

Михаил Райтман

**ИСКУССТВО  
ЛЕГАЛЬНОГО, АНОНИМНОГО  
И БЕЗОПАСНОГО ДОСТУПА  
К РЕСУРСАМ ИНТЕРНЕТА**



**Михаил Райтман**



**ИСКУССТВО  
ЛЕГАЛЬНОГО, АНОНИМНОГО  
И БЕЗОПАСНОГО ДОСТУПА  
К РЕСУРСАМ ИНТЕРНЕТА**

Санкт-Петербург  
«БХВ-Петербург»

2017

УДК 004.738.5  
ББК 32.973.26-018.2  
P12

**Райтман М. А.**

P12 Искусство легального, анонимного и безопасного доступа к ресурсам  
Интернета. — СПб.: БХВ-Петербург, 2017. — 624 с.: ил.

ISBN 978-5-9775-3745-2

Описан ряд приемов защиты персональных данных с помощью шифрования, паролей, многофакторной аутентификации, приватного обмена, бесследного удаления информации и других доступных обычному пользователю средств. Приведены способы конспиративного общения по защищенным каналам связи и подключения к анонимным сетям, таким как Tor, I2P RetroShare и др. Описаны способы получения инвайтов в закрытые сообщества, такие как What.cd, и доступа к таким ресурсам, как Pandora и Hulu. Представлено подробное руководство по операционной системе Tails, обеспечивающей максимальный уровень анонимизации и безопасности. В качестве приложения приведен экскурс в Даркнет — теневую сторону Интернета, а также сведения о «варезной» сцене и демосцене, разновидности компьютерного искусства. Краткий глоссарий в конце книги поможет разобраться в специфических терминах.

*Для широкого круга читателей*

УДК 004.738.5  
ББК 32.973.26-018.2

#### Группа подготовки издания:

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Екатерина Капалыгина</i>
Редактор	<i>Григорий Добин</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн обложки	<i>Марины Дамбиевой</i>

Подписано в печать 30.09.16.  
Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 50,31.  
Тираж 1200 экз. Заказ № 1541.  
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.  
Первая Академическая типография "Наука"  
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3745-2

© Райтман М. А., 2017  
© Оформление, издательство "БХВ-Петербург", 2017

# Оглавление

<b>ПРЕДИСЛОВИЕ. Добро пожаловать, мистер Андерсон</b> .....	<b>1</b>
<b>ЧАСТЬ I. ПОДГОТОВКА К АНОНИМНОЙ РАБОТЕ, РЕШЕНИЕ ВОПРОСОВ БЕЗОПАСНОСТИ</b> .....	<b>5</b>
<b>Глава 1. Защита персональных данных</b> .....	<b>7</b>
Обеспечение безопасности данных, хранимых на устройстве .....	8
Шифрование данных в операционной системе Windows.....	9
Установка DiskCryptor.....	10
Использование DiskCryptor для шифрования всего компьютера .....	10
Шифрование данных в операционной системе OS X.....	11
Шифрование данных в операционной системе iOS.....	14
Защита портативных носителей данных.....	16
Безопасность при использовании сетей Wi-Fi .....	17
Угрозы, возникающие при подключении к открытой сети Wi-Fi .....	17
Защита собственной сети Wi-Fi.....	20
Еще о защите персональных данных .....	24
Безопасный веб-серфинг .....	26
Приватные режимы браузеров.....	26
Использование протокола HTTPS.....	31
Расширение HTTPS Everywhere .....	31
Удаление истории посещений и cookie-файлов .....	32
Браузер Internet Explorer.....	32
Браузер Microsoft Edge .....	34
Браузер Mozilla Firefox.....	35
Браузер Opera .....	37
Браузер Google Chrome .....	38
Браузер Safari .....	40
Мобильные браузеры .....	41
<b>Глава 2. Надежные пароли и двухфакторная авторизация</b> .....	<b>43</b>
Выбор надежных паролей.....	44
О «секретных вопросах» .....	44

