Подробное руководство по защите Вашей сети

Эта книга, получившая признание как всеобъемлющее практическое руководство по защите информации, займет достойное место в вашей профессиональной библиотеке по безопасности. Бестселлер «Защита от хакеров корпоративных сетей» продемонстрирует Вам, что единственный способ остановить хакера — думать как он.

1 Законы безопасности
Узнайте об авторских методики исследования проблем безопасности и обнаружения брешей в защите при аудите или проектировании системы.

2 Семь категорий атак
Убедитесь на наглядных примерах, как отказ в обслуживании, утечка информации, доступ к файловым системам и базам данных, дезинформация, удаленное выполнение кода и получение статуса привилегированного пользователя может принести вам реальные неприятности.

3 Предотвращение прослушивания
Познакомьтесь, как сравнение программ, библиотек или файлов до или после выполнения некоторых действий может повлиять на данные в Вашей сети.

4 Стандартные алгоритмы шифрования
Проверьте, насколько защищены ваши зашифрованные файлы и надежны пароли.

5 Последовательности уязвимостей
Узнайте о новейших приемах хакеров.

6 Сессии пиратских подключений
Прочтите о расширенном применении мониторинга сетевых коммуникаций и атаках типа «злоумышленник посередине» (man-in-the-middle).

7 Туннелирование сетевого траффика
Познакомьтесь с механизмами создания враждебного сетевого окружения для перехвата сетевого трафика. OpenSSH как один из лучших современных пакетов для создания сквозных туннелей.

8 Защита Вашего оборудования
Создание продуктов с встроенными механизмами защиты: сопротивление, доказательство вторжения, поиск уязвимостей, обнаружение и ответная реакция. один из лучших современных пакетов для создания сквозных туннелей.

ISBN 598453015-5
9 785984 530156

SYNGRESS®
ДМК ПРЕСС ИЗДАТЕЛЬСТВО
www.dmk.ru
www.abook.ru
Академия АйТи
www.academy.it.ru
www.infobooks.ru

