# ОГЛАВЛЕНИЕ

**Введение.....3**

**Раздел 1. Современные основы информационной безопасности.....6**

Глава 1. Информационные факторы угроз личности, обществу, государству и субъектам хозяйствования .....6

*§ 1.1. Оценка состояния современных информационных факторов угроз личности, обществу, государству и субъектам хозяйствования..... 6*

*§ 1.2. Понятие каналов утечки информации ..... 12*

*§ 1.3. Традиционные каналы утечки информации ..... 14*

*§ 1.4. Каналы утечки информации из СКТ..... 24*

*§ 1.5. Понятие информационных войн и информационно-программного оружия ..... 36*

*§ 1.6. Основные направления обеспечения компьютерной безопасности..... 38*

Глава 2. Правовое обеспечение компьютерной безопасности .....42

*§ 2.1. Понятие правового обеспечения компьютерной безопасности. Информационное законодательство Республики Беларусь и Российской Федерации..... 42*

*§ 2.2. Уголовное преследование за совершение компьютерных преступлений в Российской Федерации и Республике Беларусь..... 56*

*§ 2.3. Зарубежный опыт правового обеспечения компьютерной безопасности ..... 75*

Глава 3. Инженерно-техническое обеспечение компьютерной безопасности .....83

*§ 3.1. Технические средства противодействия ТСВР ..... 84*

*§ 3.2. Физические средства защиты ..... 96*

*§ 3.3. Аппаратные, программные и программно-аппаратные средства защиты..... 98*

*§ 3.4. Криптографические методы защиты ..... 101*

Глава 4. Организационное обеспечение компьютерной безопасности .....102

*§ 4.1. Организационно-административные мероприятия ..... 103*

*§ 4.2. Организационно-технические и организационно-экономические мероприятия..... 106*

**Раздел 2. Криминалистическая характеристика компьютерных преступлений .....110**

Глава 1. Понятие криминалистической характеристики компьютерных преступлений .....111

Глава 2. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.....116

Глава 3. Способы совершения компьютерных преступлений.....125

*§ 3.1. Понятие способа совершения компьютерного преступления ..... 125*

*§ 3.2. Классификация способов совершения компьютерных преступлений ..... 129*

Глава 4. Особенности образования следов по делам о компьютерных преступлениях.....143

*§ 4.1. Понятие и классификация следов компьютерных преступлений ..... 143*

*§ 4.2. Регистрационные файлы операционных систем..... 148*

*§ 4.3. Регистрационные файлы СУБД ..... 159*

Глава 5. Личностная характеристика преступника, совершающего компьютерные преступления.....161

Глава 6. Особенности обстановки совершения компьютерных преступлений.....167

**Раздел 3. Использование данных криминалистической характеристики компьютерных преступлений для обнаружения, фиксации и изъятия их следов.....171**

Глава 1. Характеристика инструментальных модулей, необходимых для обнаружения следов компьютерных преступлений .....171

Глава 2. Осмотр места происшествия по делам о компьютерных преступлениях .....178

*§ 2.1. Особенности применения специальных знаний для обнаружения следов компьютерных преступлений в процессе осмотра места происшествия по делам о компьютерных преступлениях..... 181*

*§ 2.2. Особенности подготовительного этапа осмотра места происшествия по делам о компьютерных преступлениях ..... 186*

*§ 2.3. Особенности осмотра помещений, зданий, кабельного хозяйства при осмотре места происшествия по делам о компьютерных преступлениях..... 188*

*§ 2.4. Особенности криминалистического исследования компьютерных систем, их сетей и периферийного оборудования непосредственно на месте происшествия* ... *190*

*§ 2.5. Криминалистическое исследование операционных систем* ... *193*

*§ 2.6. Криминалистическое исследование СУБД* ... *200*

Глава 3. фиксация и изъятие следов компьютерных преступлений ... 204

*§ 3.1. Сущность фиксации следовой информации по делам о компьютерных преступлениях* ... *204*

*§ 3.2. Особенности фиксации следовой информации о попытках зондирования компьютерных систем или ведения радиоэлектронной разведки* ... *205*

*§ 3.3. Особенности фиксации следовой информации о действии вредоносных программ в ходе осмотра компьютерных систем и их сетей* ... *206*

*§ 3.4. Особенности фиксации следовой информации при проведении аудита компьютерных систем в ходе осмотра компьютерных систем и их сетей* ... *210*

*§ 3.5. Особенности изъятия следов компьютерных преступлений* ... *215*

Глава 4. Проведение компьютерно-технической экспертизы (КТЭ) ... 218

*§ 4.1. Классификация КТЭ* ... *218*

*§ 4.2. Компьютерно-сетевая экспертиза* ... *220*

*§ 4.3. Комплексная компьютерно-техническая и технико-криминалистическая экспертиза документов, изготовленных на матричных игольчатых принтерах* ... *223*

Глава 5. Особенности выдвижения и проверки следственных версий по делам о компьютерных преступлениях ... 229

**Общие выводы (заключение) ... 235**

**Приложение 1.** ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ... 236

I. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ ... 237

*1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение* ... *237*

*2. Виды угроз информационной безопасности Российской Федерации* ... *240*

*3. Источники угроз информационной безопасности Российской Федерации* ..... *244*

*4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению* ..... *245*

II. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ..... 249

*5. Общие методы обеспечения информационной безопасности Российской Федерации* ..... *249*

*6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни* ..... *252*

*7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности* ..... *267*

III. ОСНОВНЫЕ ПОЛОЖЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПЕРВООЧЕРЕДНЫЕ МЕРОПРИЯТИЯ ПО ЕЕ РЕАЛИЗАЦИИ ..... 268

*8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации* ..... *268*

*9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации* ..... *272*

IV. ОРГАНИЗАЦИОННАЯ ОСНОВА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ..... 273

*10. Основные функции системы обеспечения информационной безопасности Российской Федерации* ..... *273*

*11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации* ..... *274*

**Приложение 2.** ПРОЕКТ ЗАКОНА РЕСПУБЛИКИ БЕЛАРУСЬ «О ЗАЩИТЕ ИНФОРМАЦИИ» ..... 277

**Приложение 3.** КОНЦЕПЦИЯ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ..... 300

Библиография ..... 325