

Михаил Райтман

Информационная  
безопасность  
для пользователя

# ПРАВИЛА САМОЗАЩИТЫ В ИНТЕРНЕТЕ



Надёжная защита  
аккаунтов  
и многофакторная  
аутентификация



Основы  
криптографии  
и сквозное  
шифрование



Анонимные сети  
и приватное  
общение



Особенности  
защиты мобильных  
устройств



Доступ  
к заблокированным  
устройствам



Полная  
приватность  
силами  
операционной  
системы Tails



Секреты  
Даркнета  
и вarezной Сцены



Хакерские группы  
и цифровое  
искусство

**Михаил Райтман**

Информационная  
безопасность  
для пользователя

**ПРАВИЛА  
САМОЗАЩИТЫ  
В ИНТЕРНЕТЕ**

Санкт-Петербург  
«БХВ-Петербург»

2023

УДК 004.738.5  
ББК 32.973.26-018.2  
P12

**Райтман М. А.**

P12 Информационная безопасность для пользователя. Правила самозащиты в Интернете. — СПб.: БХВ-Петербург, 2023. — 400 с.: ил.

ISBN 978-5-9775-1170-4

Книга о безопасной работе в Интернете и защите персональных данных, в том числе с соблюдением мер анонимизации и приватности. Рассматриваются вопросы выбора надежных паролей, использования прокси-серверов, анонимных сетей и VPN, технологии шифрования и защищенного общения. Особое внимание уделено анонимной операционной системе Tails, рекомендуемой Эдвардом Сноуденом. Приведены способы конспиративного общения по защищенным каналам связи и подключения к анонимным сетям, таким как I2P RetroShare и др. Даются практические рекомендации по безопасной работе с торрентами, мессенджерами, файловыми архивами. Книга поможет разобраться в устройстве Даркнета и вarezной Сцены. Отдельная глава посвящена луковой архитектуре и браузеру Tor. Особое внимание уделено кастомизации устанавливаемых программ.

*Для специалистов по безопасности, системных администраторов,  
мелких пользователей Linux*

УДК 004.738.5  
ББК 32.973.26-018.2

### Группа подготовки издания:

Руководитель проекта	<i>Олег Сивченко</i>
Зав. редакцией	<i>Людмила Гауль</i>
Редактор	<i>Григорий Добин</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Дизайн обложки	<i>Зои Канторович</i>

Подписано в печать 01.07.22.

Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 32,25.

Тираж 1000 экз. Заказ № 4688.

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано с готового оригинал-макета

ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-1170-4

© ООО "БХВ", 2023  
© Оформление. ООО "БХВ-Петербург", 2023

# Оглавление

Предисловие .....	13
<b>ЧАСТЬ I. АНОНИМНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ В ИНТЕРНЕТЕ .....</b>	<b>15</b>
<b>Глава 1. Защита персональных данных .....</b>	<b>17</b>
Защита компьютеров и мобильных устройств .....	18
Шифрование данных в операционной системе Windows .....	20
Упрощенное шифрование Windows .....	20
Стандартное шифрование BitLocker .....	21
Шифрование данных в операционной системе macOS .....	22
Шифрование данных на iOS/iPadOS-устройствах .....	24
Шифрование данных на Android-устройствах .....	26
Система разблокировки Google Smart Lock .....	27
Защита портативных накопителей данных .....	28
Безопасность при использовании сетей Wi-Fi .....	29
Угрозы, возникающие при подключении к открытой сети Wi-Fi .....	30
Защита собственной сети Wi-Fi .....	33
Еще о защите персональных данных .....	36
Безопасный веб-серфинг .....	38
Приватные режимы браузеров .....	38
Использование протокола HTTPS .....	39
Расширение HTTPS Everywhere .....	40
Удаление истории посещений и cookie-файлов .....	41
<b>Глава 2. Надежные пароли и двухфакторная аутентификация .....</b>	<b>44</b>
Создание надежных паролей .....	45
О «секретных вопросах» .....	45
Менеджеры паролей .....	46
Выбор мастер-пароля .....	47
Использование файла-ключа .....	47
Комбинация мастер-пароля и файла-ключа .....	47
Работа с программой KeePassXC .....	48
Установка программы .....	48

