На правах рукописи

Евдокимов Константин Николаевич

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ: ТЕОРИЯ, ЗАКОНОДАТЕЛЬСТВО, ПРАКТИКА

Специальность 12.00.08 – Уголовное право и криминология;
уголовно-исполнительное право

Автореферат
диссертации на соискание ученой степени
доктора юридических наук

Москва – 2022

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Университет прокуратуры Российской Федерации»

Научный консультант: **Скляров Сергей Валерьевич**
доктор юридических наук, профессор

Официальные оппоненты: **Чупрова Антонина Юрьевна**
доктор юридических наук, профессор
федеральное государственное бюджетное образовательное учреждение высшего образования «Всероссийский государственный университет юстиции (РПА Минюста России)», кафедра уголовного права и криминологии, профессор
Сидоренко Элина Леонидовна
доктор юридических наук, профессор
федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации», кафедра уголовного права, уголовного процесса и криминалистики, профессор
Лопатина Татьяна Михайловна
доктор юридических наук, доцент
федеральное государственное бюджетное образовательное учреждение высшего образования «Смоленский государственный университет», кафедра уголовно-правовых дисциплин, заведующий

Ведущая организация: **Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя»**

Защита диссертации состоится 19 мая 2022 г. в 12 час. 00 мин. на заседании диссертационного совета Д 170.001.02 при Университете прокуратуры Российской Федерации по адресу: 123022, Москва, ул. 2-я Звенигородская, д.15, конференц-зал.

С диссертацией и авторефератом можно ознакомиться в библиотеке Университета прокуратуры Российской Федерации по адресу: 123022, Москва, ул. 2-я Звенигородская, 15.

С электронной версией автореферата можно ознакомиться на сайте Университета прокуратуры Российской Федерации: http://www.agprf.org, а также на сайте Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации: http://vak.minobmauki.gov.ru.

Автореферат разослан «__» февраля 2022 г.

Ученый секретарь диссертационного совета
кандидат юридических наук Д.И. Ережипалиев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современный мир характеризуется стремительным развитием информационных отношений, информационно-коммуникационных и робототехнических технологий, глобального киберпространства, социальных информационных сетей и когнитивных технологий, а также тотальной компьютеризацией человеческого общества.

Мы живем в эпоху четвертой научно-технической революции, в результате которой на смену электронно-вычислительным машинам, полупроводниковым компьютерам и информационно-коммуникационной сети «Интернет» приходят информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления и системы мгновенного обмена информацией нового поколения; средства создания, использования, обработки и распространения информации и др., которые основаны на других физических принципах.

Современное общество является информационным обществом (обществом знаний), активно использующим технологию подключения к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами, для обмена данными (индустриальный интернет); технологию объединения через сеть «Интернет» информационных устройств, вещей (предметов), применяемых человеком в повседневной жизни, для взаимодействия друг с другом или с внешней средой (интернет вещей); обеспечение посредством сети «Интернет» общего доступа к набору вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и использованы с минимальными эксплуатационными затратами (облачные вычисления); технологию расширения облачных функций хранения, вычисления и сетевого взаимодействия, в которой обработка данных осуществляется на конечном оборудовании (компьютерные устройства, средства связи, датчики, смарт-узлы и др.) в сети, а не в «облаке» (туманные

вычисления), технологически независимые программное обеспечение и сервис; самообучающиеся компьютерные программы для обработки больших объемов данных и принятия сложных решений, сопоставимых по своим результатам с интеллектуальной деятельностью человека (искусственный интеллект) и технологии искусственного интеллекта в научной, управленческой, производственной, транспортной, энергетической, военной и оборонно-промышленной сферах (компьютерное зрение; обработка, распознавание и синтез человеческой речи, принятие самостоятельных решений и др.), в финансово-экономической сфере основывается на повышении эффективности различных видов производств, коммерции, качества предоставляемых товаров, работ, услуг путем скоростной и автоматизированной обработки больших объемов цифровых данных (цифровая экономика).

Поэтому повсеместное применение человеком информационных, коммуникационных, когнитивных, робототехнических и иных высоких технологий позволяет сделать вывод о том, что современное общество является технотронным (технотро́нный [technotronic], в переводе с англ. – связанный с использованием технотроники, т.е. техники, технологий с использованием электроники, оказывающей влияние на развитие общества), где социальные процессы тесно взаимосвязаны с достижениями научно-технического прогресса и технологиями, в основе которых лежит процесс интеграции людей с миром электронных устройств.

Однако 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, как противоправное и негативное социальное явление, возникшее в результате использования людьми компьютерных и иных IT-технологий в личных, корыстных и иных преступных целях, что приводит к наступлению общественно опасных последствий.

Актуальность выбранной темы диссертационного исследования обусловлена рядом юридических и социально-значимых проблем, не позволяющих эффективно предупреждать и бороться с компьютерной преступностью.

Современное технотронное общество является полностью зависимым от информационных, коммуникационных, аэрокосмических, энергетических, транспортных, производственных, биологических, производственных, научных и иных высоких технологий. Однако при этом большинство людей, не обладая специальными познаниями, умениями и навыками, слабо представляет принципы и методы их работы.

Поэтому техническая безграмотность населения, увеличение объемов информации, сложность и многообразие современных знаний, психология потребления благ, а не созидания, творчества и познания, отсутствие индивидуальной и общественной культуры технологической безопасности и другие факторы научно-технического характера привели к возникновению компьютерной преступности и ее последующей трансформации в неконтролируемую технотронную преступность.

Кроме того, обращает на себя внимание несовершенство действующего российского уголовного законодательства в части регламентации новых составов компьютерных преступлений, дифференциации ответственности за их совершение. В условиях перехода компьютерной преступности к преступности нового поколения – технотронной, Уголовный кодекс Российской Федерации слишком узко трактует преступления, совершаемые в данной сфере, определяя их только как преступления в сфере компьютерной информации, что не соответствует современным реалиям постоянно расширяющегося перечня преступлений, совершенных с использованием высоких технологий.

Также нельзя не отметить тот факт, что ущерб, причиненный российской экономике данным видом преступности, колоссален по своим масштабам.

По данным экспертов «Лаборатории Касперского» в случае успешной атаки киберпреступников крупные компании теряют около 20 млн. рублей, а

предприятия среднего и малого бизнеса в среднем 780 тыс. рублей – за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. На ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн. рублей, а небольшие – около 300 тыс. рублей[1].

При этом размер причиненного вреда из года в год существенно возрастает. Так, если в 2015 году ущерб экономике России от киберпреступности превысил 200 миллиардов рублей (по результатам совместного исследования Фонда развития интернет-инициатив (ФРИИ) и международных компаний Group-IB, Microsoft), что составило 0,25% от ВВП Российской Федерации[2], то уже в 2018 году ущерб российской экономике от киберугроз составил более 1,1 триллионов рублей[3], в 2019 году около 2,5 триллионов рублей[4], в 2020 году 3,5 триллионов рублей, а в 2021 году экономический ущерб Российской Федерации от кибератак достиг 7 триллионов рублей (по оценкам аналитиков службы кибербезопасности ПАО Сбербанк)[5].

Между тем, отсутствие эффективных международных и национальных правовых инструментов, несовершенство механизмов международного сотрудничества между российскими и зарубежными правоохранительными органами в сфере противодействия современной компьютерной преступности, приводит только к увеличению количества преступлений и дальнейшей динамике роста данного вида преступности.

Все вышеизложенное подтверждает актуальность темы диссертационного исследования и открывает широкое поле для научной дискуссии по теоретическим, законодательным и практическим вопросам противодействия

---

[1] Так ли страшен Интернет. О настоящей опасности киберугроз рассказывает «Газета.Ru». URL: http://www.gazeta.ru/tech/2014/11/05_a_6289085.shtml (дата обращения: 10.08.2021).

[2] Ущерб экономике России от киберпреступности превысил 200 млрд рублей. URL: http://ria.ru/economy/20160413/1409855094.html#ixzz45jCApNtn (дата обращения: 10.08.2021).

