


# ЛАБОРАТОРИЯ ХАКЕРА

С. А. Бабин



Примеры взлома  
Бесплатные программы  
Атаки на Wi-Fi-сети  
О кражах паролей для соцсетей  
Радужные таблицы  
Хакинг со смартфона

bhv®

**С. А. Бабин**

# **ЛАБОРАТОРИЯ ХАКЕРА**

Санкт-Петербург  
«БХВ-Петербург»  
2016

УДК 004  
ББК 32.973.26-018.2  
Б12

**Бабин С. А.**

Б12 Лаборатория хакера. — СПб.: БХВ-Петербург, 2016. — 240 с.: ил. —  
(Глазами хакера)

ISBN 978-5-9775-3535-9

Рассмотрены методы и средства хакерства с целью понимания и применения соответствующих принципов противодействия им. В виде очерков описаны познавательные эксперименты, которые может выполнить в домашних условиях каждый желающий, начиная со старшеклассника и студента. Используемые программы, как правило, бесплатны. Теории дан минимум, зато книга насыщена практически приемами по разнообразным темам. Описан ряд способов перехвата паролей, взлома Wi-Fi-сетей, дальнейшие действия злоумышленника после проникновения в локальную сеть жертвы. Рассказано о шифровании данных, способах сохранения инкогнито в Интернете, методах взлома паролей из базы Active Directory. Много внимания уделено изучению хакинга с использованием смартфонов. Подробно рассмотрены практические методы генерации и использования радужных таблиц. За счет подробного описания настроек, качественной визуализации материала, преобладания ориентированности на Windows-системы (для примеров с UNIX подробно описывается каждый шаг), книга интересна и понятна любому пользователю персонального компьютера: от начинающего до профессионала.

*Для пользователей ПК*

УДК 004  
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>Анна Кузьмина</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн обложки	<i>Марины Дамбиевой</i>

Подписано в печать 29.04.16.  
Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 19,35.  
Доп. тираж 2000 экз. Заказ № 1385.  
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"  
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3535-9

© Бабин С. А., 2016  
© Оформление, издательство "БХВ-Петербург", 2016

# Оглавление

<b>Введение .....</b>	<b>5</b>
<b>Глава 1. Почему стало сложнее похитить пароль для входа в социальные сети "ВКонтакте", "Одноклассники"*. Фишинг. Социальная инженерия на практике .....</b>	<b>9</b>
1.1. Об атаке "человек посередине". Программы Cain & Abel и SIW .....	9
1.2. Блокнот для фишинга. Denwer. Kali Linux .....	17
1.3. Социальная инженерия .....	28
<b>Глава 2. Хэш-функции паролей. Шифрование сетевых соединений .....</b>	<b>31</b>
2.1. Немного о хэшировании паролей. Протоколы SSH, GN3, Wireshark, PuTTY .....	31
2.2. Практикум по организации домашнего стенда для изучения шифрованного сетевого канала .....	43
2.3. Более простой пример шифрованного сетевого канала .....	55
<b>Глава 3. Анонимность в сети .....</b>	<b>58</b>
3.1. Тор для обеспечения анонимности в сети .....	58
3.2. Тор на смартфоне .....	62
3.3. Заключение о Тор .....	75
3.4. Использование прокси-серверов .....	75
<b>Глава 4. Взлом Wi-Fi-роутеров: мифы и реальность .....</b>	<b>79</b>
4.1. Способ первый .....	79
4.2. Способ второй .....	100
4.3. Другие способы. Вывод .....	104
<b>Глава 5. Заключительный цикл злоумышленника, или что делает хакер после взлома Wi-Fi-сети .....</b>	<b>106</b>
5.1. Что делает хакер для продолжения проникновения .....	106
5.2. Metasploit Framework: работа из командной строки .....	133
5.3. Инструментарий для смартфона, или мобильный хакинг .....	142
5.4. Лабораторная работа для апробирования стандартных средств операционной системы .....	192

---

<b>Глава 6. Программы для взлома игрушек — вовсе не игрушки.....</b>	<b>197</b>
<b>Глава 7. Радужные таблицы, или не все в радужном цвете .....</b>	<b>206</b>
7.1. Практическое применение хакером радужных таблиц для взлома .....	206
7.2. Генерация радужных таблиц в домашних условиях.....	223
7.3. Область применения радужных таблиц. Методика взлома пароля с использованием хэш-функции из базы Active Directory сервера .....	230
<b>Заключение.....</b>	<b>239</b>