Менеджеры паролей .....	44
Использование мастер-пароля .....	45
Использование файла-ключа .....	46
Комбинация мастер-пароля и файла-ключа .....	46
Синхронизация паролей между несколькими устройствами .....	46
Менеджер паролей KeePassX .....	47
Добавление паролей .....	48
Использование паролей .....	49
Дополнительные функции .....	50
Многофакторная аутентификация и одноразовые пароли .....	51
Создание второстепенных аккаунтов .....	53
<b>Глава 3. Фишинговые атаки .....</b>	<b>54</b>
Признаки фишинговой атаки .....	54
Защита от фишинговых атак .....	62
Проверка писем через отправителей .....	62
Использование облачных хранилищ и файловых хостингов .....	62
Безопасный просмотр подозрительных документов .....	62
Анализ отправленных по электронной почте сообщений .....	63
Аутентификация электронной почты .....	63
<b>Глава 4. Вредоносные программы и защита от них .....</b>	<b>64</b>
Виды вредоносных программ .....	64
Вирусы .....	64
Черви .....	65
Троянские программы .....	66
ArcBomb .....	66
Backdoor .....	67
Banker .....	67
Clicker .....	67
DoS .....	67
Downloader .....	68
Dropper .....	68
Exploit .....	68
FakeAV .....	68
GameThief .....	69
IM .....	69
Loader .....	69
Mailfinder .....	69
Notifier .....	69
Proxy .....	69
PSW .....	69
Ransom .....	70
Rootkit .....	70
SMS .....	70
Spy .....	70

Прочие вредные программы.....	70
Adware.....	71
Pornware.....	71
Riskware.....	72
Киберпреступность.....	73
Поддержка спамеров.....	73
Организация сетевых атак.....	74
Ботнеты.....	74
Платные вызовы и SMS-сообщения.....	75
Кража электронных денег.....	75
Кража банковских данных.....	75
Кибершантаж.....	75
Целевые атаки.....	76
Защита от вредоносных программ.....	77
Антивирусные программы.....	79
Онлайн-проверка файлов на вирусы.....	82
Индикатор взлома.....	83
Действия при обнаружении вредоносной программы.....	84
<b>Глава 5. Бесследное удаление данных.....</b>	<b>85</b>
Удаление файлов в программе BleachBit.....	86
Интерфейс программы BleachBit.....	86
Безвозвратное удаление файлов и папок.....	87
Ограничения программ надежного удаления данных.....	88
Уничтожение данных с жестких дисков.....	88
Уничтожение оптических дисков.....	89
Надежное стирание данных на SSD, Flash-накопителях и SD-картах.....	90
<b>Глава 6. Вкратце о шифровании.....</b>	<b>91</b>
Шифрование: три важных понятия.....	91
Закрытые и открытые ключи.....	91
Сертификаты безопасности.....	91
Отпечатки ключей.....	92
Основы PGP-шифрования.....	92
Игра с двумя ключами.....	93
Электронная подпись.....	93
Принцип работы PGP.....	94
Сеть доверия.....	94
Метаданные: что не может PGP.....	95
Практическое руководство по PGP-шифрованию.....	96
PGP в Windows.....	97
Установка GPG4Win.....	97
Установка Mozilla Thunderbird.....	97
Установка Enigmail.....	99
Использование PGP/MIME.....	101
Оповещение адресатов об использовании PGP.....	102
Оповещение людей об использовании PGP по электронной почте.....	102