[3] Сбербанк прогнозирует ущерб экономике России от киберугроз в 2018 году в 1,1 трлн рублей. URL: https://www.kommersant.ru/doc/3676752 (дата обращения: 10.08.2021).

[4] Сбербанк оценил ущерб экономике России от кибератак в 2019 году в 2,5 трлн рублей. URL: https://www.kommersant.ru/doc/4226302 (дата обращения: 10.08.2021).

[5] Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности. URL: https://tass.ru/ekonomika/8761953 (дата обращения: 20.01.2022).

современной компьютерной преступности, разработке эффективной системы мер борьбы и предупреждения с компьютерными преступлениями, совершенствованию российского уголовного, гражданского и информационного законодательства.

Степень научной разработанности темы исследования. В рамках диссертационного исследования, необходимо отметить достаточно высокую степень научной разработанности отдельных вопросов рассматриваемой темы.

В частности, проблемам уголовно-правовой оценки преступлений в сфере компьютерной информации посвятили свои труды такие ученые, как Р.М. Айсанов, Ю.М. Батурин, И.Р. Бегишев, С.Д. Бражник, С. Ю. Бытко, В.В. Воробьев, Р.Р. Гайфутдинов, А.М. Жодзишский, У.В. Зинина, М.А. Ефремова (Зубова), А.Ж. Кабанова, Т.П. Кесареева, И.А. Клепицкий, В.Б. Клишков, В.С. Комиссаров, А.Н. Копырюлин, Ю.И. Ляпунов, В.Ю. Максимов, Д. Г. Малышенко, И.В. Никифоров, С.И. Никулин, С.А. Пашин, А.Э. Побегайло, Н.С. Полевой, С.В. Полубинская, А.Н. Попов, М.А. Простосердов, О.М. Сафонов, С.В. Скляров, Т.Г. Смирнова, М.В. Старичков, В.Г. Степанов-Егиянц, А.В. Суслопаров, В.В. Челноков, В.Н. Черкасов, З.И. Хисамова, А.Е. Шарков, С.С. Шахрай, А.Н. Ягудин, Д.А. Ястребов и другие; криминологические и отдельные криминалистические аспекты противодействия и расследования компьютерных преступлений анализировались в работах П.В. Агапова, В.А. Бессонова, В.Б. Вехова, А.Г. Волеводза, А.С. Егорашева, А. Н. Караханьяна, В.Е. Козлова, В.В. Крылова, В.В. Меркурьева, В.С. Овчинского, А.Л. Осипенко, А.Э. Побегайло, Н.С. Полевого, Л.Н. Соловьева, С.Е. Спириной, Е.В. Старостиной, Л.А. Сударевой, Н.Г. Шурухнова и других ученых.

Значительный вклад в изучение проблем противодействия компьютерной преступности и борьбе с компьютерными преступлениями внесли зарубежные ученые: Д. Айков, В. А. Голубев, И. В. Грень, П. Джонстон, А. Кемрадж, М. Кратц, Д. Лэнс, К. Сейгер, Б. Х. Толеубекова, Ф. Файтс, У. Фонсторх, В. В. Хилюта и др.

Следует отметить, что уголовно-правовым и криминологическим аспектам противодействия компьютерной преступности в России и зарубежных странах были непосредственно посвящены диссертационные исследования М. С. Гаджиева, Д. В. Добровольского, А. А. Жмыхова, Т. М. Лопатиной.

Вопросы противодействия киберпреступности в России нашли свое отражение в диссертациях на соискание ученой степени кандидата юридических наук Т. Л. Тропиной и И. Г. Чекунова, а исследование Интернет-преступности проводилось в диссертации на соискание ученой степени кандидата юридических наук Р. И. Дремлюги.

Указанные работы заложили научные основы уголовно-правового и криминологического противодействия компьютерной преступности в Российской Федерации.

Между тем проблемные вопросы контроля компьютерной преступности в Российской Федерации в условиях ее трансформации в высокотехнологическую, технотронную преступность; предупреждения, устранения причин и условий ее возникновения, минимизации и ликвидации преступных последствий остались по-прежнему неразрешенными как на научно-теоретическом и законодательном, так и практическом уровнях.

Компьютерная преступность как объект научного исследования требует дальнейшего изучения и тщательного анализа, в том числе разработки эффективной системы уголовно-правовых и криминологических мер для противодействия данному негативному социальному явлению.

Объектом диссертационного исследования выступают криминологические закономерности возникновения, становления и развития компьютерной преступности в Российской Федерации, ее трансформации в технотронную преступность, а также правоотношения в сфере уголовно-правового противодействия данному негативному социальному явлению.

Предмет диссертационного исследования образуют криминологическая характеристика компьютерной преступности, ее детерминанты и самодетерминация, меры предупреждения; нормы международного права,

зарубежного и российского уголовного законодательства, положения иных нормативных актов, направленных на противодействие компьютерной преступности, а также практика правоприменения вышеуказанных норм.

Целью диссертационного исследования является разработка теоретических, законодательных и практических основ противодействия компьютерной преступности в Российской Федерации в условиях ее трансформации в неконтролируемую технотронную преступность.

Достижение названной цели обусловило постановку и решение следующих **задач**:

- на основе существующих научных подходов, позиций, точек зрения сформулировать авторское определение понятия «компьютерная преступность»;

- осуществить оценку количественно-качественных показателей компьютерной преступности в Российской Федерации;

- обосновать систему научно-теоретических положений (частную теорию) об «Анекселенктотичной (неконтролируемой) технотронной преступности», нового вида высокотехнологической преступности, пришедшей на смену традиционной компьютерной преступности и являющейся дальнейшей формой развития преступности с использованием высоких технологий (информационных, коммуникационных, биологических, производственных, военно-технических, аэрокосмических, энергетических, научных и др.)

- раскрыть соотношение понятий «компьютерная преступность» и «технотронная преступность»;

- выявить комплекс факторов, детерминирующих компьютерную преступность в современной России;

- выделить закономерности в эволюции вредоносных компьютерных программ как фактора развития компьютерной преступности;

- выявить особенности самодетерминации современной компьютерной преступности;

- провести авторскую классификацию и типологию компьютерных преступников;

- сформулировать обобщенный криминологический портрет личности компьютерного преступника;

- раскрыть организационно-правовые основы противодействия компьютерной преступности, определяющие понятие, структуру, состояние, проблемы системы профилактики, борьбы и нейтрализации проявлений компьютерных преступлений;

- предложить комплекс мер по противодействию современной компьютерной преступности, сформулировав авторские законопроекты о внесении соответствующих изменений и дополнений в уголовное, уголовно-процессуальное и гражданское законодательство Российской Федерации;

- определить меры по совершенствованию международного сотрудничества Российской Федерации с иностранными государствами в сфере противодействия компьютерной преступности и обеспечения международной информационной безопасности;

- раскрыть международные уголовно-правовые основы противодействия компьютерной преступности;

- выявить особенности и специфику уголовного законодательства зарубежных стран, регламентирующего ответственность за совершение компьютерных преступлений;

- сформулировать в законопроектной форме научно обоснованные предложения по совершенствованию уголовного законодательства Российской Федерации, регламентирующего ответственность за совершение компьютерных преступлений;

- выработать практические рекомендации для судей, прокуроров, следователей и юристов-практиков по проблемным вопросам квалификации компьютерных преступлений;

- разработать авторский проект постановления Пленума Верховного Суда Российской Федерации «О некоторых вопросах судебной практики при

рассмотрении уголовных дел о преступлениях в сфере компьютерной информации».

Методологическую основу исследования составили базовые положения диалектического метода познания, в рамках которого применялась система общенаучных методов (логический, исторический, системно-структурный), частнонаучных методов (историко-правовой, формально-юридический, сравнительно-правовой, правового моделирования) и специальных научных методов познания (статистический, кибернетический, конкретно-социологический, метод экспертных оценок, контент-анализа и др.).