Добавление паролей .....	48
Использование паролей .....	50
Дополнительные функции .....	50
Синхронизация паролей между несколькими устройствами .....	50
Двухфакторная аутентификация и одноразовые пароли .....	51
Настройка двухфакторной аутентификации .....	51
Как включить двухфакторную аутентификацию? .....	53
Создание второстепенных аккаунтов .....	54
<b>Глава 3. Фишинговые атаки .....</b>	<b>55</b>
Признаки фишинговой атаки .....	55
Защита от фишинговых атак .....	62
Проверка писем через отправителей .....	62
Использование облачных хранилищ и файловых хостингов .....	63
Безопасный просмотр подозрительных документов .....	63
Анализ отправленных по электронной почте сообщений .....	64
Аутентификация электронной почты .....	64
<b>Глава 4. Вредоносные программы и защита от них .....</b>	<b>65</b>
Виды вредоносных программ .....	65
Вирусы .....	65
Черви .....	66
Троянские программы .....	67
DNS-спуферы .....	68
RAT-инструменты .....	68
Блокировщики .....	68
Ботнеты .....	69
Буткиты .....	69
Бэждоры .....	69
Банковские трояны .....	69
Вымогатели .....	70
Даунлоадеры .....	70
Дропперы .....	70
Загрузчики .....	71
Кейлоггеры .....	71
Кликеры .....	71
Майнеры .....	71
Оверлеи .....	71
Платные вызовы и SMS-сообщения .....	71
Прокси-трояны .....	72
Руткиты .....	72
Рутовальщики .....	72
Стилеры (PSW) .....	73
Шифровальщики .....	73
Шпионское ПО .....	73
Эксплойты .....	73
Прочие вредоносные программы .....	73
Adware .....	74
Pornware .....	74

Riskware .....	75
Stalkerware .....	76
Другие киберугрозы .....	77
APT-атаки .....	77
DDoS-атаки .....	77
MITM-атаки (атака «человек посередине») .....	77
SQL-инъекции (внедрение SQL-кода) .....	78
Вишинг .....	78
Дипфейки .....	78
Кликджекинг .....	78
Кража банковских данных .....	79
Кража личности .....	79
Целевые атаки .....	79
Как защититься от вредоносных программ? .....	80
Антивирусные программы .....	82
Онлайн-проверка файлов на вирусы .....	85
Действия при обнаружении вредоносной программы .....	86
<b>Глава 5. Бесследное удаление данных</b> .....	<b>88</b>
Удаление файлов в программе BleachBit .....	89
Интерфейс программы BleachBit .....	89
Безвозвратное удаление файлов и папок в программе BleachBit .....	90
Ограничения программ надежного удаления данных .....	91
Уничтожение данных с жестких дисков .....	91
Уничтожение оптических дисков .....	92
Надежное стирание данных с твердотельных накопителей .....	93
<b>Глава 6. Вкратце о шифровании</b> .....	<b>94</b>
Шифрование: три важных понятия .....	94
Закрытые и открытые ключи .....	94
Сертификаты безопасности .....	94
Отпечатки ключей .....	95
Основы PGP-шифрования .....	95
Шифрование с двумя ключами .....	96
Электронная подпись .....	96
Принцип работы PGP .....	97
Сеть доверия .....	98
Метаданные: что не может PGP .....	98
Практическое руководство по PGP-шифрованию .....	99
Установка Mozilla Thunderbird .....	100
Создание ключей .....	102
Оповещение своих адресатов об использовании PGP .....	103
Поиск других пользователей PGP .....	105
Подтверждение принятых ключей .....	107
Отправка зашифрованных сообщений .....	108
Чтение зашифрованных сообщений .....	109
Отзыв PGP-ключа .....	109

