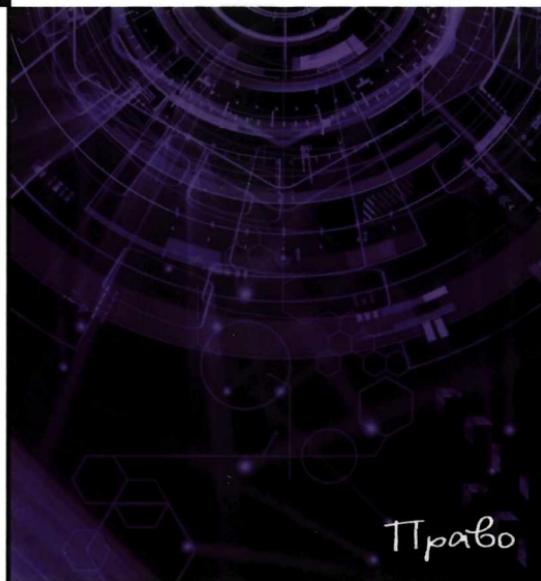


ББК  
67.408  
Р 893

НАУЧНАЯ МЫСЛЬ



*E.A. Русскевич*

УГОЛОВНОЕ ПРАВО  
И «ЦИФРОВАЯ  
ПРЕСТУПНОСТЬ»

*проблемы и решения*



НАУЧНАЯ МЫСЛЬ

СЕРИЯ ОСНОВАНА В 2008 ГОДУ

Е.А. РУССКЕВИЧ

# УГОЛОВНОЕ ПРАВО И «ЦИФРОВАЯ ПРЕСТУПНОСТЬ»

## ПРОБЛЕМЫ И РЕШЕНИЯ

МОНОГРАФИЯ

*2-е издание, переработанное и дополненное*

Электронно-  
Библиотечная  
Система  
**znanium.com**

Москва  
ИНФРА-М  
2023

УДК 343(075.4)  
ББК 67.408.125  
Р89

Русскевич Е.А.

Р89

Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е.А. Русскевич. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2023. — 351 с. — (Научная мысль). — DOI 10.12737/1840963.

ISBN 978-5-16-017297-2 (print)

ISBN 978-5-16-109835-6 (online)

Монография посвящена комплексу теоретико-прикладных проблем приспособления отечественного механизма уголовно-правовой охраны к «цифровизации» преступности в условиях становления информационного общества. Наряду с общетеоретическими вопросами глубокому анализу подвергаются зарубежное уголовное законодательство и положения норм международного права. В работе представлена уточненная уголовно-правовая характеристика преступлений в сфере компьютерной информации, в том числе новеллы российского уголовного законодательства — неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274<sup>1</sup> УК РФ), разработаны предложения по дифференциации уголовной ответственности за посягательства на безопасность компьютерных данных и систем, выработаны научно обоснованные рекомендации по квалификации.

Во втором издании отдельно проработаны вопросы дифференциации уголовной ответственности за цифровые преступления средствами Общей и Особенной части УК РФ. Проведен анализ проблем квалификации преступлений в сфере компьютерной информации, а также иных преступлений, совершаемых с использованием информационно-коммуникационных технологий, за пределами главы 28 УК РФ. С учетом полученных результатов представлен проект постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях в сфере компьютерной информации».

Предназначена для научных сотрудников, преподавателей, практикующих юристов, студентов и аспирантов юридических вузов и факультетов.

554081

УДК 343(075.4)  
ББК 67.408

БИБЛИОТЕКА  
ФГАОУ ВО  
Сибирский федеральный  
университет

© Русскевич Е.А., 2019

ISBN 978-5-16-017297-2 (print)

ISBN 978-5-16-109835-6 (online)

© Русскевич Е.А., 2021,  
с изменениями

# Оглавление

Благодарности .....	3
Предисловие.....	4

## РАЗДЕЛ I ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ «ЦИФРОВОЙ ПРЕСТУПНОСТИ»

<b>Глава 1. УГОЛОВНОЕ ПРАВО В УСЛОВИЯХ ЦИФРОВОЙ РЕАЛЬНОСТИ: ПОСТАНОВКА ПРОБЛЕМЫ .....</b>	<b>7</b>
1.1. Механизм уголовно-правовой охраны в эпоху информационного общества .....	7
1.2. Преступления, совершаемые с использованием информационно- коммуникационных технологий («цифровые преступления»): проблемы интерпретации .....	23

<b>Глава 2. МЕЖДУНАРОДНО-ПРАВОВЫЕ СТАНДАРТЫ И СРАВНИТЕЛЬНО- ПРАВОВОЙ АНАЛИЗ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ .....</b>	<b>40</b>
--	-----------