В основу диссертационного исследования положены интегративный и комплексный подходы, заключающиеся в использовании знаний различных юридических (уголовного права, криминологии) и иных гуманитарных (социологии, психологии, философии и др.) наук, в целях наиболее полного, всестороннего и системного изучения компьютерной преступности в Российской Федерации, как негативного социального и правового явления.

Теоретическую основу исследования составили научные работы ведущих отечественных и зарубежных ученых в области криминологии, криминалистики, уголовного, уголовно-процессуального, конституционного, административного, информационного, гражданского и международного права. В частности, таких ученых, как П.В. Агапов, К.И. Амирбеков, Б.В. Андреев, Ю.М. Антонян, С.В. Бажанов, Ю.М. Батурин, И.Л. Бачило, Т.А. Боголюбова, А.В. Бриллиантов, В.М. Быков, А.Б. Венгеров, В.Б. Вехов, А.Г. Волеводз, Б.В. Волженкин, Ю.В. Гаврилин, Р.Р. Галиакбаров, Л.Д. Гаухман, А.А. Герцензон, Т.А. Диканова, А.И. Долгова, Г.А. Есаков, А.М. Жодзишский, Р.В. Жубрин, О.С. Капинус, В.С. Комиссаров, С.М. Кочои, В.В. Крылов, В.Н. Кудрявцев, Н.Ф. Кузнецова, Б.А. Куринов, В.Д. Курушин, А.Н. Ларьков, В.Н. Лопатин, В.В. Лунеев, В.В. Меркурьев, А.В. Наумов, Б.С. Никифоров, В.А. Номоконов, К.В. Ображиев, В.С. Овчинский, А.Л. Осипенко, А.В. Павлинов, С.В. Пархоменко, А.А. Пионтковский, А.Н. Попов, С.В. Расторопов, А.И. Рарог, Т.В. Раскина, И.М. Рассолов, В.С. Савельева,

С.В. Скляров, Д.А. Соколов, Н.С. Таганцев, А.Н. Трайнин, В.Н. Черкасов, А.И. Чучаев, П.С. Яни и др.

Указанные ученые создали надлежащую теоретическую базу для раскрытия проблемных вопросов о факторах, детерминирующих развитие компьютерной преступности, выявления специфики личности компьютерного преступника и мотивации его противоправной деятельности, предупреждения компьютерных преступлений, квалификации преступлений в сфере компьютерной информации.

Теоретическую основу диссертационного исследования также сформировали научные доктрины, концепции, подходы и взгляды по проблемам уголовно-правового и криминологического противодействия компьютерной преступности, изложенные в научных трудах М.С. Гаджиева, И.В. Греня, Д.В. Добровольского, Р.И. Дремлюги, А.А. Жмыхова, Т.М. Лопатиной, Т.Л. Тропиной, И.Г. Чекунова.

Кроме того, теоретическую основу исследования образовали научные публикации из общедоступных Интернет-ресурсов, посвященных проблемам противодействия компьютерной преступности.

Нормативную основу исследования образуют: Конституция Российской Федерации, международные правовые акты, Уголовный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, федеральные законы и подзаконные нормативные правовые акты в сфере информационной безопасности и компьютерной преступности; зарубежное уголовное законодательство, регламентирующее ответственность за совершение компьютерных преступлений и преступлений, совершенных с использованием информационно-коммуникационных технологий.

Эмпирическую основу исследования составили аналитические материалы и статистические данные Генеральной прокуратуры Российской Федерации; прокуратур Алтайского края, Иркутской области, Красноярского края, Курганской области, Новосибирской области, Омской области,

Приморского края, Республики Бурятия, Санкт-Петербурга, Томской области, Тюменской области, Хабаровского края, Челябинской области; ГИАЦ МВД России, ИЦ ГУ МВД России по Иркутской области, материалы судебно-следственной практики по уголовным делам о преступлениях в сфере компьютерной информации и совершенных с использованием информационно-телекоммуникационных сетей за период с 2004 по 2021 годы; официальные материалы международных правоохранительных органов (Интерпола, Европола) и Федерального Бюро Расследования Соединенных Штатов Америки.

В процессе работы над диссертационным исследованием, по разработанной автором анкете, проведен опрос 410 прокурорских работников и 410 компьютерных пользователей из числа студентов образовательных организаций высшего образования.

В рамках научной работы, по составленной автором тематической программе, изучены материалы 287 уголовных дел, возбужденных по фактам совершения преступлений в сфере компьютерной информации и с использованием информационно-телекоммуникационных сетей.

Использованы материалы и статистические данные иных социологических и криминологических исследований, затрагивающих проблему противодействия компьютерной преступности.

Научная новизна исследования состоит в разработке комплекса теоретических, законотворческих и практических положений, предложений и рекомендаций по противодействию современной компьютерной преступности (в условиях ее преобразования в технотронную преступность), образующих логически обоснованное, непротиворечивое и цельное учение (частную теорию) об «Анекселенктотичной (неконтролируемой) технотронной преступности» и мерах по ее предупреждению, минимизации и ликвидации преступных последствий, устранению причин и условий совершения высокотехнологичных преступлений в Российской Федерации.

Диссертационные исследования на соискание ученой степени доктора юридических наук по рассматриваемой научной проблеме не проводились.

Положения, выносимые на защиту:

На защиту вынесены следующие научные положения, характеризующие новизну, теоретическую и практическую значимость диссертационного исследования:

1. **Комплекс научно-теоретических положений, характеризующих современную компьютерную преступность**:

1.1. Вывод о завершении процесса трансформации традиционной компьютерной преступности в новый вид высокотехнологичной преступности – технотронную преступность, представляющую собой совокупность взаимосвязанных и образующих единую целостность общественно опасных деяний, совершенных лицами с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий на определенной территории за определенный период времени, где основным объектом преступного посягательства выступают конкретные общественные отношения в сфере безопасного создания, использования и распространения высоких технологий.

1.2. Обоснованная автором теория анекселенктотичной (неконтролируемой) технотронной преступности – научная теория о появлении нового вида высокотехнологической преступности, пришедшей на смену традиционной компьютерной преступности и являющейся дальнейшей формой развития преступности с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий, которая в силу латентного, организованного, профессионального, трансграничного, транснационального характера и самодетерминации вышла из-под контроля личности, общества и государства, представляя опасность практически для всех социально значимых общественных отношений.

1.3. Трансформация компьютерной преступности в анекселенктотичную (неконтролируемую) технотронную преступность обусловлена следующими основными факторами: процессом самодетерминации компьютерной преступности на фоне стремительного развития и массового применения компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий; эволюцией вредоносных компьютерных программ в сторону автоматизации воспроизводства программных вирусов и принятия противоправных решений без вмешательства человека.

1.4. Модификация компьютерной преступности в технотронную преступность сопровождается изменением криминологически значимых характеристик личности преступника, проявляясь в повышении его интеллектуального уровня, объема специальных технических знаний, умений и навыков в области компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий, приобретенных, как правило, во время работы в высокотехнологичных сферах (наука и высшее образование, связь и телекоммуникации, логистика и транспорт, аэрокосмическая отрасль, оборонно-промышленный комплекс, финансово-банковский сектор и др.) в качестве специалиста, либо руководителя начального (среднего) уровня, в увеличении среднего возраста технотронного преступника (до 35 лет).

1.5. Научно обоснованные предложения автора о системе мер, направленных на сдерживание, нейтрализацию и снижение роста технотронных преступлений. В ее основу должны быть положены общие научно-технические меры (создание и применение российских технологий в сфере искусственного интеллекта, облачных и туманных вычислений, интернета вещей и индустриального интернета, обеспечения информационной безопасности и др.), а также ряд специальных правовых и организационно-технических мер (активизация международно-правового сотрудничества в рамках ООН с целью принятия специальной конвенции о противодействии преступности в сфере

высоких технологий; модернизация российского уголовного законодательства в части регламентации новых составов технотронных преступлений; конкретизация признаков соответствующих составов преступлений в разъяснениях Верховного Суда Российской Федерации; подготовка высококвалифицированных следователей и экспертов-криминалистов в сфере борьбы с высокотехнологичными преступлениями, оснащение их современной криминалистической техникой; привлечение специалистов в области IT-технологий для раскрытия и расследования сложных технотронных преступлений; создание единой для правоохранительных органов базы данных с элементами искусственного интеллекта по учету технотронных преступников, совершенных ими преступных деяний и обнаруженных следов преступлений; общественный контроль за контентом в киберпространстве и др.), которые должны создать необходимые условия для эффективного выявления, пресечения, раскрытия и расследования технотронных преступлений.