<b>Глава 7. Приватный обмен информацией</b> .....	<b>111</b>
<b>Основы безопасного общения</b> .....	111
Принцип работы сквозного шифрования .....	111
Голосовые вызовы .....	112
SMS- и MMS-сообщения.....	112
Мгновенные сообщения .....	112
Электронная почта.....	113
<b>Безопасность при использовании сотовой связи</b> .....	113
<b>Определение местонахождения</b> .....	115
Отслеживание сигнала по вышкам сотовой связи .....	115
Отслеживание сигнала с помощью IMSI-ловушки.....	115
Отслеживание сигнала с помощью Wi-Fi и Bluetooth .....	116
Утечка данных о местонахождении при работе приложений и веб-серфинге .....	117
Пользовательские данные .....	118
Выключение телефона.....	118
Одноразовые телефоны .....	118
Защита от прослушивания сотовой связи .....	120
Заражение телефона вредоносной программой .....	120
Защита от анализа содержимого телефона .....	121
Приватная электронная почта.....	121
Приватное получение/отправка SMS-сообщений.....	123
Приватная голосовая связь .....	124
<b>Программа Signal</b> .....	124
Установка и первый запуск.....	125
Делаем зашифрованный звонок .....	126
Отправляем зашифрованное сообщение.....	126
Приватный обмен мгновенными сообщениями.....	127
Клиентское приложение qTox .....	127
Telegram .....	129
Общение в Telegram .....	130
Секретные чаты.....	131
Создание секретного чата.....	132
Самоуничтожение сообщений.....	132
Удаление аккаунта.....	132
Pidgin.....	133
Установка Pidgin с OTR .....	133
Добавление учетной записи .....	134
Добавление контакта .....	135
Настройка модуля OTR.....	136
Безопасное общение .....	137
Adium .....	138
Установка программы Adium .....	139
Настройка учетной записи .....	139
Защищенный чат .....	140
<b>Глава 8. Безопасное подключение к Интернету</b> .....	<b>143</b>
Использование альтернативных адресов веб-ресурсов .....	144
Использование анонимайзеров.....	148

Настройка системы для работы через прокси-серверы.....	151
Подключение компьютеров.....	151
Настройки для Windows.....	152
Настройки для macOS.....	153
Подключение мобильных устройств.....	154
Настройки для iOS.....	154
Настройки для Android.....	155
Использование цепочек прокси.....	155
Использование сценариев автоконфигурации прокси-сервера.....	157
Подключение компьютеров.....	157
Настройки для Windows.....	157
Настройки для macOS.....	158
Подключение мобильных устройств.....	158
Настройки для iOS.....	158
Настройки для Android.....	159
Использование VPN-сервисов.....	159
VPN-сервис Surfshark.....	160
Универсальное решение ZenMate.....	162
SSH-туннель к серверу Amazon.....	164
Изменение IP-адресов DNS-серверов.....	171
Настройки для Windows.....	173
Настройки для macOS.....	176
Настройки для iOS/iPadOS.....	176
Настройки для Android.....	177
Маршрутизаторы и прочие сетевые устройства.....	177
Использование туннельных брокеров IPv6.....	178
Вкратце о IPv4 и IPv6.....	179
Использование туннельных брокеров.....	181
Подключение к Интернету через внешние устройства.....	184
Настройки для Android.....	185
Настройки для iOS/iPadOS.....	187
<b>ЧАСТЬ II. АНОНИМНЫЕ СЕТИ.....</b>	<b>189</b>
<b>Глава 9. Основные анонимные сети.....</b>	<b>191</b>
Базовые сведения об анонимных сетях.....	191
Децентрализованные анонимные сети.....	192
Bitmessage.....	192
Freenet.....	194
Gnutella.....	194
I2P.....	196
RetroShare.....	196
ZeroNet.....	196
Гибридные анонимные сети.....	197
Cjdns.....	197
Psiphon.....	198
Tor.....	200
JAP.....	200



<b>Глава 10. Freenet: концепция свободной сети .....</b>	<b>204</b>
Принцип работы .....	204
Установка и настройка клиента .....	205
Просмотр и публикация фрисайтов .....	205
<b>Глава 11. I2P: проект невидимого Интернета .....</b>	<b>207</b>
Принцип работы сети I2P .....	208
Чесночная маршрутизация .....	210
Установка программного обеспечения I2P .....	211
Настройка браузеров для работы с I2P .....	214
Настройки для Windows .....	215
Настройки для macOS .....	216
Проверка работоспособности I2P .....	216
<b>Глава 12. Платформа RetroShare .....</b>	<b>218</b>
Принцип работы .....	218
Общение в RetroShare .....	219
Обмен файлами в RetroShare .....	220
Установка и настройка клиента RetroShare .....	221
Добавление друзей .....	222
<b>Глава 13. Tor: луковая маршрутизация .....</b>	<b>225</b>
Луковая маршрутизация .....	226
Принцип работы Tor .....	227
Установка приложения Tor Browser .....	230
<b>ЧАСТЬ III. ОБЕСПЕЧЕНИЕ МАКСИМАЛЬНОГО УРОВНЯ АНОНИМНОСТИ И БЕЗОПАСНОСТИ С ПОМОЩЬЮ TAILS .....</b>	<b>233</b>
<b>Глава 14. Основы операционной системы Tails .....</b>	<b>235</b>
Что такое Tails? .....	235
Системные требования Tails .....	236
Программное обеспечение в составе Tails .....	236
Проблемы безопасности при работе в Tails .....	238
Скомпрометированное аппаратное обеспечение .....	239
Установка и подключение к недоверенным системам .....	239
Модификация BIOS и другого встроенного ПО .....	239
Перехват трафика с выходных узлов Tor .....	239
Вскрытие использования Tor и Tails .....	240
Атаки посредника .....	240
Атаки на опознание трафика .....	241
Недостатки шифрования документов .....	241
Метаданные документов и открытые данные зашифрованных сообщений .....	242
Системы глобальной слежки .....	242
Двойная жизнь .....	243
Слабые пароли .....	243
Эволюция Tails .....	243
Обеспечение защиты пользователя Tails .....	243