Оповещение людей об использовании PGP через веб-сайт.....	103
Загрузка ключей на сервер ключей.....	104
Поиск других пользователей PGP .....	105
Получение открытого ключа по электронной почте.....	105
Получение открытого ключа в виде файла .....	106
Получение открытого ключа с сервера ключей.....	106
Отправка зашифрованных сообщений.....	107
Чтение зашифрованных сообщений.....	109
Отзыв PGP-ключа .....	109
Отзыв PGP-ключа с помощью Enigmail .....	109
Отзыв PGP-ключа с помощью сертификата отзыва.....	109
PGP в OS X.....	110
Установка программы GPGTools .....	110
Создание PGP-ключей.....	111
Создание сертификата отзыва .....	114
Создание резервных копий PGP-ключей.....	114
Отправка зашифрованного/подписанного сообщения в Mail.....	114
Настройка почтового клиента Mozilla Thunderbird .....	115
PGP в Linux.....	119
Установка Thunderbird, GnuPG и Enigmail .....	120
Настройка Thunderbird .....	120
Настройка Enigmail.....	122
Использование PGP/MIME .....	123
<b>Глава 7. Приватный обмен информацией.....</b>	<b>124</b>
Основы безопасного общения .....	124
Принцип работы сквозного шифрования .....	124
Голосовые вызовы .....	125
SMS- и MMS-сообщения.....	125
Мгновенные сообщения.....	126
Электронная почта.....	126
Ограничения сквозного шифрования.....	127
Угрозы безопасности сотовой связи.....	127
Определение местонахождения.....	128
Отслеживание сигнала по вышкам сотовой связи .....	128
Отслеживание сигнала с помощью IMSI-ловушки.....	128
Отслеживание сигнала с помощью Wi-Fi и Bluetooth .....	129
Утечка данных о местонахождении при работе приложений и веб-серфинге .....	130
Выключение телефона.....	130
Одноразовые телефоны.....	131
Спутниковые системы навигации.....	132
Прослушивание сотовой связи .....	132
Заражение телефона вредоносной программой .....	133
Анализ содержимого телефона.....	133
Приватная электронная почта.....	134
Приватное получение/отправка SMS-сообщений.....	136

Приватная голосовая связь .....	140
Программа Signal .....	140
Установка и первый запуск .....	140
Делаем зашифрованный звонок .....	141
Отправляем зашифрованное сообщение .....	141
Система Stealthphone .....	142
Blackphone 2 .....	143
Другие устройства .....	145
Приватный обмен мгновенными сообщениями .....	146
qTox .....	146
ChatSecure .....	148
Установка и настройка .....	149
Работа в программе .....	151
Telegram .....	152
Поддержка русского языка в Telegram .....	153
Основы Telegram .....	155
Секретные чаты .....	157
Создание секретного чата .....	158
Самоуничтожение сообщений .....	159
Удаление аккаунта .....	159
Pidgin .....	159
Установка и настройка Pidgin с OTR .....	160
Установка в Windows .....	160
Установка в Linux .....	161
Добавление учетной записи .....	162
Добавление контакта .....	163
Настройка модуля OTR .....	164
Безопасное общение .....	164
Adium .....	166
Установка программы .....	167
Настройка учетной записи .....	167
Защищенный чат .....	168
Протокол sMix .....	171
Другие программы .....	171

## **ЧАСТЬ II. ЗАЩИЩЕННЫЕ СПОСОБЫ ПЕРЕДАЧИ ДАННЫХ..... 173**

<b>Глава 8. Использование прокси-серверов.....</b>	<b>175</b>
Использование альтернативных адресов веб-ресурсов .....	176
Использование анонимайзеров .....	180
Настройка браузеров для работы через прокси-серверы .....	185
Браузер Internet Explorer .....	185
Браузер Mozilla Firefox .....	186
Браузер Opera .....	188
Браузер Google Chrome .....	189
Браузер Safari .....	191



Настройка мобильных устройств для работы через прокси-серверы .....	191
Операционная система iOS .....	192
Операционная система Windows Phone .....	193
Сети Wi-Fi .....	193
Сотовые сети для передачи данных .....	193
Операционная система Android .....	194
Сети Wi-Fi .....	194
Сотовые сети для передачи данных .....	194
Операционная система Blackberry OS .....	195
Сети Wi-Fi .....	195
Сотовые сети для передачи данных .....	196
Использование цепочек прокси .....	197
Использование файлов автоконфигурации прокси-сервера .....	199
Браузер Internet Explorer .....	199
Браузер Mozilla Firefox .....	200
Браузер Google Chrome .....	201
Браузер Opera .....	202
Браузер Safari .....	203
Использование файлов автоконфигурации прокси-сервера на мобильных устройствах .....	204
Операционная система iOS .....	204
Операционная система Android .....	205
<b>Глава 9. Виртуальные частные сети .....</b>	<b>207</b>
Программа Hotspot Shield .....	208
Универсальное решение ZenMate .....	211
Настройка VPN-туннелей через протокол SSTP .....	213
SSH-туннель к серверу Amazon .....	215
Регистрация учетной записи AWS .....	215
Создание виртуального сервера .....	218
Настройка подключения к виртуальному серверу .....	224
<b>Глава 10. Подмена IP-адресов DNS-серверов .....</b>	<b>226</b>
Подмена IP-адресов DNS-серверов в операционной системе Windows .....	228
Подмена IP-адресов DNS-серверов в операционной системе OS X .....	229
Подмена IP-адресов DNS-серверов в операционной системе iOS .....	230
Подмена IP-адресов DNS-серверов в операционной системе Android .....	231
Подмена IP-адресов DNS-серверов на маршрутизаторе Zyxel Keenetic .....	232
<b>Глава 11. Использование протокола IPv6 .....</b>	<b>234</b>
Основы IPv4, IPv6 и NAT .....	234
Настройка протокола IPv6/Teredo .....	237
С помощью BAT-файла .....	238
Настройка вручную .....	239
Отключение IPv6/Teredo .....	244
Использование туннельных брокеров .....	244
IPv6 через <i>tunnelbroker.net</i> .....	244