1.6. С целью минимизации рисков неконтролируемого использования достижений научно-технического прогресса в преступных целях обоснована необходимость реализации следующих мер: лицензирование деятельности физических и юридических в высокотехнологичных сферах; усиление государственного контроля (надзора) в указанных областях; обеспечение неотвратимости уголовной ответственности за преступления в области высоких технологий.

1.7. Для повышения эффективности существующей системы противодействия компьютерной преступности, обоснована необходимость расширения сферы деятельности негосударственных правоохранительных организаций: народных дружин (кибердружин), частных охранных предприятий, частных детективных агентств по выявлению, предупреждению, пресечению компьютерных преступлений. Предлагается законодательно разрешить вышеуказанным негосударственным организациям иметь в штате технических специалистов и программные (аппаратно-программные) средства для выявления и блокирования противоправного контента в информационно-

коммуникационных сетях, включая сеть Интернет; закрепить полномочия коммерческих организаций по охране конфиденциальной компьютерной информации, информационно-коммуникационных сетей; средств создания, обработки, передачи информации; поиску утраченной компьютерной информации физических и юридических лиц на договорной основе.

2. Комплекс научно-исследовательских положений, направленных на оптимизацию и повышение эффективности уголовного законодательства Российской Федерации в противодействии компьютерной преступности:

2.1. С учетом конституционных требований к криминализации общественно опасных деяний обоснована потребность в установлении уголовной ответственности за:

- хищение компьютерной информации и ее физических носителей с целью неправомерного доступа к информации ограниченного доступа;

- перехват компьютерной информации с целью ее незаконного уничтожения, блокирования, модификации, копирования или нейтрализации средств защиты;

- создание, приобретение, использование и распространение, инфицированных вредоносными компьютерными программами и объединенных в общую сеть компьютеров либо иных компьютерных устройств, находящихся в фактическом владении правообладателей, но удаленно используемые преступниками для совершения различного вида противоправных деяний; приобретение вредоносных компьютерных программ для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

2.2. Предложено скорректировать законодательное определение компьютерной информации (примечание к ст. 272 УК РФ), изложив его в следующем виде: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме любых сигналов физического

характера (механических, электрических, квантовых, гравитационных, молекулярных и т.д.), независимо от средств их создания, хранения, обработки и передачи».

2.3. Обоснована необходимость изменения подхода к пенализации преступлений в сфере компьютерной информации, повлекших тяжкие последствия или создавших угрозу их наступления, путем отнесения указанных деяний к категории особо тяжких преступлений.

2.4. С учетом проведенного социологического исследования, зарубежного опыта, анализа судебно-следственной практики и других эмпирических материалов обоснована необходимость снижения возраста привлечения к уголовной ответственности с 16 до 14 лет для лиц, совершивших преступления в сфере компьютерной информации, повлекших причинение тяжких последствий или создавших угрозу их наступления.

2.5. Научно обоснованное предложение автора о правовой регламентации совершения преступлений с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий как способа совершения общественно опасного деяния, путем закрепления последнего в российском уголовном законодательстве в качестве обстоятельства, отягчающего уголовное наказание.

2.6. Вывод о неизбежности концептуального обновления российского уголовного права в части введения института ответственности юридических лиц, в том числе за совершение преступлений в сфере компьютерной информации и деяний, совершенных с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий.

Предлагается признавать юридическое лицо виновным в совершении компьютерного преступления, если будет установлено, что у него имелась возможность для соблюдения правил и норм, за нарушение которых Уголовным кодексом Российской Федерации предусмотрено наказание, но

данным лицом не были приняты все зависящие от него меры по их соблюдению.

При этом обоснован вывод, что назначение наказания юридическому лицу не должно освобождать от уголовной ответственности за совершение данного компьютерного преступления виновное физическое лицо, равно как и привлечение к уголовной ответственности указанного физического лица не освобождает от наказания за совершение данного компьютерного преступления юридическое лицо.

2.7. Обоснована необходимость переименования главы 28 УК РФ с «Преступления в сфере компьютерной информации» на «Технотронные преступления», что обусловлено стремительным развитием общественных отношений в сфере применения высоких технологий, необходимостью их уголовно-правовой охраны, спецификой объекта и предмета преступного посягательства, совершенного с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий.

Теоретическая значимость исследования.

Результаты диссертационного исследования концептуально определяют направления и систему мер научно-теоретического, законодательного и практико-прикладного характера для эффективного противодействия компьютерной преступности как крупной социально-правовой проблемы современного российского государства и общества, а также закладывают теоретическую основу для последующих научных работ в области криминологии и уголовного права по данной проблематике.

Практическая значимость исследования состоит в том, что сформулированные диссертантом положения, выводы и рекомендации по противодействию компьютерной преступности в Российской Федерации, в контексте ее трансформации в неконтролируемую технотронную преступность, могут быть использованы:

- в правотворческом процессе для совершенствования уголовного законодательства Российской Федерации, регламентирующего ответственность за преступления в сфере компьютерной информации, для разработки подзаконных правовых актов в сфере противодействия компьютерной преступности;

- в образовательном процессе при преподавании учебных дисциплин «Криминология», «Уголовное право (Особенная часть)» и специальных дисциплин уголовно-правового цикла на юридических факультетах высших учебных заведений;

- при подготовке учебников, учебных и учебно-методических пособий, комментариев, фондовых лекций, методических рекомендаций по уголовному праву и криминологии, посвященных темам и вопросам противодействия компьютерной преступности;

- в разработке основ уголовно-правовой политики Российской Федерации, федеральных и региональных целевых программ по вопросам кибербезопасности органов власти, предприятий, учреждений, организаций, предупреждения, борьбы, устранения причин и условий совершения преступлений в сфере компьютерной информации, минимизации и ликвидации общественно опасных последствий компьютерных преступлений;

- при разработке научно-практических рекомендаций для судей, прокуроров, следователей по вопросам квалификации преступлений в сфере компьютерной информации;

- для совершенствования судебной практики рассмотрения уголовных дел о преступлениях в сфере компьютерной информации и деяний, совершенных с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), в т.ч. разработки соответствующих проектов пленума Верховного Суда Российской Федерации;

- для профессиональной переподготовки и повышения квалификации судей, прокуроров, следователей, специалистов в области информационной безопасности и защиты компьютерной информации;

- в практической деятельности правоохранительных органов при предупреждении, выявлении, раскрытии, расследовании компьютерных преступлений.

В диссертационном исследовании заложены методические и практические основы для его использования в других научно-прикладных и практико-организационных целях по противодействию преступности в Российской Федерации.

Достоверность результатов исследования обеспечена: применением апробированных методов и методик проведения диссертационных исследований; соблюдением научных требований криминологии и уголовного права, их методологических принципов; использованием достижений других наук; комплексностью и междисциплинарностью исследования при безусловном соблюдении криминологических и уголовно-правовых приоритетов анализа; тщательным отбором эмпирического материала, репрезентативной базой статистических данных, обобщением практического опыта правоохранительных органов, материалами судебно-следственной практики, использованием в диссертационном исследовании научных работ общепризнанных отечественных и зарубежных ученых в области криминологии и уголовного права.

Апробация результатов исследования. Основные результаты диссертационного исследования нашли свое отражение в опубликованных автором 91 научной, научно-практической и учебной работах: в 7 монографиях, 81 научной статье, в том числе в 33 статьях, опубликованных в изданиях, рекомендуемых Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации, и 8 статьях в изданиях, входящих в международные реферативные базы данных и системы цитирования (Scopus, WoS), Комментарии к Уголовному кодексу Российской Федерации, 2 учебниках по криминологии.