2.1. Международно-правовые стандарты противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий .....	40
2.2. Сравнительно-правовой анализ уголовного законодательства зарубежных стран об ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий .....	48

## РАЗДЕЛ II ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» КАК ОСНОВНОЕ НАПРАВЛЕНИЕ МОДЕРНИЗАЦИИ ОТЕЧЕСТВЕННОГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА

<b>Глава 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ДИФФЕРЕНЦИАЦИИ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» .....</b>	<b>101</b>
---	------------

<b>Глава 2. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» СРЕДСТВАМИ ОБЩЕЙ ЧАСТИ УГОЛОВНОГО ПРАВА.....</b>	<b>112</b>
--	------------

2.1. Дифференциация ответственности за «цифровые преступления» средствами института преступления .....	112
2.2. Дифференциация ответственности за «цифровые преступления» средствами института наказания .....	124

<b>Глава 3. ДИФФЕРЕНЦИАЦИЯ ОТВЕТСТВЕННОСТИ ЗА «ЦИФРОВЫЕ ПРЕСТУПЛЕНИЯ» СРЕДСТВАМИ ОСОБЕННОЙ ЧАСТИ УГОЛОВНОГО ПРАВА .....</b>	<b>135</b>
3.1. Дифференциация ответственности за компьютеризированные преступления ....	135
3.2. Дифференциация ответственности за преступления в сфере компьютерной информации (компьютерные преступления).....	149
 <b>РАЗДЕЛ III</b>	
<b>ЮРИДИЧЕСКИЙ АНАЛИЗ И ПРОБЛЕМЫ КВАЛИФИКАЦИИ «ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ»</b>	
<b>Глава 1. ЮРИДИЧЕСКИЙ АНАЛИЗ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ).....</b>	<b>179</b>
1.1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).....	179
1.2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).....	208
1.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ст. 274 УК РФ) .....	222
1.4. Неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274 <sup>1</sup> УК РФ) .....	236
<b>Глава 2. ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ .....</b>	<b>245</b>
2.1. Проблемы квалификации преступлений в сфере компьютерной информации (компьютерных преступлений).....	245
2.2. Проблемы квалификации компьютеризированных преступлений .....	269
2.3. Проблемы квалификации мошенничества в сфере компьютерной информации (ст. 159 <sup>6</sup> УК РФ) .....	291
2.4. Проблемы квалификации преступлений, совершаемых с использованием, в отношении и по поводу цифровых финансовых активов (криптовалют) .....	314
<b>Заключение.....</b>	<b>333</b>
<b>Библиографический список .....</b>	<b>336</b>
<b>Приложение.</b> Постановление Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях в сфере компьютерной информации» (проект).....	340

## **Благодарности**

Эта книга не появилась бы на свет без активной поддержки и участия этих прекрасных людей. Я хотел бы поблагодарить:

**Любовь Русскевич**, мою любимую жену, которая терпела мое физическое и умственное отсутствие в период работы над монографией и поддерживала меня на всем пути;

**Андрея Петровича Дмитренко**, доктора юридических наук, профессора, моего научного консультанта – за помощь в работе и поддержку;

**Николая Григорьевича Кадникова**, доктора юридических наук, профессора – за структурные правки и общие советы;

**Олега Валентиновича Зиборова**, первого заместителя начальника Московского университета МВД России имени В.Я. Кикотя, доктора юридических наук, доцента – за поддержку на всех этапах проведения исследования и написания книги;

**Михаила Михайловича Дайшутова**, начальника кафедры уголовного права Московского университета МВД России имени В.Я. Кикотя, кандидата юридических наук, доцента – за помощь в работе и поддержку;

**Игоря Геннадьевича Чекунова**, заместителя генерального директора по юридическим вопросам и безопасности компании «Лаборатория Касперского», кандидата юридических наук – за исключительные знания и опыт, переданные как в режиме онлайн, так и при личном общении;

**Владимира Владимировича Гончара**, кандидата юридических наук, доцента – за его дружбу и поддержку;

**Александра Юрьевича Решетникова**, кандидата юридических наук, доцента – за его дружбу и честный отзыв;

**всех участников «Кибергруппы»** Московского университета МВД России имени В.Я. Кикотя – за обмен знаниями, творческую атмосферу и сотрудничество;

**команду издательства «ИНФРА-М»** – за их энтузиазм, скрупулезный и творческий подход к работе.

Выражаю глубокую благодарность **Ильдару Рустамовичу Бегишеву, Сергею Викторовичу Борисову, Людмиле Александровне Букалевой, Виктору Ивановичу Динеке, Марине Александровне Ефремовой, Валерию Александровичу Жабскому, Артему Владимировичу Иванчину, Нодару Шотаевичу Козаеву, Станиславу Львовичу Нуделю, Константину Викторовичу Ображиеву, Роману Борисовичу Осокину, Александру Михайловичу Плещакову, Юрию Евгеньевичу Пудовочкину, Элине Леонидовне Сидоренко, Павлу Сергеевичу Яни, Борису Викторовичу Яцененко** за поддержку, критику, сотрудничество и обмен знаниями.

