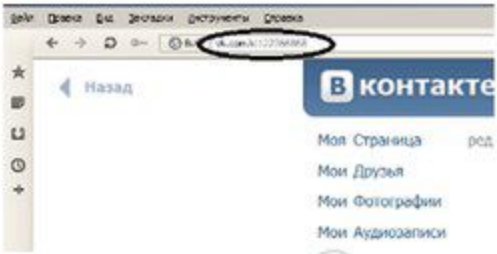
Порядок действий:

1. Определить уникальный идентификатор анкеты пользователя в социальной сети.

Ниже приведены примеры получения информации в наиболее популярных социальных сетях:

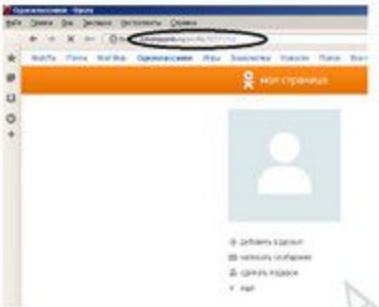
«В Контакте»

Идентификатор указан в адресной строке браузера после текста «vk.com/». Может состоять как из последовательности цифр, так и латинских букв:



«Одноклассники»

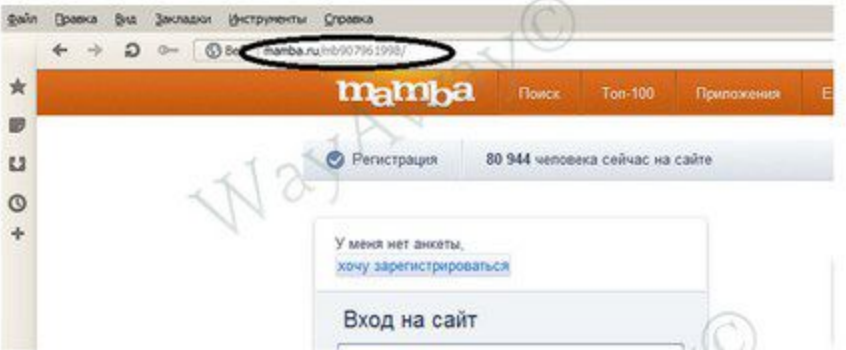
Идентификатор указан в адресной строке браузера после текста «odnoklassniki.ru/profile/»



Нажмите на это изображение для просмотра полноразмерной версии.

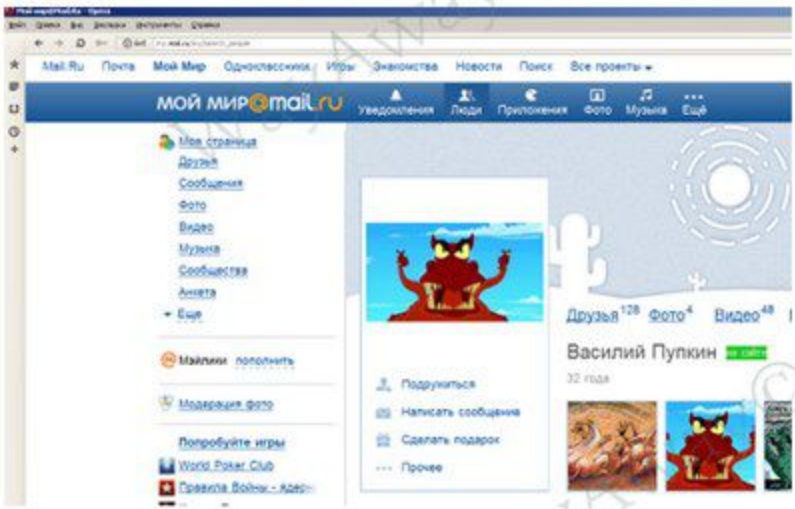
«Мамба»

Идентификатор указан адресной строке браузера после текста «mamba.ru»:



В нижней части страницы указан ID анкеты:

«Мой мир»



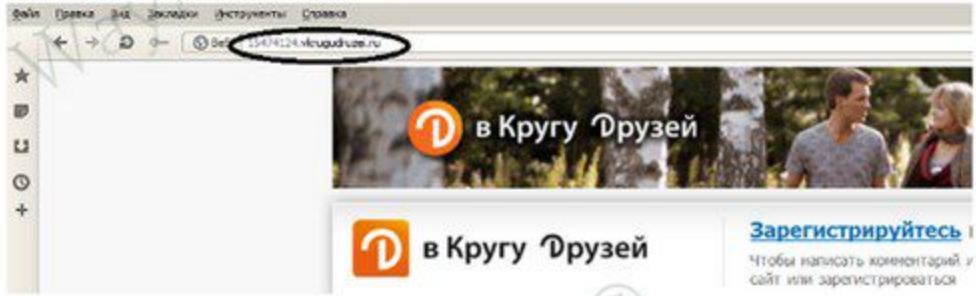
Под фотографией пользователя навести курсор на пункт меню «Сделать подарок», нажать правую кнопку мыши, выбрать пункт «Скопировать адрес ссылки/Копировать адрес ссылки», вставить в текстовый документ.