Основные положения и выводы диссертации докладывались и обсуждались на заседаниях отдела научного обеспечения прокурорского

надзора и укрепления законности в сфере уголовно-правового регулирования, исполнения уголовных наказаний и иных мер уголовно-правового характера НИИ и кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации.

Материалы диссертации были использованы в разработке предложений по вопросу целесообразности внесения в Уголовный кодекс Российской Федерации изменений в части усиления уголовной ответственности за преступления, совершенные с использованием современных информационно-коммуникационных технологий, а также расширения перечня объектов уголовно-правовой охраны в рассматриваемой сфере с учетом использования опыта зарубежных стран и договоров, ратифицированных Российской Федерацией.

Результаты проведенного исследования докладывались и обсуждались на 25 международных, всероссийских, региональных, внутривузовских научных и научно-практических конференциях, круглых столах, семинарах и совещаниях в городах Москва (2018, 2019), Лондон (2016), Санкт-Петербург (2015, 2018), Иркутск (2009-2020), Казань (2017), Калининград (2014), Красноярск (2020), Минск (2020), Тольятти (2014), а также получили апробацию при участии автора в программе «Повышение эффективности уголовного судопроизводства по делам о киберпреступлениях для обеспечения национальной безопасности» (договор № 14.Z56.14.2691-МД об условиях использования гранта Президента Российской Федерации для государственной поддержки молодых российских ученых с организациями-участниками конкурсов, имеющими трудовые отношения с молодыми учеными МД-2691.2014.6.).

Основные положения диссертационного исследования используются в научной деятельности Университета прокуратуры Российской Федерации, Байкальского государственного университета, учебном процессе Тольяттинского государственного университета при преподавании дисциплин «Уголовное право», «Криминология».

Результаты диссертационного исследования были использованы в практической деятельности прокуратуры Иркутской области.

Структура исследования определяется его целями и задачами. Диссертация состоит из введения, двух разделов, шести глав, девятнадцати параграфов, заключения, библиографического списка и приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается выбор и актуальность темы, формулируется цель и задачи исследования, его объект и предмет, раскрываются методологическая, нормативная, теоретическая и эмпирическая основы диссертации, определяется ее научная новизна и положения, выносимые на защиту, доказывается их теоретическая ценность и практическая значимость, содержатся сведения о достоверности и апробации основных выводов и предложений диссертационного исследования, внедрении в практику полученных результатов.

Раздел I «Криминологическая организация (инжиниринг) противодействия компьютерной преступности» состоит из трех глав.

В **главе 1 «Криминологическая характеристика компьютерной преступности»** раскрывается понятие и сущность компьютерной преступности в глобальном информационном обществе (§ 1), исследуется состояние, структура и динамика компьютерной преступности в Российской Федерации (§ 2), анализируется генезис компьютерной преступности в период 4-й научно-технической революции и формулируется авторская теория «Анекселенктотичной (неконтролируемой) технотронной преступности» (§ 3), рассматривается специфика личности компьютерного преступника (§ 4).

В параграфе 1 «Понятие и сущность компьютерной преступности в глобальном информационном обществе» автором исследуются сложившиеся в современной криминологической науке подходы к определению понятия и сущности компьютерной преступности в условиях активно развивающегося глобального информационного общества.

С учетом существующих научных мнений, автор полагает, что понятие и термин «киберпреступность» справедливо применять только к совокупности

компьютерных преступлений, совершенных в пространстве информационно-телекоммуникационных сетей, либо с использованием информационно-телекоммуникационных сетей, в т.ч. сети «Интернет», для достижения преступных целей. При этом понятие «Интернет-преступность» будет охватываться понятием «Киберпреступность», т.к. глобальная сеть «Интернет» является лишь одной из многих существующих информационно-телекоммуникационных сетей, которая может быть использована киберпреступниками в противоправных целях.

В свою очередь, «компьютерная преступность» по отношению к «киберпреступности» выступает родовым понятием, т.к. с криминологической и технической точек зрения, информационно-телекоммуникационные сети выступают только средством передачи компьютерной информации в преступных целях, а основные же преступные действия по созданию, обработке, хранению компьютерной информации по-прежнему выполняют различные компьютерные устройства.

Компьютерную преступность предлагается рассматривать в узком и широком смыслах, поскольку дуалистический подход в определении рассматриваемого понятия позволяет более полно оценить всю сложность, разнообразие, многоуровневость рассматриваемого криминального явления.

Под компьютерной преступностью в узком смысле предлагается понимать совокупность преступлений, совершенных лицами на определенной территории за определенный период времени, где основным объектом преступного посягательства выступают конкретные общественные отношения в сфере безопасного функционирования компьютерной информации, средств поиска, сбора, хранения, обработки, предоставления, распространения, защиты компьютерной информации, информационно-коммуникационных устройств, а компьютерная информация, компьютерные сети, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи компьютерной информации являются не только предметом

преступного посягательства, но и используются в качестве средства и (или) орудия совершения преступления.

Таким образом, компьютерная преступность в ее «узком смысле» шире по своему объему и содержанию таких понятий как «киберпреступность», «интернет-преступность», «преступность в сфере компьютерной информации», «преступность в сфере информационных технологий», включая их с точки зрения объективных и субъективных признаков состава преступления (объект и предмет преступного посягательства; вид деяния; способ, средства, орудия преступления; общий и специальный субъекты преступления и т.д.).

Компьютерная преступность в широком смысле представляет собой противоправное и негативное социальное явление, возникшее в результате использования людьми компьютерных и иных IT-технологий в личных, корыстных и иных преступных целях, что приводит к наступлению общественно опасных последствий.

Сущность компьютерной преступности в Российской Федерации определяется рядом характеризующих ее признаков, наиболее существенными и значимыми из которых являются: самостоятельный характер ее существования, тесная взаимосвязь с другими видами преступности, высокотехнологичность, латентность, организованность, профессионализм компьютерных преступников, трансграничность и транснациональность, самодетерминация, ярко выраженная экономическая и политическая направленность, неконтролируемость со стороны личности, общества и государства.

В параграфе 2 «Состояние, структура и динамика компьютерной преступности в Российской Федерации» рассматривается, анализируется и сравнивается структура компьютерной преступности, отраженная в уголовном законе, в научных работах отечественных и зарубежных авторов, экспертных отчетах специалистов в области компьютерной защиты и информационной безопасности, формах статистической отчетности правоохранительных органов и других эмпирических материалах.

В результате автор приходит к выводу, что с нормативной точки зрения, структуру компьютерной преступности образовывают как преступления в сфере компьютерной информации (ст. ст. 272-274[1] УК РФ), так и деяния, совершенные с использованием информационно-коммуникационных технологий (ст. ст. 138, 138[1], 146, 158, 159, 159[3], 159[6], 163, 165, 171[2], 183, 228[1], 230, 242, 242[1], 242[2], 280, 282 УК РФ и др.)

В свою очередь, экспертное сообщество (специалисты Group-IB, Dr.Web, Symantec, «Лаборатории Касперского», ПАО Сбербанка и др.) в структуре компьютерной преступности выделяет такие деяния как мошенничество в системах интернет-банкинга, фишинг, хищение электронных денег на криптовалютных биржах, услуги обналичивания иных нелегальных доходов, спам; незаконная продажа трафика, эксплойтов, загрузок; анонимизация, DDoS-атаки, атаки на объекты критической информационной инфраструктуры (ART-атаки), хактивизм, кибершпионаж и др.

Представители криминологической науки (Т. М. Лопатина, В. А. Номоконов, А. Д. Саидов, Д. А. Рагимханов, Т. Л. Тропина, М. Б. Эмиров и др.) в структуре данного вида преступности выделяют промышленный шпионаж; саботаж; вандализм; спуфинг (взлом паролей); мошенничество, либо исходят из сложного характера структуры компьютерной преступности и рассматривают входящие в нее преступные деяния по нескольким критериям: от объекта, от предмета преступного посягательства, в зависимости от способов совершения преступления(например, М. А. Ефремова – преступления против права на информацию, преступления против безопасности информационных ресурсов, преступления против безопасности информационно-телекоммуникационных технологий; Е. А. Русскевич – компьютерные и компьютеризированные преступления) и т.д.