Событие факта использования Tails.....	245
Важные замечания касательно посещаемых сайтов.....	245
Важные замечания касательно провайдеров и сетевых администраторов.....	245
<b>Глава 15. Загрузка и установка Tails.....</b>	<b>246</b>
Загрузка и проверка образа Tails.....	246
Выбор типа носителя.....	247
Развертывание ISO-образа системы.....	248
Развертывание ISO-образа Tails на DVD.....	248
OC Windows.....	248
MacOS.....	250
OC Linux.....	250
В окружении GNOME.....	250
В окружении KDE.....	251
Развертывание ISO-образа Tails на Flash-накопитель.....	251
OC Windows.....	251
MacOS.....	252
OC Linux.....	252
Развертывание Tails на Flash-накопитель с помощью Tails Installer.....	252
Обновление Tails.....	254
Автоматическое обновление с помощью Tails Upgrader.....	254
Обновление вручную с помощью Tails Installer.....	255
<b>Глава 16. Запуск Tails.....</b>	<b>256</b>
Запуск операционной системы Tails.....	256
Параметры загрузки.....	260
Пароль администратора.....	260
Анонимизация MAC-адресов.....	261
Необходимость в смене MAC-адреса.....	261
Отмена анонимизации MAC-адреса.....	262
Офлайнный режим.....	263
Небезопасный браузер.....	263
Настройка подключения через Tor.....	264
Обзор рабочего стола Tails.....	268
Верхняя навигационная панель.....	268
Обзор приложений.....	270
Рабочий стол.....	270
Зашифрованное хранилище.....	271
Меры безопасности при работе с зашифрованным хранилищем.....	271
Создание зашифрованного хранилища.....	272
Запуск мастера создания зашифрованного хранилища.....	272
Настройки хранилища.....	273
Использование зашифрованного хранилища.....	276
Копирование зашифрованного хранилища на новый носитель.....	276
Удаление зашифрованного хранилища.....	277
Безопасное стирание зашифрованного хранилища.....	277
Завершение работы Tails.....	277
Безопасное стирание Tails.....	278
OC Windows.....	278

MacOS .....	279
☉C Linux .....	280
<b>Глава 17. Анонимное подключение к Интернету в Tails.....</b>	<b>282</b>
Способы подключения к Интернету в Tails .....	282
Информация о подключении в приложении Onion Circuits .....	284
Безопасный веб-серфинг в Tor Browser .....	285
Упреждающая защита с помощью AppArmor .....	285
Шифрование передачи данных с помощью HTTPS .....	285
Расширение HTTPS Everywhere .....	286
Защита от вредоносного JavaScript-кода .....	287
Дополнение NoScript для управления JavaScript-сценариями .....	287
Изменение уровня безопасности .....	287
Смена цепочки узлов в Tor Browser .....	288
Смена личности в Tor Browser.....	288
Функция Letterboxing.....	289
Анонимное общение в мессенджере Pidgin.....	289
Протокол шифрования OTR .....	290
Защищенная электронная почта Thunderbird .....	290
Настройка учетной записи .....	290
OpenPGP-шифрование.....	292
Обеспечение дополнительной защиты.....	292
Обмен файлами с помощью OnionShare .....	292
<b>Глава 18. Шифрование и конфиденциальность в Tails .....</b>	<b>294</b>
Доступ к жесткому диску компьютера .....	294
Экранная клавиатура .....	295
Зашифрованные разделы .....	295
Создание зашифрованных разделов.....	295
Определение внешнего носителя .....	295
Форматирование носителя .....	296
Создание зашифрованного раздела .....	296
Доступ к ранее созданным зашифрованным разделам.....	298
Шифрование текста с помощью OpenPGP .....	299
Шифрование сообщения с помощью пароля .....	300
Шифрование и подписание сообщения с помощью открытого ключа .....	302
Расшифровка и проверка сообщения .....	303
Надежное удаление данных .....	305
Бесследное удаление файлов .....	307
Затирание свободного места.....	308
Управление паролями с помощью KeePassXC .....	308
Создание и сохранение базы паролей .....	309
Разблокировка базы данных в новом сеансе работы .....	310
Использование KeePassXC для подстановки паролей.....	310
Вычисление контрольных сумм с помощью GtkHash .....	310
Предотвращение атак методом холодной перезагрузки .....	311
<b>Глава 19. Работа с файлами в Tails.....</b>	<b>312</b>
Работа с документами .....	312
Просмотр и редактирование графических файлов .....	313