В интернет браузере Internet Explorer ссылка отображается в левом нижнем углу при наведении курсора на «Сделать подарок»

В полученной строке вида *http://my.mail.ru/my/gifts?send=* ***vasil12345678@mail.ru,*** идентификатором является электронный почтовый ящик указанный после send=.

«В кругу друзей»

Идентификатор указан в адресной строке браузера перед текстом «.vkrugudruzei.ru»



«Loveplanet»

Идентификатор указан в адресной строке браузера после текста «loveplanet.ru/page/», может быть как в виде последовательности цифр, так и состоять из латинских букв.

2. Направить запрос в организацию, владеющей указанной социальной сетью.

Пример: Запрос регистрационных данных владельца анкеты (профиля):

… прошу предоставить регистрационные данные, информацию об IP-адресах и времени авторизации (с указанием часового пояса), контактные данные (телефон, e-mail), номера электронных кошельков, с которых производилась оплата услуг, владельца профиля №…

Адреса для направления запросов:

Соц. сеть	Организация	Адрес
Mail.ru (Мой мир)	ООО «Мэйл.ру»	Ленинградский проспект, д. 47, стр.2, г. Москва, 125167
Odnoklassniki.ru	ООО «Одноклассники	Ленинградский проспект, д. 47, стр. 2, БЦ «Авион», 5 этаж, г. Москва,125167
Vkontakte.ru (vk.com)	ООО «В контакте»	195015 г. Санкт-Петербург, ул. Тверская 8лит. Б
Mamba.ru	ЗАО «Мамба»	ул. 2я Звенигородская, д. 13, стр. 42, г. Москва, 123022
vkrugudruzei.ru	ООО «КМ онлайн»	127549, г. Москва, ул. Пришвина, д.8, корп.1
Loveplanet.ru	Группа компаний «РосБизнесКонсалтинг»	117393, г. Москва, ул. Профсоюзная, д. 78, стр.1

В полученном ответе, как правило, содержится информация об IP-адресах, с которых происходило управление анкетой, достоверные номер телефона и электронный почтовый ящик.

3. Направить необходимые запросы для получения информации по IP-адресу и электронной почте.

Примечание: Социальные сети facebook.com, twitter.com, livejournal.com, blogspot.com принадлежат компаниям, находящимся за пределами Российской Федерации.

Установление владельца электронного кошелька (счета)

Электронный кошелек (счет) – в данном случае, интернет-сервис, предназначенный для пополнения, хранения и перечисления электронных денег, которыми можно оплачивать различные услуги и обменивать их на реальные деньги.

Порядок действий:

1. Определить уникальный идентификатор кошелька (счета) в электронной платежной системе и направить соответствующий запрос.

Ниже приведены примеры получения информации в наиболее популярных платежных системах:

«WebMoney»

Электронные кошельки платежной системы ООО «ВебМани.Ру» «WebMoney» имеют вид R141501221907 (где R-рубли, Z-доллары США, U-украинские гривны). Уникальный номер пользователя имеет вид WMID 125292778908. Одному пользователю может принадлежать несколько кошельков. Так как номер кошелька и номер пользователя содержат по 12 цифр, то необходимо правильно указывать в запросе тип запрашиваемой информации.

Образец запроса по WMID:

Образец запроса по WMID:

… прошу вас предоставить:

1. Регистрационные данные участника, зарегистрировавшего в системе «Webmoney transfer» WMID ……;
2. Информацию о всех кошельках, зарегистрированных вышеуказанным участником и историю операций по ним за весь имеющийся период с указанием IP-адресов, с которых происходила авторизация участника;
3. В случае перечисления средств с кошельков, зарегистрированных данным участником, другим участникам Вашей системы, за исключением сервисов обмена электронных денег, прошу предоставить по этим кошелькам аналогичную информацию…

Образец запроса по номеру кошелька R, Z, U:

… прошу Вас предоставить:

1. Регистрационные данные и WMID владельца кошелька R…
2. Информацию о всех кошельках, зарегистрированных вышеуказанным участником и историю операций по ним за весь имеющийся период с указанием IP-адресов, с которых происходила авторизация участника;
3. В случае перечисления средств с кошельков, зарегистрированных данным участником, другим участникам Вашей системы, за исключением сервисов обмена электронных денег, прошу предоставить по этим кошелькам аналогичную информацию…