<b>Глава 12. Дополнительные способы альтернативной передачи данных.....</b>	<b>248</b>
Turbo-режимы в браузерах.....	248
Браузер Opera.....	248
Яндекс.Браузер.....	249
Использование систем онлайн-переводов.....	250
Использование специальных расширений браузеров.....	251
Подключение к Интернету через мобильные устройства.....	252
Операционная система Android.....	253
Операционная система Windows Phone.....	254
Операционная система iOS.....	255
Операционная система Blackberry OS.....	256
Внешние устройства и подключения.....	257
<b>ЧАСТЬ III. АНОНИМНЫЕ СЕТИ: ЗАЩИЩЕННАЯ РАБОТА В ИНТЕРНЕТЕ.....</b>	<b>259</b>
<b>Глава 13. Основные анонимные сети.....</b>	<b>261</b>
Основы анонимных сетей.....	261
Децентрализованные анонимные сети.....	262
ANts P2P.....	262
Bitmessage.....	263
Freenet.....	265
Gnutella.....	265
I2P.....	267
RetroShare.....	267
Гибридные анонимные сети.....	267
Cjdns.....	268
Psiphon.....	269
Tor.....	270
Java Anonymous Proxy.....	270
<b>Глава 14. Freenet: концепция свободной сети.....</b>	<b>275</b>
Принцип работы.....	275
Установка и настройка клиента.....	276
Просмотр фрисайтов.....	277
<b>Глава 15. I2P: проект невидимого Интернета.....</b>	<b>278</b>
Принцип работы.....	279
Чесночная маршрутизация.....	281
Установка программного обеспечения.....	282
Настройка браузеров для работы с I2P.....	285
Браузер Internet Explorer.....	285
Браузер Mozilla Firefox.....	286
Браузер Opera.....	287
Браузер Google Chrome.....	288
Браузер Apple Safari.....	290
Проверка работоспособности I2P.....	291

Удаление зашифрованного хранилища.....	369
Безопасное стирание зашифрованного хранилища .....	369
Решение проблем запуска .....	369
Завершение работы Tails.....	370
Безопасное стирание Tails.....	371
Linux.....	371
Использование дисковой утилиты.....	371
Сброс носителя с Tails.....	372
Windows: использование утилиты Diskpart .....	372
OS X: использование приложения Дисковая утилита .....	373
<b>Глава 20. Анонимное подключение к Интернету .....</b>	<b>375</b>
Подключение к сети .....	375
Общие положения.....	375
Регистрация на порталах перехвата .....	376
Управление Tor с помощью Vidalia .....	377
Карта сети.....	378
Смена личности в Vidalia .....	379
Безопасный веб-серфинг в Tor Browser .....	379
Упреждающая защита с помощью AppArmor .....	379
Шифрование передачи данных с помощью HTTPS .....	380
Дополнение HTTPS Everywhere .....	381
Torbutton .....	381
Защита от вредоносного кода JavaScript.....	381
Изменение уровня безопасности .....	382
Смена личности в Tor.....	382
Дополнение NoScript для управления сценариями JavaScript.....	383
Анонимное общение в мессенджере Pidgin.....	383
Предустановленные учетные записи.....	384
Протокол шифрования OTR .....	384
Блокировка Tor IRC-серверами .....	384
Генерация имени пользователя.....	384
Поддержка других протоколов.....	385
Защищенная электронная почта Icedove (Thunderbird).....	385
Настройка учетной записи .....	385
OpenPGP-шифрование с помощью Enigmail .....	386
Обеспечение дополнительной защиты с помощью TorBirdy.....	387
Обмен биткоинов в Electrum.....	387
Использование сети I2P .....	387
Причины низкой скорости передачи данных в Tor .....	388
Сложные схемы передачи данных.....	388
Качество ретрансляторов .....	389
Злоупотребление сетью Tor .....	389
<b>Глава 21. Шифрование и конфиденциальность.....</b>	<b>390</b>
Доступ к жесткому диску компьютера .....	390
Виртуальная клавиатура.....	391