## Предисловие

*Посвящается моему учителю,  
заслуженному деятелю науки РФ,  
доктору юридических наук, профессору  
Ветрову Николаю Ивановичу*

На протяжении всей истории человеческая цивилизация подвергалась фундаментальным изменениям благодаря информации. Возникновение письменности, появление книгопечатания, а затем и первых технических средств коммуникации (телефона, телеграфа, радио и телевидения) оказали самое глубокое воздействие как на отдельного человека, так и на все сферы общественной жизни и государство. Появление электронно-вычислительных машин и распространение сети «Интернет» ознаменовало переход человечества уже в цифровую эпоху. Современный человек стал частью информационного (цифрового) общества, в котором его повседневная жизнедеятельность все более связана с компьютерами, сетевыми ресурсами и данными.

Сложно переоценить значение высокотехнологичных средств коммуникации в решении глобальных вызовов и угроз современного мира. Так, остановить атипичную пневмонию во многом стало возможным благодаря Интернету. Через несколько дней после вспышки смертельной эпидемии Всемирная организация здравоохранения (ВОЗ) запустила защищенный сайт, на котором проводились видеоконференции по проблеме, осуществлялся обмен рентгеновскими снимками легких, на основе чего был разработан протокол диагностики вместе с рекомендациями по карантину инфицированных пациентов. Несмотря на то что атипичная пневмония по длительности инкубационного периода, легкости распространения и смертности существенно превосходила известную эпидемию испанского гриппа<sup>1</sup>, пострадало от нее лишь 8422 человека<sup>2</sup>.

Вместе с тем стремительно развивающаяся архитектура виртуального пространства не только качественно улучшает нашу жизнь,

<sup>1</sup> С 1918 по 1920 г. около трети населения мира (полмиллиарда человек) заразилось смертельной формой гриппа, унесшей около 50 миллионов жизней. См.: Jeffery Taubenberger, David Morens. 1918 Influenza: the Mother of all pandemics // Emerging infections diseases. 2006. № 12.

<sup>2</sup> World Health Organization, SARS: How a global epidemic was stopped (Geneva: WHO Press, 2006).

но и параллельно с этим генерирует новые риски и угрозы. Негативным следствием глобальной информатизации явилось появление не только нового вида преступлений (преступлений в сфере компьютерной информации, как их принято именовать в отечественной уголовно-правовой доктрине), но и существенное изменение облика преступности в целом, которая в связи с использованием информационно-коммуникационных технологий приобрела несвойственные ей ранее признаки: экстерриториальность, гипертаргетированность, мультиплективность и др.

С одной стороны, ситуация мимикрирования преступности вполне типична, а такое ее свойство как историческая изменчивость знакомо любому специалисту в области криминологии. Вместе с тем также известно и то, что качественное изменение преступности, как правило, обусловлено серьезными социально-экономическими преобразованиями. Однако с преступностью нового поколения ситуация несколько иная. Их возникновению и продуцированию способствовали иные факторы.

Несмотря на весьма активное обсуждение этой проблемы, использование информационно-коммуникационных технологий в преступных целях в последние годы по-прежнему является серьезным вызовом как для правоохранительных, так и законодательных органов. Жертвами преступлений, совершаемых с использованием информационно-коммуникационных технологий, ежегодно становятся миллионы людей и организаций, а также органы власти конкретных государств.

Вместе с ведущими странами мира Российской Федерации активно включилась в процесс построения информационного пространства. Планируемое перспективное развитие предполагает повсеместное внедрение технологий больших данных, нейротехнологий, искусственного интеллекта, систем распределенного реестра, квантовых технологий, компонентов робототехники, технологий виртуальной реальности и др. В соответствии с указом Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» государство поставило своей целью обеспечить благоприятные условия для применения информационных и коммуникационных технологий, что также предполагает комплексное совершенствование законодательства<sup>1</sup>.

Преступность, существующая в онлайн-пространстве или использующая достижения и возможности информационно-коммуникационных технологий, проявляет себя как новое, слабо

<sup>1</sup> Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

изученное негативное киберсоциальное явление, для противодействия которому требуются особый подход и инструментарий. Познание ее характеристик, особенностей детерминации и выработки направлений уголовно-правового противодействия представляется важнейшей задачей современного общества для обеспечения национальной и международной безопасности.