

*В диссертационный совет Д 170.001.02 при  
Университете прокуратуры Российской Федерации  
по адресу: 123022, г. Москва, ул. 2-ая Звенигородская,  
д. 15, конференц-зал*

## **ОТЗЫВ**

**о диссертации Евдокимова Константина Николаевича «Противодействие компьютерной преступности: теория, законодательство, практика», представленной на соискание ученой степени доктора юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право (Москва, 2022)**

**Актуальность** представленной на защиту диссертации не вызывает сомнений. В условиях активной цифровизации общества и появления принципиально новых видов правоотношений на первый план выходят вопросы поиска оптимальных моделей правового регулирования цифровых процессов и обеспечения информационной безопасности общества и государства. Совершенно очевидно, что успех этому поиску могут принести не умозрительные заключения о природе информатизации и цифровизации, а детальный анализ тех правовых вопросов, которые они ставят. И чем более конкретно эти вопросы обозначены, тем более внятными и обоснованными должны быть предложения о необходимости корректировки регулятивного и охранительного законодательства при несомненной приоритетности последнего. На последнем тезисе хотелось бы остановиться особо.

Если регулятивное право призвано обеспечить адаптивность и прозрачность нормативного закрепления основ информационного общества, то охранительное право должно определить межевую линию между допустимым и запретным поведением, указать, где границы личной свободы участников информационно-коммуникационных отношений угрожают публичным интересам информационной безопасности. К сожалению, далеко не всеми специалистами понимается значимость такого разграничения. Это объясняется тем, что с первых дней своего существования Интернет развивался под флагом свободы слова и технического плюрализма, и именно это долгое время обеспечивало относительную гибкость и дискретность его регулирования. Однако по мере

проникновения новых технологий во все сферы публичной жизни и возникновения реальных угроз личной, общественной и государственной безопасности стали очевидными необходимостью пересмотра принципов развития информационных отношений и поиск баланса между индивидуальными и коллективными интересами безопасности.

Сегодня правоведы поставлены перед сложной юридической и мировоззренческой задачей: найти бесспорные и объективные критерии общественно опасного поведения в сфере информационных технологий и на основе этих критериев предложить адекватные современным условиям меры противодействия компьютерной преступности. Проблема осложняется тем, что в условиях развития цифровых технологий и появления неконтролируемой технотронной преступности, существенно трансформируются институты и категории уголовного права. Изменение философии взаимодействия между участниками информационного общества с неизбежностью приводит к глобальной перестройке охраняемых законом общественных отношений, а они, в свою очередь, изменяют подход уголовного права к таким, казалось бы, традиционным категориям, как момент окончания преступления, способы его совершения, предметы и средства посягательств и др., и существенно корректируют криминологические механизмы предупреждения преступности.

Наиболее ярко эти тектонические сдвиги обозначились в части предупреждения компьютерных преступлений. Можно сколько угодно долго размышлять о том, какая причина была первичной - стремительное развитие информационных технологий, или излишняя косность и традиционность юридического категориального аппарата, но очевидно одно: уголовная политика России оказалась неготовой к эффективному отражению информационных угроз и стремительному росту компьютерной преступности.

Решение данной проблемы видится в создании целостной, завершенной концепции противодействия компьютерной преступности, которая была бы вписана в общую канву уголовно-правового и криминологического воздействия и одновременно соответствовала бы современным веяниям цифровизации.

С этих позиций диссертационное исследование Евдокимова Константина Николаевича, посвященное теории, законодательству и практики противодействия компьютерной преступности, может быть оценено как **актуальный научный труд и хорошая методологическая основа** для развития информационной уголовной политики.

В своем исследовании автор обратился к рассмотрению одной из наиболее обсуждаемых, но вместе с тем слабо изученных проблем – определению современного состояния компьютерной преступности и ключевых трендов ее развития. Как справедливо отмечает диссертант, современные «высокие технологии – это своеобразный «ящик Пандоры», который несет обществу не только блага, но и различные проблемы социально-негативного характера. Одной из таких проблем для мирового сообщества и современного российского общества выступает компьютерная преступность» (С. 4).