Зашифрованные разделы .....	391
Создание зашифрованных разделов .....	392
Определение внешнего носителя .....	392
Форматирование носителя .....	392
Создание зашифрованного раздела .....	392
Использование созданного раздела .....	395
Доступ к ранее созданным зашифрованным разделам .....	395
Шифрование текста с помощью OpenPGP .....	396
Шифрование сообщения с помощью пароля .....	396
Шифрование и подпись сообщения с помощью открытого ключа .....	398
Расшифровка и проверка сообщения .....	400
Надежное удаление данных .....	401
Бесследное удаление файлов .....	403
Затирание свободного места .....	404
Управление паролями с помощью KeePassX .....	405
Создание и сохранение базы паролей .....	405
Разблокировка базы данных в новом сеансе работы .....	406
Использование KeePassX для подстановки паролей .....	407
Вычисление контрольных сумм с помощью GtkHash .....	408
Предотвращение атак методом холодной перезагрузки .....	409
<b>Глава 22. Работа с файлами в Tails .....</b>	<b>410</b>
Работа с документами .....	410
Просмотр и редактирование графических файлов .....	412
Управление мультимедийными данными .....	415
Печать и сканирование .....	418
<b>Глава 23. Дополнительные возможности работы с Tails .....</b>	<b>420</b>
Установка дополнительного программного обеспечения .....	420
Запуск Tails в виртуальной машине .....	422
Обеспечение безопасности .....	422
Приложения виртуализации .....	422
VirtualBox .....	423
Установка VirtualBox .....	423
Запуск Tails из ISO-образа .....	423
VMware Workstation Player .....	425
Установка VMware Workstation Player .....	425
Запуск Tails из ISO-образа .....	426
Боксы .....	429
Установка программы .....	429
Запуск Tails из ISO-образа .....	429
Общий буфер обмена .....	430
Менеджер виртуальных машин .....	431
Установка программы .....	432
Запуск Tails из ISO-образа .....	432
Запуск Tails с USB- или SD-носителя .....	434

Ресурсы в локальной сети .....	435
Обеспечение безопасности при работе в локальной сети .....	436
Веб-серфинг в локальной сети .....	436
Скачивание файлов с локального веб-сайта .....	436
Скачивание файлов с локального FTP-сервера .....	436
Подключение беспроводных устройств .....	436
Некоторые известные проблемы и пути их решения .....	438
Проблемы с запуском Tails .....	438
Проблемные Flash-накопители .....	438
Проблемные компьютеры .....	438
Компьютеры Mac .....	439
Компьютеры с переключаемыми графическими картами .....	439
Архитектура ARM, Raspberry Pi и планшеты .....	440
Передача Tails другому загрузчику .....	440
Проблемы с Wi-Fi .....	440
Интерфейс Broadcom Wi-Fi .....	440
Интерфейс Broadcom BCM43224 802.11a/b/g/n .....	441
Проблемы безопасности .....	441
Tails не стирает содержимое памяти после завершения работы .....	441
Tails не стирает содержимое видеопамати .....	441
Не работает экстренное завершение работы .....	441
Ошибка выброса DVD с Tails .....	441
Не выполняется полная перезагрузка/выключение Tails .....	441
Прочие проблемы .....	442
Контент в формате Adobe Flash не отображается .....	442
Пользовательские настройки системы не сохраняются .....	443
Утерян пароль для доступа к зашифрованному хранилищу .....	443
Скачивание файлов по протоколу BitTorrent .....	443
Скачивание видеофайлов из Интернета .....	443
Сложности обмена файлами в браузере I2P .....	443
Проблемы отображения меню загрузки .....	444
Bluetooth-устройства не работают .....	444
Сбой применения раскладки клавиатуры .....	444
Tails не загружается после обновления .....	444
Сбой предварительного просмотра печати в Tor Browser .....	444
Замедление графики на некоторых картах NVidia .....	444
<b>ПРИЛОЖЕНИЯ .....</b>	<b>445</b>
<b>Приложение 1. Даркнет: подполье Интернета .....</b>	<b>447</b>
Глубинная Паутина и Даркнет .....	447
Доступ к Даркнету .....	448
Анонимная мобильность .....	448
Аудитория Даркнета .....	449
Черные рынки Даркнета .....	451
Криптовалюты .....	453
Реакция властей на Даркнет .....	454
Заключение .....	454