Между тем, по мнению автора, для уяснения структуры компьютерной преступности в России, предпочтительней использовать комплексный подход правоохранительных органов (по объекту и предмету преступного посягательства; месту, орудию, средству и способу совершения преступления с соотношением к соответствующей статье УК РФ), в частности данные

Генеральной прокуратуры Российской Федерации (Форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений»), что обусловлено существующей методикой сбора и учета данных о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации.

Поэтому структуру рассматриваемого вида преступности будут образовывать как преступления в сфере компьютерной информации (ст. ст. 272-274^1 УК РФ), так и деяния, совершенные с использованием информационно-телекоммуникационных технологий (ст. ст. 138, 138^1, 146, 158, 159, 159^3, 159^6, 163, 165, 171^2, 183, 228^1, 230, 242, 242^1, 242^2, 280, 282 УК РФ и др.).

При оценке состояния, уровня и интенсивности компьютерной преступности в России автор приходит к выводу, что с 2015 года, отмечается динамика постоянного роста зарегистрированных компьютерных преступлений, составив 1164,9 % (с 43816 преступлений в 2015 году до 510396 преступлений в 2020 году).

В свою очередь, уровень компьютерной преступности в абсолютных цифрах возрастал ежегодно в арифметической прогрессии и в 2020 году достиг объема в 510396 преступлений, удельный вес компьютерных преступлений составил 25 % от общего количества зарегистрированных деяний (в 2015 году – 43816 компьютерных преступлений или 1,83 % от числа зарегистрированных деяний), число выявленных компьютерных преступников с 2863 лиц в 2015 году (удельный вес в общем числе выявленных лиц, совершивших преступления – 0,27 %) увеличилось до 65665 в 2020 году (удельный вес в общем числе выявленных лиц, совершивших преступления – 7,7 %).

Интенсивность компьютерной преступности в последние годы растет уже в геометрической прогрессии. Так коэффициент преступности на 100 000 населения, достигшего возраста привлечения к уголовной ответственности, вырос с 36,1 в 2015 году до 424,3 в 2020 году почти в 12 раз (1175, 3%),

коэффициент преступного поведения (лиц, совершивших компьютерные преступления на 100 000 населения старше 14 лет) возрос с 2,4 до 54,6, т.е. более чем 22 раза (2275%). При этом количество и удельный вес профессиональных преступников (крэкеров, вирусмейкеров, кардеров и др.), т.е. лиц, совершающих преступления в сфере компьютерной информации, выявленных правоохранительными органами, остается очень низким и снизился с 552 лиц в 2015 году (удельный вес профессиональных компьютерных преступников в общем числе выявленных лиц, совершивших компьютерные преступления – 19,28 %) до 389 в 2020 году (удельный вес профессиональных компьютерных преступников в общем числе выявленных лиц, совершивших компьютерные преступления – 0,59 %).

Основными тенденциями развития компьютерной преступности в последние годы является динамика ее постоянного роста, увеличение в ее структуре преступлений корыстной направленности (краж, мошенничеств и др.). При этом жертвами компьютерных преступлений все чаще становятся не обычные граждане, а банки, финансово-кредитные организации, крупные компании и корпорации, т.к. преступники используют возможность получить больший преступный доход при тех же ресурсно-временных затратах.

Другими негативными тенденциями генезиса компьютерной преступности является массовое использование преступниками анонимных средств IT-технологий (информационно-коммуникационных сетей, мессенджеров, криптовалют и т.д.), а также увеличение количества кибератак на объекты критической информационной инфраструктуры, которые наносят серьезный вред национальной безопасности России: затрудняя или блокируя деятельность государственных органов и учреждений, автоматизированных систем государственного управления, причиняя существенный ущерб экономической, общественной, информационной, транспортной, энергетической и иным видам безопасности.

В параграфе 3 «Генезис компьютерной преступности в информационом обществе (теория «Анекселенктотичной

(неконтролируемой) технотронной преступности»)» отмечается, что компьютерная преступность в последние годы, за счет противоправного использования компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий, вышла на новый качественный технологический уровень, и трансформировалась в технотронную преступность.

При этом, взаимосвязь компьютерной и технотронной преступности предлагается рассматривать как соотношение частного и общего понятий, где компьютерная преступность является составной частью технотронной преступности, которая представляет собой совокупность преступлений, совершенных лицами на определенной территории за определенный период времени с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий.

Автор обосновывает научную (частную) теорию «Анекселенктотичной (неконтролируемой) технотронной преступности» (anexélenktos ανεξέλεγκτος в переводе с греч. – неконтролируемый, неуправляемый; технотро́нный [tʲɪxnɐˈtronːɨn̪] (в переводе с англ.) – связанный с использованием технотроники, т.е. техники, технологий с использованием электроники, оказывающей влияние на развитие общества), т.е. научную теорию о появлении нового вида высокотехнологической преступности, пришедшей на смену традиционной компьютерной преступности и являющейся дальнейшей формой развития преступности с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий – технотронной преступности, которая вышла из-под контроля личности, общества и государства, представляя опасность практически для всех жизненно важных общественных отношений и требует принятия скорейших мер для ее нейтрализации, предупреждения, устранения причин и условий возникновения.

Данная научная теория основывается на следующих положениях и выводах:

1. Современное общество является технотронным и складывающиеся социальные отношения обусловлены влиянием техники, существенно зависимы от использования высоких технологий. Однако при этом большинство людей слабо представляют принципы и способы их работы, не обладают специальными техническими познаниями и навыками. Поэтому техническая безграмотность населения, отсутствие индивидуальной и общественной культуры технологической безопасности, приводит к неконтролируемости технотронной преступности обществом и отдельными индивидуумами.

2. Латентность технотронных преступлений, сложность их выявления, раскрытия и расследования правоохранительными органами, привела к тому, что количество раскрытых преступлений, выявленных преступников и уголовных дел, направленных в суд с обвинительным заключением, из года в год сокращается.

По данным Генеральной прокуратуры Российской Федерации в 2020 году зарегистрировано 510396 преступлений, совершенных с использованием информационно-телекоммуникационных технологий. При этом направлены в суд уголовные дела с обвинительными заключениями только по 82977 преступлениям, т.е. около 16, 3 %; из 4498 зарегистрированных преступлений в сфере компьютерной информации направлены в суд с обвинительным заключением уголовные дела только по 480 преступным деяниям (10, 7 %). Например, по факту совершения неправомерного доступа к компьютерной информации (ст. 272 УК РФ) было зарегистрировано 4105 преступлений, но предъявлено обвинение и направлены в суд для постановления обвинительного приговора уголовные дела по 375 преступлениям, т.е. чуть больше 9 %[6].

При этом количество выявленных профессиональных технотронных преступников, а именно лиц, совершивших преступления в сфере

---

[6] Форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за 2020 год.

компьютерной информации, также неуклонно снижалось в последние годы. Так, например, с 2010 по 2020 годы число выявленных лиц, совершивших неправомерный доступ к компьютерной информации (ст. 272 УК РФ), сократилось с 3973 до 247 (более чем в 16 раз)[7].

Поэтому данные официальной статистики указывают на неспособность правоохранительных органов в настоящее время сдержать и нейтрализовать технотронную преступность.

3. Крэкеры, майнеры, вирусмейкеры и прочие профессиональные технотронные преступники образуют теневую технократию, неконтролируемую обществом, но оказывающую на общество и его институты (государство, СМИ, политические партии, местное самоуправление, избирательную систему и процесс, финансово-банковскую систему и др.) сильное негативное воздействие.

