

ОГЛАВЛЕНИЕ

Вместо предисловия. Киберпреступность
и киберполиция не имеют национальных границ 9

Введение 16

Глава I ИННОВАЦИИ В ПОЛИЦИИ

§ 1. Общие положения	19
Прогнозирование и стратегическое планирование	22
Технологии	22
Партнерство и сотрудничество	23
Законодательная работа	23
Методы и подходы к инновациям	24
§ 2. Дроны: угрозы, инструмент, средства доказательства.	26
Дроны в руках преступников и полиции	27
Дроны как инструмент полиции	30
Развитие дронов	33
§ 3. Искусственный Интеллект (ИИ)	35
Угрозы ИИ.	37
Потенциал использования ИИ правоохранительными органами.	42
§ 4. Робототехника и киберполиция	43
Промышленные роботы	45
Сервисные роботы	46
Социальные роботы	47

Военные роботы.	47
Беспилотные автомобили.	48
Потенциальные возможности робототехники.	49
Осмотр подозрительных предметов.	52
Автоматизация анализа доказательств.	53
Роботы для уличных патрулей.	53
Преступники тоже используют роботов.	54
§ 5. Печать — 3D и 4D	56
3D-печатное огнестрельное оружие	59
Правовые подходы к напечатанному огнестрельному оружию.	62
3D-печать и интеллектуальная собственность	64
Потенциальные возможности для полиции	64
3D-печать. Доказательства	64
3D-печать для копирования отпечатков	65
3D-печать для уголовных расследований	65
3D-печать для повышения безопасности полицейских	66
Направления прогресса для полицейских органов	67

Глава II КИБЕРПОЛИЦИЯ И КИБЕРПРЕСТУПНОСТЬ

§ 1. Международно-правовое определение киберпреступности	69
§ 2. Киберпреступность.	85
Специализированное вирусное программное обеспечение	90
Атаки на критическую инфраструктуру	91
Кражи данных и сетевые атаки	92
Крупнейшие в истории хищения данных.	93
Масштабы DDoS-атак увеличиваются.	95
Инструменты DDOS-атак легко доступны	97
Взлом сайтов. Низкая эффективность и разнообразная мотивированность	97
§ 3. Смычка киберпреступности и кибертерроризма.	97
Террористические группы в цифровом подполье	98
Неэффективность террористических кибератак	99

Джихадистские сети экспериментируют с криптовалютами	100
§ 4. Онлайн сексуальная эксплуатация детей	102

Глава III
АНОНИМНЫЕ СЕТИ, ТЕНЕВОЙ ИНТЕРНЕТ
И КРИМИНАЛЬНАЯ ОНЛАЙН-ТОРГОВЛЯ

§ 1. Анонимные сети и теневой интернет	114
Интернет	116
Темный «интернет»	119
Сеть Tor	120
§ 2. Типы преступлений в Darknet	122
Криминальная торговля	122
Преступление как услуга (CaaS)	122
Жестокое обращение с детьми	123
Экстремизм	123
Нелегальные финансовые системы	124
§ 3. Криминальная онлайн-торговля	125
Darknet-рынки	126
Активизация вторичных рынков	128
Наркоторговля продолжает доминировать в Darknet	128
Рынки Darknet утрачивают значимость для киберпреступников	129
Торговля контрафактными товарами	130
Торговля оружием процветает в Darknet	131
Украденные данные — главный товар в сети Darknet	132

Глава IV
КИБЕРПРЕСТУПЛЕНИЯ И ТЕЛЕКОММУНИКАЦИИ

§ 1. Понятие и история развития телекоммуникаций	133
Типы современных сетей связи	136
5G порождает ряд новых острых проблем для правоохранительных органов	139
Ряд понятий, используемых в современных телекоммуникациях	139
Законодательные ограничения	142

§ 2. Сущности современного мира телекоммуникаций	143
Умные города	143
Умные предприятия	145
Умный дом.	146
Робот (устройство)	146
Смарткар, или автономный автомобиль	146
Смартфон (персональное устройство)	147
Технологии проникновения коммуникаций:	
Фемто- и пиктосоты	147
§ 3. Виды мошенничества в сфере телекоммуникаций	148
Мошенничества с использованием доступа	
к абонентским терминалам	149
Доступ мошенников к личному кабинету клиента	153
Доступ к инфраструктуре телекоммуникационных	
операторов	153
Новые виды мошенничеств в телекоммуникационной	
сфере	154
Новое поколение сетей — новые угрозы	157
Физические атаки на телекоммуникационную	
инфраструктуру	160
Платежные мошенничества с использованием	
телекоммуникационной инфраструктуры	
и социального инжиниринга.	161
§ 4. Мошенничество в сфере финансовых технологий	167

Глава V

КИБЕРПОЛИЦИЯ И ИНТЕРНЕТ ВЕЩЕЙ

§ 1. Понятие интернета вещей.	176
§ 2. Интернет вещей — риски и угрозы	178
§ 3. Основные направления преступности	
с использованием IoT	187
§ 4. Киберполиция	
на защите интернета вещей	192

Глава VI

КИБЕРПОЛИЦИЯ ДЛЯ УМНОГО ГОРОДА

§ 1. Особенности умного города	205
§ 2. Риски умного города	208

§ 3. Киберполиция против новых рисков	210
Государственно-частное партнерство по обеспечению безопасности умного города	214

Глава VII
КИБЕРПОЛИЦИЯ И ЦИФРОВАЯ ВАЛЮТА

§ 1. Цифровые валюты: определение, характеристики и пользователи.	218
Ключевые определения	218
Типы криптовалют, их особенности и пользователи	219
Примеры использования криптоактивов криминалом	226
Централизованные виртуальные деньги	229
§ 2. Бэкграунд усилий по предотвращению отмывания денег и финансирования организованной преступности и терроризма через криптовалюты	231
FATF и новые технологии	234
Реакция ЕС	238
Оценка рисков использования террористами и киберкриминалом виртуальных валют	243
Риски за пределами терроризма и организованной преступности	249
Конвергенция киберкриминала и терроризма	261
§ 3. Юридические и регуляторные механизмы борьбы с блокчейн-преступностью	264
Саморегулирование	276
Рекомендации правоохранительным и законодательным органам	278
Заключение	283