Научная смелость соискателя проявилась в том, что он не ограничился формально-юридическим подходом к рассмотрению признаков составов главы 28 УК РФ, а раскрыл криминологическую и уголовно-правовую природу компьютерной преступности сквозь призму куда более важной и ценной для современной юридической науки проблематики, а именно: через поиск комплексного (системного) подхода к предупреждению всех преступлений, совершаемых с использованием современных информационных технологий. Он предложил на суд читателей методологически выверенное исследование, способное стать отправной точкой для дальнейшего научного анализа вопросов противодействия компьютерной преступности.

Диссертационная работа, судя по хронологии представленного в автореферате списка научных публикаций, является итогом многолетней научной практики диссертанта.

Полагаю, не будет преувеличением сказать, что именно глубокое проникновение в тему и комплексность представленного анализа гарантировали научный успех диссертации и исключили риск случайных выводов, непродуманных и поверхностных суждений.

В отдельных своих рассуждениях диссертант проявляет некоторую горячность и категоричность, однако при более детальном ознакомлении с текстом убеждаешься в том, что это является проявлением научной принципиальности соискателя, основанной на глубоком знании материала.

О солидном информационном материале работы хотелось бы сказать особо. Автор проанализировал большой массив аналитических и статистических данных Генеральной прокуратуры Российской Федерации и отдельных субъектов РФ (Алтайского края, Иркутской области, Красноярского края, Курганской области, Новосибирской области, Омской области, Приморского края, Республики Бурятия, Санкт-Петербурга, Томской области, Хабаровского края, Челябинской области), материалы ГИАЦ МВД России, ИЦ ГУ МВД по Иркутской области, материалы судебно-следственной практики; обобщил и критически оценил находящиеся в свободном доступе итоги многочисленных социологических замеров; провел опрос 410 прокурорских работников и 410 компьютерных пользователей из числа студентов образовательных организаций высшего образования.

Репрезентативная эмпирическая база эффективно дополнена результатами изучения нормативных и теоретических источников. В работе представлен тщательный анализ действующего законодательства, причем не только с точки зрения его догмы, но и в сравнительном аспекте.

Что же касается теоретической базы, то ее можно признать образцом преемственности научного знания, сочетания юридических традиций и инноваций. Комплексный характер исследования не позволил ограничиться изучением работ по главе 28 УК РФ, а потребовал расширить научный поиск изучением широкого массива научных исследований по вопросам квалификации и предупреждения преступлений, совершенных с использованием информационных технологий. Это позволило обогатить диссертацию оригинальными выводами, и придать аргументам соискателя обоснованность, аргументированность и дополнительный научный вес.

Именно качество источников и искусное использование методов научного анализа предопределили высокий коэффициент результативности проведенного

исследования. Содержание диссертации не дает оснований усомниться в том, что автор принимал личное участие на всех этапах сбора, обработки первичной научной информации и апробации результатов исследования.

Говоря о рецензируемой работе, нельзя обойти вниманием вопрос о ее научной новизне. Для труда, претендующего на соискание докторской степени, недостаточно последовательно освещать важные и актуальные вопросы с новой стороны. Гораздо более важным и ценным является поиск принципиально новой оси координат или, если угодно, шкалы оценок, которая позволяет не только посмотреть на проблему с качественно новой стороны, но и видоизменить саму проблему, представив ее сквозь призму новых научных целей, задач и категорий. Иными словами, научная новизна докторской диссертации состоит, как мне представляется, в том, чтобы увидеть то, что видят все, но на этой основе обосновать то, что другим не приходит в голову. Именно это и сделал в работе соискатель.

Он посмотрел на компьютерную преступность как на сложное динамическое явление, находящееся на этапе перехода к сложной и непрогнозируемой стадии – к неконтролируемой технотронной преступности, и предложил комплекс теоретических, законодательных и практических положений, предложений и рекомендаций по противодействию ей.

