

УДК 004.056  
ББК 32.972.13  
М31

Масалков А. С.

М31 Особенности киберпреступлений: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.: ил.

**ISBN 978-5-97060-651-3**

Материал книги помогает разобраться в том, что обычно скрывается за терминами и шаблонными фразами «взлом электронной почты», «кибершпионаж» и «фишинг».

Автор старался показать информационную безопасность как поле битвы с трех сторон: со стороны преступного сообщества, использующего информационные технологии, со стороны законодательства и правоохранительной системы и со стороны атакуемого.

Основная идея состоит в том, чтобы доступно представить картину сегодняшней киберпреступности на актуальных примерах, включая применение фишинг-атак, но не ограничиваясь этим.

Приводимые методы атак подкрепляются примерами из реальной жизни. Углубленно разбираются механизмы получения незаконного доступа к учетным записям информационных ресурсов, в частности электронной почты. Акцентируется внимание на методе проведения фишинг-атак как наиболее эффективном на сегодняшний день инструменте получения паролей.

Фишинг рассматривается как универсальный инструмент, находящий свое проявление в различных мошеннических и хакерских комбинациях, как с технической, так и с юридической стороны.

Книга включает практический взгляд на механизмы, используемые киберпреступниками, а также процесс формирования судебного производства и методов расследования таких преступлений.

Материал дает возможность пересмотреть и адекватно оценивать риски, эффективность используемых систем защиты, выстроить политику безопасности в соответствии с реальностью. Приводятся советы по предотвращению кибератак и алгоритм первоначальных действий, которые необходимо предпринимать при наступлении инцидента и которые направлены на фиксацию следов, эффективное расследование и взаимодействие с правоохранительными органами.

**УДК 004.056  
ББК 32.972.13**

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-5-97060-651-3

© Масалков А. С., 2018  
© Оформление, издание, ДМК Пресс, 2018

# СОДЕРЖАНИЕ

<b>Введение</b> .....	<b>6</b>
<b>Глава 1. Хищение паролей методом фишинг-атак</b> .....	<b>20</b>
Методы несанкционированного получения пароля.....	20
Особенности фишинга.....	25
Виды фишинговых атак.....	26
Слепой фишинг.....	26
Целенаправленный фишинг.....	28
1.1. Как это происходит? Фишинг-атака со стороны пользователя на примере электронного почтового ящика.....	30
1.2. Роль социальной инженерии в фишинг-атаке.....	41
1.3. Фишинг изнутри. Анализ используемых для атаки инструментов.....	49
Схема взаимодействия с почтовым сервером.....	50
Три основные функции фишинг-движка.....	51
Демонстрация механизма функционирования фишинг-движков на локальном сервере.....	52
Фишинг-движок изнутри. Пример 1.....	55
Фишинг-движок изнутри. Пример 2.....	61
Фишинг-движок изнутри. Пример 3.....	64
Автоматическая проверка похищенного пароля.....	64
Фишинг-движок изнутри. Пример 4.....	67
Примеры интерфейсов.....	69
Доменные имена.....	73
Размещение фэйка на сервере.....	77
<b>Глава 2. Комбинированные атаки с использованием фишинга</b> .....	<b>79</b>
2.1. Подготовка к персонализированной фишинговой атаке. Некоторые специфические способы сбора информации.....	80
Определение браузера и операционной системы атакуемого.....	81
Определение IP-адресов атакуемого.....	85
Анализ служебных заголовков.....	86
2.2. Атака с использованием «заброса» вредоносных программ.....	87

## 4 СОДЕРЖАНИЕ

2.3. Атака с использованием маскировки под легальное программное обеспечение или файлы .....	100
Анализ зараженной системы.....	113
2.4. Атака на мобильные телефоны .....	115
<b>Глава 3. Особенности киберпреступлений .....</b>	<b>125</b>
3.1. Мистика киберпреступности .....	126
Незримое присутствие .....	128
Прочитанные и непрочитанные письма.....	129
Переписка с несуществующим адресатом .....	130
3.2. Характеристика киберпреступления, проблемы идентификации и трудности перевода .....	136
3.3. Доступность инструментов анонимной связи и управления ресурсами .....	144
3.3.1. Доступность анонимной связи и управления .....	146
3.3.2. Виртуальный хостинг, выделенный сервер, VPN.....	155
3.3.3. Инструменты управления финансами .....	163
<b>Глава 4. Противодействие и защита.....</b>	<b>168</b>
4.1. Правоохранительная система.....	168
4.2. Некоторые национальные особенности борьбы с киберпреступлениями.....	175
4.3. Традиционная защита и рыночные тенденции.....	185
4.4. Дешевые правила дорогого спокойствия. Советы по защите информации .....	190
Защита личных данных .....	190
Защита корпоративной информации.....	191
4.4.1. Реакция на инциденты .....	192
4.4.2. Обучение в форме учений, приближенных к реальности.....	193
4.4.3. Учет и контроль .....	195
4.4.4. Аудит и разбор полетов.....	196
4.4.5. Целесообразность автоматических операций.....	197
4.4.6. «Отголоски пиратства» .....	198
4.5. Что делать, если произошел инцидент.....	199
4.5.1. Изоляция системы .....	201
4.5.2. Изготовление клонов носителей информации.....	201
4.5.3. Проведение исследований и компьютерно-технических экспертиз.....	202
4.5.4. Обращение в правоохранительные органы .....	208
<b>Глава 5. Никакой мистики, только бизнес. Обзор черного рынка информационных услуг в России .....</b>	<b>210</b>
Первый блок.....	211
Второй блок.....	212
Третий блок.....	213
Четвертый блок.....	214
Пятый блок.....	215
<b>Заключение.....</b>	<b>217</b>
<b>Предметный указатель .....</b>	<b>221</b>