ОГЛАВЛЕНИЕ

Введение 3

1. Классификация и риск-анализ разновидностей атак деструктивной социальной инженерии 6

1.1. Методика классификации атак по материалам IC3 .. 6

1.2. Сравнительный анализ многообразия атак по их частоте и наносимому ущербу 13

2. Атаки категории «Фишинг и спуфинг» 20

2.1. Временная динамика развития атак категории «Фишинг и спуфинг» 20

2.2. Сценарии реализации атак категории «Фишинг и спуфинг» 21

2.3. Особенности политики обеспечения безопасности при защите от атак категории «Фишинг и спуфинг» 26

3. Атаки категории «Компрометация деловой переписки» 34

3.1. Временная динамика развития атак категории «Компрометация деловой переписки» 34

3.2. Сценарии реализации атак категории «Компрометация деловой переписки» 35

3.3. Особенности политики обеспечения безопасности при защите от атак категории «Компрометация деловой переписки» 39

4. Атаки категории «Мошенничество под видом технической поддержки» 45

4.1. Временная динамика развития атак категории «Мошенничество под видом технической поддержки» 45

4.2. Сценарии реализации атак категории «Мошенничество под видом технической поддержки» 46

4.3. Особенности политики обеспечения безопасности при защите от атак категории «Мошенничество под видом технической поддержки» 51
5. Атаки категории «Инвестиционное мошенничество» 57
5.1. Временная динамика развития атак категории «Инвестиционное мошенниче-ство» 57
5.2. Сценарии реализации атак категории «Инвестиционное мошенничество» 58
5.3. Особенности политики обеспечения безопасности при защите от атак категории «Инвестиционное мошенничество» 63
6. Атаки категории «Имитация государственных органов» 68
6.1. Временная динамика развития атак категории «Имитация государственных органов» 68
6.2. Сценарии реализации атак категории «Имитация государственных органов» 69
6.3. Особенности политики обеспечения безопасности при защите от атак категории «Имитация государственных органов» 73
7. Атаки категории «Мошенничество при трудоустройстве» 78
7.1. Временная динамика развития атак категории «Мошенничество при трудоустройстве» 78
7.2. Сценарии реализации атак категории «Мошенничество при трудоустройстве» 79
7.3. Особенности политики обеспечения безопасности при защите от атак категории «Мошенничество при трудоустройстве» 83
8. Атаки категории «Мошенничество с доверительными отношениями» 88
8.1. Временная динамика развития атак категории «Мошенничество с доверитель-ными отношениями» 88
8.2. Сценарии реализации атак категории «Мошенничество с доверительными от-ношениями» 89
8.3. Особенности политики обеспечения безопасности при защите от атак категории «Мошенничество с доверительными отношениями» 93
9. Атаки категории «Мошенничество в сфере недвижимости» 98

9.1. Временная динамика развития атак категории «Мошенничество в сфере недвижимости» 98
9.2. Сценарии реализации атак категории «Мошенничество в сфере недвижимости» 99
9.3. Особенности политики обеспечения безопасности при защите от атак категории «Мошенничество в сфере недвижимости» 103
10.Атаки категории «мошенничество с кредитными картами/чеками» 108
10.1. Временная динамика развития атак категории «Мошенничество с кредитными картами/чеками» 108
10.2. Сценарии реализации атак категории «Мошенничество с кредитными карта-ми/чеками» 109
10.3. Особенности политики обеспечения безопасности при защите от атак категории «Мошенничество с кредитными картами/чеками» 117
11. Атаки категории «Мошенничество связанное с «Неоплатой/непоставкой» 118
11.1. Временная динамика развития атак категории «Неоплата/непоставка» 118
11.2. Сценарии реализации атак категории «Неоплата/непоставка» 119
11.3. Особенности политики обеспечения безопасности при защите от атак категории «Неоплата/непоставка» ... 125
12. Атаки категории «Мошенничество, связанное с переплатой денежных средств» 131
12.1. Временная динамика развития атак категории «Переплата» 131
12.2. Сценарии реализации атак категории «Переплата» .. 132
12.3. Особенности политики обеспечения безопасности при защите от атак категории «Переплата» 135
13. Атаки категории «Мошенничество, связанное с «авансовыми платежами/предоплатой» и «Лотереями/розыгрышами/наследством» 139
13.1. Временная динамика развития атак категории «Авансовые платежи/предоплата» и «Лотереи/розыгрыши/наследство» 140
13.2. Сценарии реализации атак категории «Авансовые платежи/предоплата» и «Лотереи/розыгрыши/наследство» 142

13.3. Особенности политики обеспечения безопасности при защите от атак категории «Авансовые платежи/предоплата» и «Лотереи/розыгрыши/наследство» 151
14. Атаки категории «Мошенничество, связанное с вымогательством» 152
14.1. Временная динамика развития атак категории «Вымогательство» 152
14.2. Сценарии реализации атак категории «Вымогательство» 153
14.3. Особенности политики обеспечения безопасности при защите от атак категории «Вымогательство» 158
Заключение 163
Литература 167

Серия «Теория сетевых войн»
Выпуск 12

Учебное издание

Остапенко Григорий Александрович,
Линец Александр Александрович, **Калашников** Андрей Олегович,
Остапенко Александр Алексеевич, **Мирошниченко** Татьяна Юрьевна

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ:
ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА

Под редакцией академика РАН Д. А. Новикова

Работа выполнена при частичной поддержке РФФИ (проект 18-29-22042), а также в рамках проекта «Безопасный Интернет» (рег. № АААА-А18-118050700061-7)

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника В. Г. Ситникова

Адрес издательства в Интернет WWW.TECHBOOK.RU

Подписано в печать 02.11.2026. Формат 60×90/16. Усл. печ. л. 11,25
Печать цифровая. Изд. №271233. Тираж 500 экз. (1-й завод – 50 экз.)
ООО «Научно-техническое издательство «Горячая линия – Телеком»