

Содержание

ВВЕДЕНИЕ.....	10
ЛАЙФХАК 1. ПАРОЛЬНАЯ ЗАЩИТА БЕСПРОВОДНОЙ СЕТИ	12
ЛАЙФХАК 2. БЕЛЫЕ/ЧЕРНЫЕ СПИСКИ MAC-АДРЕСОВ	18
ЛАЙФХАК 3. ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ WI-FI	20
ЛАЙФХАК 4. ОТКЛЮЧЕНИЕ WI-FI SENSE	22
ЛАЙФХАК 5. ВЫБОР ОПТИМАЛЬНОГО СРЕДСТВА ЗАЩИТЫ ДАННЫХ НА ДИСКЕ.....	25
ЛАЙФХАК 6. ПРОЗРАЧНОЕ ШИФРОВАНИЕ ПАПКИ СРЕДСТВАМИ EFS. ВКЛЮЧЕНИЕ ШИФРОВАНИЯ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ	31
ЛАЙФХАК 7. АРХИВАЦИЯ КЛЮЧА ВОССТАНОВЛЕНИЯ	36
ЛАЙФХАК 8. ВОССТАНОВЛЕНИЕ ДОСТУПА К ЗАШИФРОВАННЫМ ПАПКАМ С ПОМОЩЬЮ АГЕНТОВ ВОССТАНОВЛЕНИЯ	40
ЛАЙФХАК 9. ШИФРОВАНИЕ РАЗДЕЛА ЖЕСТКОГО ДИСКА С ПОМОЩЬЮ BITLOCKER ...	44

ЛАЙФХАК 10. ЗАЩИТА ДИСКА, ЗАШИФРОВАННОГО С ПОМОЩЬЮ BITLOCKER	58
ЛАЙФХАК 11. ИСПОЛЬЗОВАНИЕ КРИПТОКОНТЕЙНЕРОВ	65
ЛАЙФХАК 12. ЗАЩИТА ОТ ВИРУСОВ– ШАНТАЖИСТОВ	73
ЛАЙФХАК 13. СПОСОБЫ СОКРЫТИЯ ИНФОРМАЦИИ. ДЮЖИНА СОВЕТОВ В ОДНОМ	79
#1. ПРИМЕНЕНИЕ АТРИБУТОВ	80
#2. ПЕРЕМЕЩЕНИЕ В ПАПКИ «ПОДАЛЬШЕ»	81
#3. ПРЯЧЕМ В АРХИВЕ	81
#4. ПЕРЕИМЕНОВАНИЕ ФАЙЛА.....	82
#5. ПЕРЕИМЕНОВАНИЕ ПАПКИ	82
#6. АРХИВ С ШИФРОВАНИЕМ.....	83
#7. ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ПРОГРАММ ДЛЯ СОКРЫТИЯ ФАЙЛОВ.....	84
#8. ПРЯЧЕМ ЛОГИЧЕСКИЕ ДИСКИ	84
#9. СТЕГАНОГРАФИЯ	85
#10. ПОТОКИ ДАННЫХ NTFS (ADS)	86
#11. ДОЗАПИСЬ В СЕКТОР.....	86
#12. УДАЛЕНИЕ	87
ЛАЙФХАК 14. УДАЛЕНИЕ РЕКЛАМНЫХ И ВРЕДНОСНЫХ ПРОГРАММ	88
ЛАЙФХАК 15. БЕЗОПАСНОЕ УДАЛЕНИЕ ДАННЫХ	90

ЛАЙФХАК 16. РЕЗЕРВНОЕ КОПИРОВАНИЕ	94
ЛАЙФХАК 17. ЗАЩИТА DNS	97
ЛАЙФХАК 18. ЗАЩИТА ПЕРЕДАВАЕМЫХ ПО СЕТИ ДАННЫХ. VPN-СЕРВИСЫ	101
ЛАЙФХАК 19. ЗАЩИТА ПОЧТОВОГО ЯЩИКА	106
ЛАЙФХАК 20. ВЫБОР БЕЗОПАСНОГО МЕССЕНДЖЕРА	110
ЛАЙФХАК 21. БОРЕМСЯ ЗА КОНФИДЕНЦИАЛЬНОСТЬ.....	117
ЛАЙФХАК 22. ПРИДУМЫВАЕМ НАДЕЖНЫЕ ПАРОЛИ	124
ЛАЙФХАК 23. ЗАПОМИНАЕМ ПАРОЛИ. МЕНЕДЖЕРЫ ПАРОЛЕЙ	129
ЛАЙФХАК 24. ОЧИСТКА КОМПЬЮТЕРА ПЕРЕД ЕГО ПЕРЕДАЧЕЙ.....	134
ЛАЙФХАК 25. ЗАЩИТА ВЕБ-КАМЕР И МИКРОФОНА.....	141
ЛАЙФХАК 26. ЗАЩИТА ПРИНТЕРА	144
ЛАЙФХАК 27. ЗАЩИТА МОБИЛЬНОГО БАНКИНГА	146
ЛАЙФХАК 28. БЕЗОПАСНОСТЬ ANDROID-СМАРТФОНА.....	152