В первую очередь, обращает на себя внимание то обстоятельство, что автор рассматривает информационную безопасность как квинтэссенцию правовой политики информационного общества. Анализируя криминологические параметры компьютерной преступности, он грамотно, уверенно и емко выделяет слабые места современной системы информационной безопасности и выходит на важные для государства предложения по минимизации рисков.

И хотя сама система информационной безопасности не заявлена самостоятельным объектом научного анализа (С. 8), она тем не менее пронизывает все содержание работы и выводит автора на рассмотрение важных прикладных аспектов ее укрепления.

Красной линией в работе проходит мысль о том, что компьютерная (технотронная) преступность – это не «вещь в себе», а комплексное правовое и

социальное явление, которое может быть рассмотрено не иначе, как в тесной взаимосвязи с другими правовыми явлениями. А принимая во внимание объективную новизну цифровой преступности, задачи, стоящие перед соискателем, кажутся еще более сложными и амбициозными.

Именно системный подход позволил полно осветить ключевые аспекты инжиниринга (криминологической организации) противодействия компьютерной преступности: от определения глубинных основ ее детерминации и самодетерминации до разработки специальных мер противодействия. И несмотря на то, что не со всеми позициями автора можно согласиться, нельзя не признать высокий уровень проработки и научной новизны положений диссертации.

Не имея склонности к преувеличению заслуг соискателя, тем не менее предположу, что настоящая диссертация обладает всеми признаками научной новизны, выраженной не только в комплексной оценке правовой природы компьютерной преступности, но и в том, что в работе представлен структурный анализ ее криминологической и правовой природы; развернуто описан генезис компьютерной преступности (С. 84 – 101), раскрыта природа ранее не изученного феномена самодетерминации компьютерных преступлений (С. 150 – 168), сформулирован ряд интересных выводов по совершенствованию уголовного законодательства в части регламентации составов компьютерных преступлений (С. 394 – 410).

Содержание работы так или иначе выстроено около следующей методологической посылки: «Компьютерная преступность переживает этап трансформации в более сложное и неконтролируемое явление – технотронную преступность. И вся система ее предупреждения должна быть построена с учетом этого неустойчивого – трансформационного – состояния». И хотя эта посылка в работе раскрывается не всегда последовательно и полно (в отдельных фрагментах и вовсе отрицается синергетический принцип нелинейной детерминации открытых систем), он тем не менее позволяет рассматривать настоящую диссертацию как некий старт принципиально нового направления

комплексных научных исследований преступности в условиях информационного общества.

Говоря о научной новизне диссертации, нельзя обойти вниманием сформулированные предложения по совершенствованию российского уголовного законодательства. В авторском проекте федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» (С. 501 – 509) обосновывается необходимость дополнения главы 28 УК РФ новыми составами: ст. 272.1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации», ст. 272.2 «Перехват компьютерной информации с целью ее незаконного уничтожения, блокирования, модификации, копирования или нейтрализации средств защиты» и ст. 273.1 «Приобретение, создание, использование и распространение вредоносной компьютерной сети (ботнета)». При этом автор выдерживает аргументацию в духе последовательного выявления и предупреждение любых фактов несанкционированного доступа к информации. И хотя не со всем в работе можно согласиться, нельзя упрекнуть соискателя в голословности или в некорректной дискуссии с научными оппонентами.

Диссертационное исследование написано хорошим литературным языком, выдержано в рамках научного стиля подачи материала, оформлено в соответствии с требованиями государственных стандартов.

Соискатель поставил перед собой крайне сложную и амбициозную цель – предложить основанную на новейших криминологических данных комплексную систему предупреждения компьютерной преступности. И по большей части он справился с поставленными задачами.

Хотелось бы поздравить диссертанта с тем, что ему удалось избежать крайностей в теоретическом анализе компьютерной преступности и предложить на суд экспертов интересный научный труд, где на основе осмысления современных вызовов предложено пусть и не безупречное, но обоснованное, интересное и логически выверенное понимание стратегии противодействия технотронной преступности в современных криминологических и техногенных условиях.