4. В рамках информационных войн, происходит симбиоз преступной технократии с государственными спецслужбами, для осуществления последними кибершпионажа, киберсаботажа, кибершантажа и других высокотехнологичных преступлений с целью оказания политического, экономического, финансового давления на критическую инфраструктуру государств-соперников. Технотронные преступники, работая по найму, выполняют «государственный заказ» спецслужб, который в силу действия правового режима государственной тайны является негласным для общества, а, следовательно, неконтролируемым со стороны социума.

5. Эволюция компьютеров, информационно-коммуникационных систем, привела к применению в преступных целях новых компьютерных устройств, технологий искусственного интеллекта, облачных и туманных вычислений, интернета вещей, промышленного интернета, т.е. технологий, работающих автономно без участия человека и в режиме «самообучения», что также выводит технотронную преступность из-под контроля человека и общества.

---

[7] Форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за 2010-2020 год.

6. Вирусмейкеры (вирусописатели) создают вредоносные компьютерные программы-генераторы, которые в свою очередь, производят компьютерные вирусы целыми семействами (штаммами), что приводит к неконтролируемому появлению их в мировом киберпространстве от нескольких десятков до нескольких сотен тысяч в день. При этом, вирусмейкеры знают только основной код исходной вредоносной компьютерной программы, часто не представляя всех функциональных свойств модификаций основной программы, а также не всегда обладая возможностью уничтожить либо блокировать созданный компьютерный вирус, что приводит к выходу последних из-под контроля своих создателей и человеческого общества, причиняя огромный материальный ущерб.

7. Масштабное использование технотронными преступниками анонимных информационно-коммуникационных сетей (например, TOR, Freenet, Zeronet и др.) и мессенджеров (Wickr, Brosix, Jabber и др.) для совершения преступных деяний также обусловил процесс выхода из-под контроля правоохранительных органов технотронной преступности.

8. Современные технотронные преступники легализуют доходы от преступной деятельности, финансируют, получают плату за совершение противоправных действий, используя неконтролируемые государством и обществом криптовалюты (Bitcoin, Litecoin, Ethereum и др.), которые являются анонимными электронными средствами платежа и фактически составляют финансовую основу технотронной преступности.

9. Организованные преступные группы бесконтрольно совершают преступления, как на территории России, так и на территории зарубежных стран. При этом противоправной деятельности технотронных преступников не препятствуют ни государственные границы, ни таможенный, полицейский или пограничный контроль.

10. Неконтролируемость технотронной преступности вытекает из несовершенства правового механизма международного сотрудничества между российскими и зарубежными правоохранительными органами. В настоящее

время, отсутствует конвенция ООН о противодействии компьютерной преступности, а двухсторонние договоры о взаимной правовой помощи по уголовным делам между Российской Федерацией и такими странами как Великобритания, Канада, Колумбия, США, Япония и др., не предусматривают возбуждение уголовного преследования и последующую выдачу лиц, совершивших компьютерные преступления (экстрадицию) по запросам России.

В параграфе 4 «Специфика личности компьютерного преступника» проводится исследование личностных свойств (качеств) компьютерного преступника в условиях его трансформации в технотронного преступника.

Анализируются результаты проведенного автором исследования личности 300 компьютерных преступников, в результате формулируется вывод о типовом портрете российского технотронного преступника.

Типичным технотронным (компьютерным) преступником в России является гражданин Российской Федерации, мужчина в возрасте 18 - 35 лет, городской (местный) житель, не состоящий в семейном браке (холост либо разведен); имеющий среднее (полное) общее либо среднее профессиональное образование; обладающий навыками, умениями, опытом работы в информационно-коммуникационных сетях и на компьютерных устройствах; наемный работник или служащий, имеющий доступ к служебным компьютерным устройствам, компьютерным сетям и базам данных (системный администратор, менеджер, консультант и т.п.), в том числе недавно уволенный с работы наемный работник или служащий (не имеющий постоянного финансового дохода, но не получивший официальный статус безработного), который в силу трудовых (служебных) обязанностей имеет (имел) доступ к служебным компьютерным устройствам, компьютерным сетям и базам данных. В прошлом судимости не имел и к уголовной ответственности не привлекался. Преступления предпочитает совершать в одиночку, т.к. обладает низкой социальной коммуникативностью. Преступная деятельность характеризуется множественностью совершенных деяний.

С позиции научно-технических качеств, среднестатистический технотронный преступник постоянно занимается самообразованием и поддержанием своего профессионально-технического уровня, стараясь быть специалистом высокого класса.

В свою очередь, если вести речь о профессиональных компьютерных (технотронных) преступниках, то при тех же половозрастных, семейных, юридических и других криминологических характеристиках, что и у типичных компьютерных преступников, среди них значительно возрастает доля лиц, имеющих высшее образование (с 11,2 до 27,2 %, т.е. более чем в 2 раза) и обладающих более высоким социальным статусом и должностным положением. В частности, среди них больше доля лиц занимающих должности руководителей (технические директора, начальники отделов, лабораторий и т.д.), высококвалифицированных специалистов (главный специалист, ведущий специалист, инженер-программист) в коммерческих организациях (увеличение с 11,5 до 33,2 %, т.е. почти в 3 раза) и как следствие меньшее количество граждан не имеющих постоянного финансового дохода (снижение с 63,0 до 31,6, т.е. в 2 раза)[8].

Автор приходит к выводу, что за истекший период произошли существенные изменения в возрастной и социальной характеристике личности технотронного преступника: если в конце 1990-х – начале 2000-х годов среди компьютерных преступников преобладали «скрипткидди», т.е. молодежь (школьники, учащиеся или студенты образовательных учреждений в возрасте до 25 лет), не обладающая профессиональными навыками и опытом работы в сфере IT-технологий, то в настоящее время, это люди более зрелые (возраст до 35 лет), работающие (либо недавно уволенные специалисты) в сфере предоставления банковских, коммерческих, информационных и иных высокотехнологических услуг.

---

[8] Форма федерального статистического наблюдения № 2-ЕГС «Сведения о лицах, совершивших преступления». Раздел 1. Сведения о возрастных, гендерных, образовательных и криминологических характеристиках лиц, совершивших преступления за 2020 год.

Обращается внимание, что в настоящее время среди лиц, совершающих технотронные преступления, увеличилось количество женщин, которые составили около 22,7 % от общего числа преступников (ранее около 1-2 %). Материалы судебно-следственной практики показывают, что в основном это девушки или молодые женщины в возрасте до 25 лет, не замужем либо разведенные (в этом случае имеют на иждивении 1-2 малолетних детей); безработные; имеющие общее среднее образование; не являющиеся специалистами в области IT-технологий и не обладающие техническим образованием. Данные лица совершали несложные с технической точки зрения преступные деяния, которые не требовали от них наличия специальных знаний, навыков, умений в сфере IT-технологий (например, незаконный взлом электронной почты, страниц и аккаунтов своих знакомых в социальных сетях; хищения электронных денежных средств с использование логинов, паролей, компьютерных кодов, которые были ранее ими похищены, либо получены обманным путем).

Предлагается разделять технотронных преступников не только по уровню их профессиональной подготовки, социальному положению, мотивам совершения деяния, но и по нравственно-психологическим особенностям их личности, выделив три типа лиц, совершающих технотронные преступления.

К первому типу, условно обозначенному автором как «социально-дезодаптированный», относятся лица, характерными чертами которых является аутизация и интравертность, т.е. уход в себя, отгороженность от окружающих, направленность интересов лишь на удовлетворение своих собственных, в основном нематериальных, информационных потребностей. Для таких лиц достаточно важным является причисление себя к классу «хакеров», т.е. отождествление с одной из существующих социальных групп, посредством чего они внутренне хотят преодолеть свое социальное отчуждение, почувствовать свою значимость, а также получить возможность быть уверенным и понятым в этой социальной среде (например, «хакеры» или

«одержимые программисты», новички - «скрипт кидди» и другие некорыстные преступники).