ЛАЙФХАК 29. БЕЗОПАСНОСТЬ IPHONE	155
ЛАЙФХАК 30. ЗАЩИТА ДАННЫХ, ХРАНИМЫХ НА ANDROID	158
ГЛАВА 1. КАК ШИФРОВАТЬ ЛИЧНЫЕ ДАННЫЕ	161
1.1. МЕТОДЫ КРИПТОГРАФИИ. СИММЕТРИЧНАЯ И АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ.....	162
1.2. АЛГОРИТМЫ ШИФРОВАНИЯ.....	163
1.3. СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ	166
1.3.1. PGP.....	166
1.3.2. Стандарт S/MIME.....	168
1.3.3. Безопасные почтовые сервисы. HushMail	170
1.3.4. Плагины браузера.....	173
Плагин браузера PGP Mail	173
Плагин браузера SecureGmail	174
Плагин браузера Encrypted Communication	175
1.3.5. Плагины почтовых клиентов.....	176
Плагин почтового клиента Enigmail.....	176
Плагин почтового клиента CyberSafe Mail.....	176
1.4. СРАВНЕНИЕ СРЕДСТВ ЗАЩИТЫ. ВЫБОР ИДЕАЛЬНОГО СРЕДСТВА	177
1.4.1. Проблема выбора	177
1.4.2. Выводы.....	183
ГЛАВА 2. МЕТОДЫ ВЗЛОМА ЛИЧНОЙ ИНФОРМАЦИИ	184
2.1. ТРОЯНСКИЙ КОНЬ	185
2.2. ВЗЛОМ ПО НОМЕРУ ТЕЛЕФОНА	190
2.3. ФИЗИЧЕСКИЙ ДОСТУП К КОМПЬЮТЕРУ	192
2.4. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ИЛИ ПРОСТО ОБМАН	195
2.5. МОДНОЕ СЛОВО «ФИШИНГ»	196
2.6. ВОССТАНАВЛИВАЕМ ПАРОЛЬ	200

2.7. КРАЖА COOKIES	201
2.8. XSS-УЯЗВИМОСТИ.....	203
2.9. МЕТОД ГРУБОЙ СИЛЫ	203
ГЛАВА 3. КАК ЗАЩИТИТЬ СВОЮ ЭЛЕКТРОННУЮ ПОЧТУ	205
3.1. НЕМНОГО ТЕОРИИ. S/MIME, PKI И PGP	206
3.2. КАК БУДЕМ ЗАЩИЩАТЬ ПОЧТУ	209
3.3. ИСПОЛЬЗОВАНИЕ OPENSLL	210
3.4. ИСПОЛЬЗОВАНИЕ CYBERSAFE TOP SECRET	210
3.5. НАСТРОЙКА MICROSOFT OUTLOOK	215
3.6. НАСТРОЙКА ШИФРОВАНИЯ В ДРУГИХ ПОЧТОВЫХ КЛИЕНТАХ	222
ГЛАВА 4. ЭЛЕКТРОННАЯ ПОДПИСЬ И ЕЕ ИСПОЛЬЗОВАНИЕ	223
4.1. ЧТО ТАКОЕ ЭЛЕКТРОННАЯ ПОДПИСЬ?	224
4.2. СЛУЧАИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В НЕБОЛЬШОЙ КОМПАНИИ.....	224
4.2.1. Внутренний документооборот	224
4.2.2. Обмен документами с филиалами и партнерами	225
4.2.3. Некоторые проблемы внедрения электронной подписи	226
4.3. РАБОТА С ЭЛЕКТРОННОЙ ПОДПИСЬЮ ПОСРЕДСТВОМ ПОЧТОВОГО КЛИЕНТА.....	228
4.4. РАБОТА С ЦИФРОВОЙ ПОДПИСЬЮ В LINUX	229
ГЛАВА 5. КАК СОХРАНИТЬ АНОНИМНОСТЬ В ИНТЕРНЕТЕ	235
5.1. ПОСТАНОВКА ЦЕЛЕЙ.....	236
5.2. ВЫБОР СПОСОБА ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ.....	237
5.2.1. Разовое сокрытие IP-адреса и анонимайзеры	237
5.2.2. Постоянное сокрытие IP-адреса и анонимные прокси	238

5.2.3. Изменение региона, сокрытие IP и шифрование данных	241
5.3. ПОДВОДИМ ИТОГИ	242
5.4. ЧТО ЕЩЕ НУЖНО ЗНАТЬ ОБ АНОНИМНОСТИ	243
ГЛАВА 6. ТЕНЕВОЙ ИНТЕРНЕТ - ПРОЕКТ TOR.....	245
6.1. ПРИНЦИП РАБОТЫ TOR.....	246
6.2. ЧТО ЛУЧШЕ – TOR ИЛИ VPN?	248
6.3. КОМБИНИРУЕМ VPN И TOR	249
6.4. ЧТО ДЕЛАТЬ С DNS-ТРАФИКОМ?	249
6.5. ИСПОЛЬЗОВАНИЕ TOR	250
ГЛАВА 7. VPN-АНОНИМАЙЗЕР — ЭТО ПРОСТО	256
7.1. КАК РАБОТАЕТ PIA.....	257
7.2. КАК УСТАНОВИТЬ PIA	257
7.3. ИСПОЛЬЗОВАНИЕ PIA	260
ГЛАВА 8. ЗАЩИТА ОТ ВИРУСОВ	262
8.1. КАК БУДЕТ ПРОИЗВОДИТЬСЯ ТЕСТИРОВАНИЕ	264
8.2. KASPERSKY INTERNET SECURITY	267
8.3. DR.WEB SECURITY SPACE	277