В комплементарной части отзыва нельзя не отметить и **теоретическую ценность исследования**. Сегодня наука как никогда остро нуждается в пересмотре и жесткой ревизии законодательства на предмет его дальнейшего реформирования. И в этой связи сформулированные в работе положения, выводы и рекомендации позволяют существенно расширить охват этого анализа, дополнить и углубить категориальный аппарат уголовного и информационного права, расширить теоретико-методологическую основу доктрины за счет аккуратного вживления в нее новых правовых конструкций и установок, а главное – за счет правильного и последовательного внедрения в него криминологического базиса.

Современная криминологическая наука пережила пусть непродолжительный, но трагический по последствиям период своей дискредитации. Ее исключение из перечня основных дисциплин правового цикла привело к неконтролируемым цепным реакциям повсеместного отказа от криминологических сентенций и выводов при обосновании законодательных предложений. Итог очевиден: фрагментация и бесплодная умозрительность научных положений, казуичность законодательства и объективная ограниченность научных прогнозов.

Представленная на защиту работа является ярким образцом того, что криминологические знания могут обогатить предмет анализа и раскрыть его с принципиально новых, ранее не изученных сторон. Научное новаторство автора выразилось в том, что он не просто представил криминологический анализ компьютерной преступности, а предложил именно инжиниринг противодействия ей, тем самым подчerkнув системность, устойчивость и значимость криминологических основ компьютерной преступности.

Думаю, не будет преувеличением сказать, что практическая ценность работы заключается в том, что она является образцом умелого и методологически выдержанного сочетания криминологического и уголовно-правового анализа.

Скажу больше: в диссертации Евдокимова К.Н. мы встречаем фактически первый в российской науке, оригинальный по композиции, информационно и



методически обеспеченный, качественный по своим результатам опыт осмысления достаточно широкого спектра проблем предупреждения крайне опасного по последствиям и динамике явления – компьютерной преступности.

Рецензируемую диссертацию можно охарактеризовать и **как практически значимое исследование**. Ее практическая ценность обусловлена четкой направленностью на решение конкретных практических задач.

Структура работы определена внутренней логикой избранной темы исследования. Автореферат и опубликованные автором работы полностью отражают содержание и основные научные результаты диссертационного исследования.

Работа состоит из введения, двух разделов, включающих в себя шесть глав, заключения, библиографии и приложений.

В первом разделе соискатель с присущей ему основательностью определяет исходные теоретические посылки исследования, сосредоточивая внимание на проблемах инжиниринга противодействия компьютерной преступности: дает развернутый анализ понятия и признаков этой преступности (С. 32 - 36), последовательно и подробно определяет ее криминологические тренды (С. 89 – 99), выявляет основные факторы детерминации (С. 148 – 150) и самодетерминации компьютерных преступлений; дает развернутую характеристику личности компьютерного преступника (С. 105 – 114) и др.

Второй раздел диссертации посвящен анализу уголовно-правовой превенции компьютерных преступлений. Допуская методологический плюрализм и многообразие исходных начал исследования, автор обращается к международно-правовым мерам противодействия компьютерной преступности (С. 257 – 275), раскрывает закономерности криминализации деяний в уголовном законодательстве зарубежных стран (С. 285 – 300). Кроме того, он на достойном научном уровне анализирует объективные и субъективные признаки деяний и формирует новаторские предложения по совершенствованию действующего уголовного законодательства.

Полнота представленного материала, а также логика, системная согласованность и научная обоснованность выводов со всей очевидностью указывают на высокий уровень проведенного научного исследования.

Научная смелость автора рельефно проявляется в целостной совокупности конкретных теоретически и практически значимых результатов, которую можно с полным основанием оценить как оригинальное и методологически выдержанное исследование компьютерных и технотронных преступлений.