Управление мультимедийными данными.....	314
Печать и сканирование.....	315
<b>Глава 20. Дополнительные возможности работы с Tails .....</b>	<b>317</b>
Установка дополнительного программного обеспечения.....	317
Запуск Tails в виртуальной машине.....	318
Обеспечение безопасности.....	318
Приложения виртуализации.....	319
VirtualBox.....	319
Установка VirtualBox.....	319
Запуск Tails из ISO-образа.....	319
Обеспечение безопасности при работе в локальной сети.....	322
<b>ПРИЛОЖЕНИЯ .....</b>	<b>323</b>
<b>Приложение 1. Даркнет: подполье Интернета .....</b>	<b>325</b>
Глубинная паутина и Даркнет.....	325
Доступ к Даркнету.....	326
Анонимная мобильность.....	326
Аудитория Даркнета.....	327
Черные рынки Даркнета.....	329
Криптовалюты.....	329
Реакция властей на Даркнет.....	330
Заклочение.....	330
<b>Приложение 2. Вarez и Сцена .....</b>	<b>332</b>
Вarez: киберпиратство.....	332
История киберпиратства.....	334
Причины, повлиявшие на рост пиратства.....	334
Распространение через скомпрометированные FTP-серверы.....	335
Автоматизированное распространение вarezа с помощью IRC-ботов.....	335
Разновидности вarezа.....	336
Пиратство в сфере киноиндустрии.....	337
Обозначения вarezных файлов.....	338
Формат.....	339
Архивация.....	339
Имена файлов.....	340
Сопроводительные файлы релизов.....	340
Файл <i>FILE_ID.DIZ</i> .....	340
NFO-файлы.....	341
SFV-файл.....	343
Прочие файлы.....	343
Последствия нарушения стандартов.....	344
Аудио- и видеорелизы.....	344
Типы видеорелизов.....	344
Типы аудиорелизов.....	350
Релизы программного обеспечения.....	351
Инструменты обхода защиты программ от нелегального копирования.....	352
Преследование по закону.....	355

Опасности, связанные с использованием варежа.....	355
Варезные сайты.....	358
Форумы, где ссылки лежат.....	361
FTP- и HTTP-архивы.....	362
Электронные библиотеки.....	364
Сцена: андеграунд Интернета.....	365
Развитие Сцены.....	365
Создание релизов.....	366
«Нюки» релизов.....	366
Взлом и обратная разработка.....	368
Топ-сайты.....	368
Система кредитов.....	369
Варезные группы.....	369
Курьеры.....	369
Релизные группы.....	369
aPOCALYPSE pRODUCTION cREW (aPC).....	370
Challenge Of Reverse Engineering (CORE).....	370
Centropy.....	371
CLASS (CLS).....	371
DEViANCE.....	372
DrinkOrDie.....	372
Echelon.....	374
FairLight.....	374
HYBRID.....	375
International Network of Crackers (INC).....	375
Kalisto.....	375
LineZero (Lz0).....	376
Myth.....	376
PARADOX (PDX).....	377
Rabid Neurosis (RNS).....	377
Radium.....	378
Razor 1911 (RZR).....	378
RELOADED (RLD).....	379
RiSCiSO.....	379
SKiDROW.....	380
Superior Art Creations (SAC).....	381
The Humble Guys (THG).....	381
Tristar and Red Sector Incorporated (TRSI).....	383
United Software Association (USA).....	383
Несколько слов в заключение раздела.....	383
<b>Приложение 3. Компьютерное искусство.....</b>	<b>385</b>
Искусство ASCII-Art.....	385
Трекерная музыка.....	387
Интро, демо и крэктро.....	390
<b>Источники.....</b>	<b>393</b>
<b>Предметный указатель.....</b>	<b>394</b>