<b>Приложение 2. Вarez и Сцена .....</b>	<b>456</b>
Вarez: киберпиратство .....	456
История киберпиратства .....	458
Причины, повлиявшие на рост пиратства .....	458
Распространение через скомпрометированные FTP-серверы .....	459
Автоматизированное распространение вarezа с помощью IRC-ботов .....	460
Разновидности вarezа .....	460
Пиратство в сфере киноиндустрии .....	462
Обозначения вarezных файлов .....	463
Формат .....	463
Архивация .....	464
Имена файлов .....	464
Сопроводительные файлы релизов .....	464
Файл <i>FILE_ID.DIZ</i> .....	464
NFO-файлы .....	465
SFV-файл .....	467
Прочие файлы .....	467
Последствия нарушения стандартов .....	468
Аудио- и видеорелизы .....	468
Типы видеорелизов .....	468
Типы аудиорелизов .....	474
Релизы программного обеспечения .....	475
Инструменты обхода защиты программ от нелегального копирования .....	476
Преследование по закону .....	479
Опасности, связанные с использованием вarezа .....	479
Вarezные сайты .....	482
Форумы, где ссылки лежат .....	485
FTP- и HTTP-архивы .....	486
Электронные библиотеки .....	488
<b>Сцена: андеграунд Всемирной паутины .....</b>	<b>490</b>
Развитие Сцены .....	491
Создание релизов .....	492
«Нюки» релизов .....	492
Взлом и обратная разработка .....	494
Топ-сайты .....	494
Система кредитов .....	494
Вarezные группы .....	495
Курьеры .....	495
Релизные группы .....	495
aPOCALYPSE pRODUCTION cREW (aPC) .....	496
Challenge Of Reverse Engineering (CORE) .....	496
Centropy .....	497
CLASS (CLS) .....	497
DEVIANCE .....	498
DrinkOrDie .....	498
Echelon .....	500
FairLight .....	500

HYBRID .....	501
International Network of Crackers (INC).....	501
Kalisto .....	501
LineZero (Lz0) .....	502
Myth .....	502
PARADOX (PDX).....	503
Rabid Neurosis (RNS).....	504
Radium .....	504
Razor 1911 (RZR).....	504
RELOADED (RLD).....	505
RiSCiSO .....	506
SKIDROW .....	506
Superior Art Creations (SAC) .....	506
The Humble Guys (THG).....	508
Tristar and Red Sector Incorporated (TRSI).....	509
United Software Association (USA) .....	510
Несколько слов в заключение раздела .....	510
<b>Приложение 3. Компьютерное искусство.....</b>	<b>512</b>
Искусство ASCII-Art.....	512
Трекерная музыка .....	514
Интро, демо и крэктро.....	517
<b>Приложение 4. Получение нввайтс на закрытые сайты (на примере <i>What.cd</i>).....</b>	<b>520</b>
<b>Приложение 5. Краткий глоссарий терминов пользователя .....</b>	<b>525</b>
<b>Источники.....</b>	<b>587</b>
<b>Предметный указатель .....</b>	<b>589</b>