ЗАЩИТА ОТ ХАКЕРОВ КОРПОРАТИВНЫХ СЕТЕЙ

ЗАЩИТА ОТ ХАКЕРОВ КОРПОРАТИВНЫХ СЕТЕЙ

Академия АйТи
SYNGRESS®

SYNGRESS®

ЗАЩИТА ОТ ХАКЕРОВ

КОРПОРАТИВНЫХ СЕТЕЙ

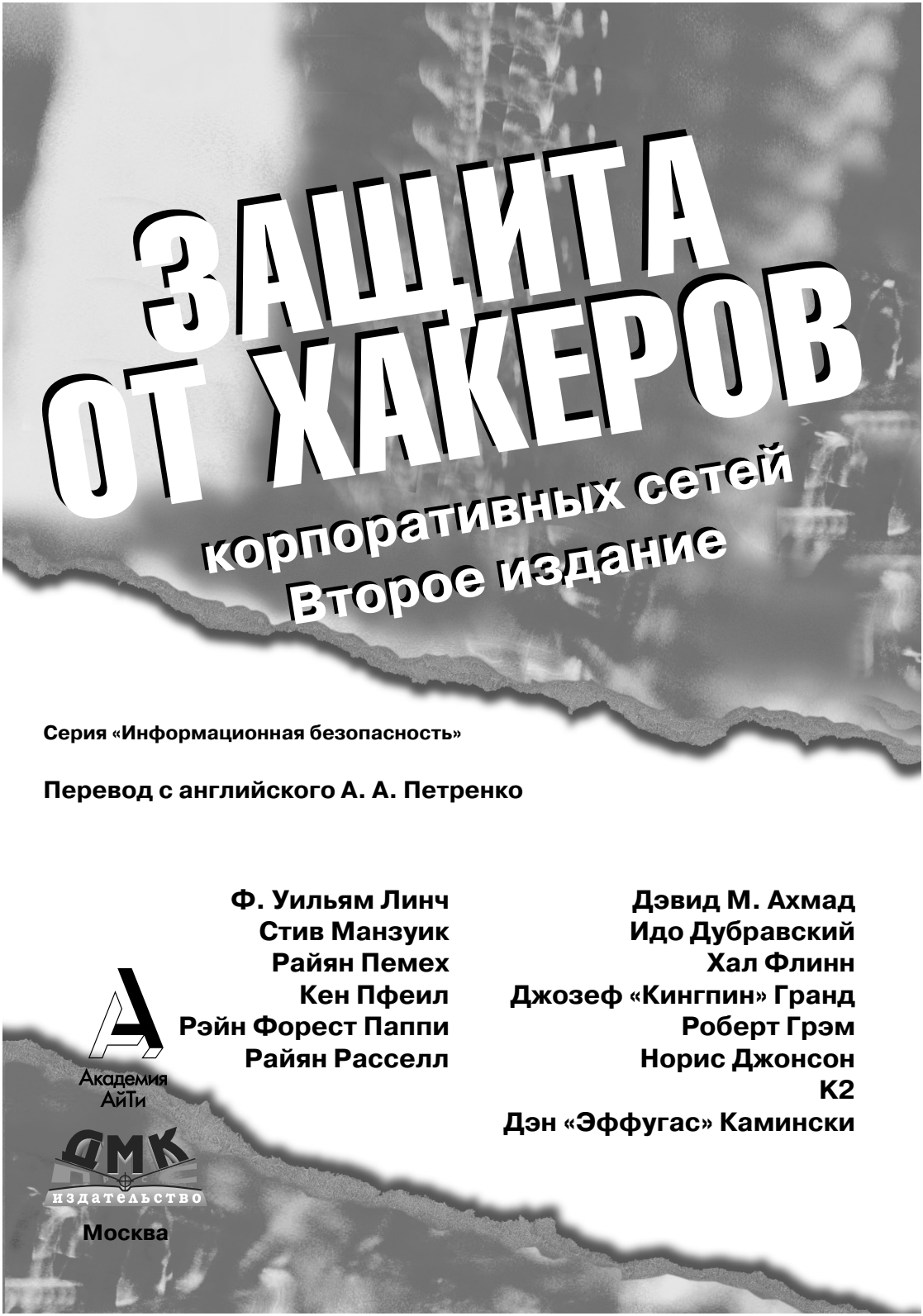
ВТОРОЕ ИЗДАНИЕ

Единственный способ остановить хакера — думать как он

Ф. Уильям Линч
Стив Манзуик
Райян Пемех
Кен Пфеил
Рэйн Форест Паппи
Райян Расселл
Дэн «Эффугас» Камински
Дэвид М. Ахмад
Идо Дубравский
Хал Флинн
Джозеф «Кингпин» Гранд
Роберт Грэм
Норис Джонсон
К2

Академия АйТи

ДМК ПРЕСС ИЗДАТЕЛЬСТВО



ЗАЩИТА ОТ ХАКЕРОВ

корпоративных сетей
Второе издание

Серия «Информационная безопасность»

Перевод с английского А. А. Петренко

Ф. Уильям Линч
Стив Манзуик
Райян Пемех
Кен Пфеил
Рэйн Форест Паппи
Райян Расселл

Дэвид М. Ахмад
Идо Дубравский
Хал Флинн
Джозеф «Кингпин» Гранд
Роберт Грэм
Норис Джонсон
K2
Дэн «Эффугас» Каминski

Академия АйТи

ДМК издательство

Москва

УДК 004.056
ББК 32.973.202
А95

А95 **Дэвид М. Ахмад, Идо Дубравский, Хал Флинн, Джозеф «Кингпин» Гранд, Роберт Грэм, Норис Джонсон, К2, Дэн «Эффугас» Камински, Ф. Уильям Линч, Стив Манзуик, Райян Пемех, Кен Пфеил, Рэйн Форест Паппи, Райян Расселл**
Защита от хакеров корпоративных сетей: Пер. с англ. А. А. Петренко. Второе издание. – М.: Компания АйТи; ДМК-Пресс. – 864 с.: ил. (Серия «Информационная безопасность»).

ISBN 5-98453-015-5

В книге рассматривается современный взгляд на хакерство, реинжиниринг и защиту информации. Авторы предлагают читателям список законов, которые определяют работу систем компьютерной безопасности и как можно применять эти законы в хакерских технологиях. Описываются типы атак и возможный потенциальный ущерб, который они могут нанести компьютерным системам. В книге широко представлены различные методы хакинга, такие как поиск различий, методы распознавания шифров, основы их вскрытия и схемы кодирования. Освящаются проблемы безопасности, возникающие в результате непредсказуемого ввода данных пользователем, методы использования машинно-ориентированного языка, возможности применения мониторинга сетевых коммуникаций, механизмы туннелирования для перехвата сетевого трафика. В книге представлены основные сведения о хакерстве аппаратных средств, вирусах, троянских конях, и червях. В этой книге читатель узнает о методах, которые в случае неправильного их применения приведут к нарушению законодательства и связанным с этим последствиям.

Лучшая защита – это нападение. Другими словами, единственный способ остановить хакера заключается в том, чтобы думать как он. Эти фразы олицетворяют подход, который, по мнению авторов, позволит наилучшим образом обеспечить безопасность информационной системы.

УДК 004.056
ББК 32.973.202

ISBN 1-928994-70-9 (англ.) Copyright © by Singress Publishing, Inc.
ISBN 5-98453-015-5 (АйТи) © Перевод на русский язык. Компания АйТи
© Оформление, издание. ДМК-Пресс

Содержание

ŋqdqyǝʎ bɆ dǝdɆbʎɜǝ d ɐɔɑbɔʎ Ɉqdqʎqʎǝ̀

ŋqdpγeɣ þƐ dəpƐbɣɜe d ɕɑɑbɔɣ Ɉqdpɣqɣè