Высоко оценивая содержание диссертации и в целом разделяя предложенную в ней концепцию, не могу не отметить, что она, как и любая новаторская работа, не свободна от некоторых дискуссионных положений и выводов:

1. Раскрывая степень научной разработанности проблемы и теоретическую основу исследования, автор, как мне видится, необоснованно исключает из поля зрения большой блок исследований, так или иначе связанных с технотронной преступностью.

В частности, незаслуженно обойдены вниманием работы, посвященные уголовно-правовым и криминологическим аспектам совершения корыстных преступлений с использованием информационных (преимущественно цифровых) технологий. Как следствие: вне рамок рецензируемого исследования остались вопросы квалификации деяний, совершаемых в сфере сквозных технологий (Интернета вещей, машинного обучения, блокчейна, роботехники, виртуальной реальности и др.). А между тем, бессилие современной уголовной политики и косность категориального аппарата со всей очевидностью проявляются при совершении именно такого рода преступлений. Но в работе этим проблемам уделяется крайне мало внимания.

Представляется, что в докторской диссертации, претендующей на разработку адекватной современным условиям системы положений о противодействии компьютерной преступности, сквозные компьютерные технологии должны быть проанализированы более глубоко и рельефно.

2. Обращает на себя внимание некоторая непоследовательность соискателя в определении объекта исследования. Таковым он признает

«криминологические закономерности возникновения, становления и развития компьютерной преступности, ее трансформации в технотронную преступность, а также правоотношения в сфере уголовно-правового противодействия данному негативному социальному явлению» (С. 8).

К компьютерной преступности он относит преимущественно деяния, предусмотренные главой 28 УК РФ. Однако по мере изложения материала соискатель постоянно обращается к проблеме технотронной преступности. Последнюю он рассматривает более широко и включает в нее широкий перечень преступлений, совершаемых с использованием компьютерных технологий. Если принять во внимание, что в основе рассуждений автора заложена диаграмма Эйлера и технотронная преступность поглощает компьютерную, этот подход можно только приветствовать.

Но судя по другим рассуждениям соискателя, этот вывод ошибочен. Дело в том, что красной линией в работе прослеживается мысль о том, что процесс трансформации традиционной компьютерной преступности в технотронную (высокотехнологичную) преступность завершен (положение 1, выносимое на защиту), т.е. компьютерная преступность стала технотронной. Но если это так, возникает закономерный вопрос: «Почему в спектр уголовно-правового анализа компьютерных преступлений не включены корыстные и иные деяния, совершаемые с использованием компьютерных технологий и составляющие базу технотронной преступности?».

В продолжение темы объекта исследования нельзя не упомянуть и об ограничении масштабов исследования за счет изучения исключительно юридических и гуманитарных трудов (С. 11). Как следует из содержания работы, соискатель намеренно исключает из методологии диссертации технические методы, а из теоретической основы – техническую литературу, что заметно обедняет анализ таких сложных социально-правовых явлений, как компьютерная и технотронная преступность.

3. Несомненной заслугой диссертанта стал глубокий и последовательный анализ криминологической картины компьютерной

преступности. Но вместе с тем, в работе наличествуют выводы, нуждающиеся в корректировке и дополнительной аргументации.

Речь, в частности, идет о детерминантах компьютерной преступности. В рассуждениях о личности преступника автор упоминает о «повышении его интеллектуального уровня, объеме специальных технических знаний», а ранее в числе факторов воспроизводства компьютерной преступности называет «техническую безграмотность населения». Не кажется ли автору, что здесь заложено некоторое противоречие? Техническая безграмотность населения даже при самом внимательном прочтении не может быть оборотной стороной технического прогресса, о котором много говорится в работе. Равно как и постоянный рост уровня технических знаний преступника не может быть обусловлен низким уровнем грамотности потенциальных потерпевших. Детерминационные связи между этими явлениями гораздо более тонкие и сложные, и они не ограничиваются узко заданными линейными связями «причина – следствие». Полагаю, работа только выиграла бы, если бы в ней был проведен корреляционный анализ влияния социальных процессов на воспроизводство компьютерной преступности (и особенно на этапе ее трансформации в технотронную преступность).

Оценивая первый раздел работы, нельзя не упомянуть и криминологический портрет компьютерного преступника. В числе его типовых социально-демографических признаков автор называет среднее общее либо среднее специальное образование, что находится в некотором противоречии с ранее высказанным тезисом о повышении общего уровня грамотности преступников. Согласно официальной статистике, сегодня в России среди граждан в возрасте 25-35 лет высшее образование имеют больше 41% граждан. Значит ли это, что компьютерные преступники менее образованы, чем население в целом? И на основе каких эмпирических данных автор делает свой вывод, если проведенный им опрос охватывал только 410 компьютерных пользователей из числа студентов вузов?

4. Вызывают возражения и некоторые предложения *de lege ferenda*. Так, преждевременным выглядит предложение о необходимости введения

института ответственности юридических лиц за совершение преступлений в сфере компьютерной информации.

Сама идея наказуемости организаций не нова и с большим успехом используется сторонниками усиления репрессий за коррупцию. Однако применительно к компьютерным преступлениям она не кажется столь уж блистательной. Причина тому – полное отсутствие цифрового комплаенса в организациях. А без него вопрос о привлечении юридического лица к уголовной ответственности – не более чем оригинальное предложение на долгосрочную перспективу.

В дополнительной аргументации нуждается и предложение о введении в ст. 63 УК РФ такого обстоятельства, отягчающего наказание, как совершение преступления с использованием компьютерных, информационно-телекоммуникационных, космических, когнитивных и иных высоких технологий. Совершенно очевидно, что расплывчатость и фактически открытый перечень цифровых средств совершения преступлений могут создать удобную ситуацию для злоупотреблений и необоснованного ужесточения наказания виновного.

Отмеченные замечания, однако, не влияют на общую положительную оценку работы, цельность и обоснованность представленной в ней концепции.

На основании изучения текста рукописи диссертационного исследования, автореферата и научных трудов соискателя можно заключить следующее:

1. Диссертация Евдокимова Константина Николаевича «Противодействие компьютерной преступности: теория, законодательство, практика» полностью отвечает требованиям пунктов 9-11, 13 и 14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 (в ред. Постановления Правительства Российской Федерации от 11 сентября 2021 г. №1539).

В работе содержатся важные теоретические положения, совокупность которых можно квалифицировать как научное достижение.

Рецензируемая диссертационная работа, по моему убеждению, представляет

собой самостоятельно выполненное, цельное, логически выстроенное, эмпирически подтвержденное и всесторонне аргументированное комплексное исследование важной для отечественной и зарубежной юридической науки проблемы, результаты которого имеют значение для развития отечественной юридической науки и практики противодействия преступности.

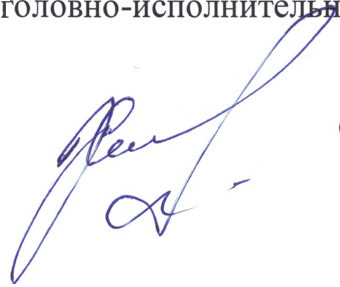
2. Рецензируемое диссертационное исследование отвечает всем предъявляемым требованиям, а его автор – Евдокимов Константин Николаевич – заслуживает присуждения ему искомой ученой степени доктора юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право.

**Официальный оппонент:**

профессор кафедры уголовного права, уголовного процесса и криминалистики международно-правового факультета федерального государственного автономного образовательного учреждения высшего образования «Московский государственный институт Международных отношений (университет) Министерства иностранных дел

Российской Федерации»,

доктор юридических наук по научной специальности 12.00.08 (уголовное право и криминология; уголовно-исполнительное право), доцент



Сидоренко Элина Леонидовна

«25» апреля 2022 г.

Адрес: 119454, г. Москва, просп. Вернадского, 76

Телефон: 8-915-146-20-52 (моб), 8-495-225-31-04 (кафедра)

e-mail: 12011979@list.ru