Ко второму типу, условно обозначенному автором «эмоционально-восприимчивый», предлагается относить лиц, которые приобщились к совершению преступлений, для удовлетворения своих личных интересов и потребностей. Этот тип лиц обладает повышенной восприимчивостью и особой чувствительностью ко всему, что касается интересов личности. В основном данный тип преступников совершает правонарушения из корыстных мотивов с целью удовлетворения своих материальных потребностей, реже потребности в знаниях, либо других интересах. В отличие от правонарушителей первого типа, это лица, обладающие лидерскими наклонностями, с достаточно высоким уровнем интеллекта. Они самолюбивы, проявляют завидную энергию и активность в достижении поставленных целей, гибкость и легкость в общении, установлении социальных контактов (например, «белые воротнички», «крэкеры», «вирусмейкеры», «майнеры», «фримеры» и другие профессиональные преступники).

Третий тип, названный автором как «социально-неадекватный», представлен в основном молодыми людьми с высшим образованием, высоким интеллектуальным уровнем, материально обеспеченными. Корысть и удовлетворение материальных интересов для них не имеют значения, на первый план выходит удовлетворение иных, нематериальных потребностей. Для этих лиц характерны политические, хулиганские или исследовательские мотивы (например, «компьютерные шпионы», «вандалы», «хактивисты» и др.).

Глава 2 «Комплекс факторов, детерминирующих компьютерную преступность» состоит из трех параграфов.

В параграфе 1 «Основные факторы компьютерной преступности в Российской Федерации» рассматриваются основные факторы, определяющие развитие современной компьютерной преступности и преобразование ее в преступность высоких технологий, т.е. технотронную.

Анализ судебно-следственной практики, статистических данных, экспертных оценок, результатов анкетирования сотрудников правоохранительных органов и компьютерных пользователей, интервью специалистов в области компьютерной безопасности, контента интернет-ресурсов, публикаций в средствах массовой информации и других общедоступных источников информации позволяет сделать вывод, что комплекс факторов компьютерной преступности достаточно разнообразен. Поэтому факторы компьютерной преступности представляется возможным классифицировать, например, по сферам общественной жизни на: социальные, экономические, юридические, кадровые, организационно-технические, политические и др.

По мнению автора, в последние годы получили развитие политические факторы совершения компьютерных преступлений.

В частности, можно вести речь о геополитических (военно-политических, глобально-экономических, международно-политических), контрольно-надзорных (отсутствие полного социального и государственного контроля (надзора) над киберпространством), политико-криминальных (кибертерроризм, киберэкстремизм, хактивизм и другие преступные деяния политической направленности), политико-информационных (кибершпионаж, «информационные» войны со стороны подконтрольных государству или иным политическим структурам мультимедиа, электронных СМИ, блоггеров и т.д.), политико-институциональных (например, противоправное использование IT-технологий в избирательных компаниях при формировании органов власти или назначении должностных лиц), а также других политических факторах компьютерной преступности.

Вместе с тем, по действию в пространстве можно выделить международные, национальные и региональные (местные) факторы компьютерной преступности. Например, корыстный мотив у компьютерных преступников и профессионализм их преступной деятельности как факторы компьютерной преступности, безусловно, носят международный характер. В

свою очередь, уровень жизни граждан, отношение средств массовой информации и общества к компьютерным преступникам являются факторами национальными. Между тем, такие факторы компьютерной преступности как уровень развития информационных технологий и компьютеризации общества, финансово-банковских институтов, доступность населения к высокотехнологичным услугам, количество компьютерных пользователей носят региональный характер. Например, количество компьютерных преступлений в Москве, Санкт-Петербурге и других технологически развитых субъектах Российской Федерации значительно выше, чем в регионах со слаборазвитой информационной инфраструктурой. Так, например, в так называемых «дотационных» регионах Северо-Кавказского и Южного федеральных округов (Республика Дагестан, Республика Ингушетия, Чеченская Республика, Республика Калмыкия, Республика Адыгея и др.) коэффициент компьютерной преступности и коэффициент преступного поведения значительно ниже общероссийских показателей, что связано с более низким уровнем развития научно-образовательной, промышленной, коммерческой, банковско-финансовой и иной информационной инфраструктуры.

По действию во времени факторы компьютерной преступности могут быть постоянными и временными (например, стремление преступников к обогащению и профессионализм компьютерной преступности – это постоянные причины данного вида преступности, а несовершенство уголовного законодательства, судебной практики, оперативно-розыскной деятельности правоохранительных органов, несомненно, носят временный характер).

По характеру возникновения факторы компьютерной преступности могут быть объективными (например, всеобщая компьютеризация и развитие информационно-коммуникационных технологий в современном обществе, технотронный характер человеческой цивилизации) и субъективными (существующее национальное законодательство, сложившаяся судебная практика, эффективность деятельности правоохранительных органов зависит от вполне конкретных лиц: депутатов парламента, судей, прокуроров,

следователей, а также непосредственно компьютерных преступников, которые выражают свое личное, т.е. субъективное отношение к процессу противодействия компьютерной преступности).

Автор приходит к выводу, что все факторы совершения компьютерных преступлений тесно взаимосвязаны между собой, образуя комплекс факторов, детерминирующих развитие компьютерной преступности и ее трансформацию в более высокотехнологичную – технотронную преступность.

Параграф 2 «Процесс самодетерминации компьютерной преступности как основополагающий фактор ее генезиса и трансформации в технотронную преступность» посвящен анализу процесса самопроизводства компьютерной преступности в условиях преобразования ее в технотронную преступность.

Автор приходит к выводу, что самодетерминация компьютерной преступности представляет собой способность данного вида преступности автономно репродуцировать, т.е. самостоятельно воспроизводить в социальной среде компьютерные преступления.

Самодетерминацию компьютерной преступности предлагается рассматривать в узком и широком смыслах.

В широком смысле самодетерминация компьютерной преступности выступает внутрисистемным и качественным признаком ее как противоправного и негативного социального явления, наряду с такими имманентными свойствами как высотехнологичность, латентность, организованность, профессиональный характер, транснациональность, трансграничность и др.

В свою очередь самодетерминация компьютерной преступности в узком смысле, с нашей точки зрения, представляет собой один из основных факторов (причин, условий, обстоятельств и т.д.) возникновения, существования и развития компьютерной преступности не только в России, но и в зарубежных странах, который носит комплексный характер.

Для более полной криминологической оценки процесса трансформации компьютерной преступности в технотронную преступность, существующие причины, условия, обстоятельства самодетерминации компьютерной преступности как фактор ее генезиса и трансформации в технотронную преступность предлагается классифицировать по видам:

1) по способу воздействия на:

- прямые, т.е. непосредственно оказывающие влияние на процесс самовоспроизводства компьютерных преступлений (существование организованной, профессиональной преступности, противоправное использование IT-технологий для совершения преступлений других видов, латентность компьютерных преступлений, криминальная субкультура компьютерных преступников и др.);

- косвенные, действующие опосредовано на самодетерминацию компьютерной преступности (всеобщая информатизация современного общества, развитие высоких технологий, деятельность СМИ, недостатки национального законодательства и др.);

2) по направленности действия на:

- внешние (например, использование глобальных информационно-телекоммуникационных сетей и мессенджеров, промышленного интернета, интернета вещей, дистанционных банковских услуг, криптовалют, электронной коммерции, применение облачных и туманных вычислений, т.е. всеобщая информатизация систем связи, коммерции и логистики, цифровизация экономики, применение искусственного интеллекта в различных социальных сферах);

- внутренние (например, криминальная субкультура компьютерных преступников, национальное уголовное законодательство, уровень благосостояния граждан).

3) в зависимости от уровня воздействия на:

- международные (международная организованная преступность, трансграничная преступность, транснациональная преступность, недостатки международного уголовного права);

- национальные (уровень информатизации общества, правовая аномия общества, безразличное отношение общества к компьютерным преступникам);

- региональные (рецидивная преступность, региональная экономика и инфраструктура);

- местные (пенитенциарная преступность, «теневая юстиция», комфортность проживания в населенных пунктах и доступность информационно-телекоммуникационных услуг для местных жителей);

4) по социальным сферам на:

- политические (политическая преступность, влияние хактивистских движений на политический строй и партийную систему, особенности избирательного процесса, симбиоз хакерского сообщества с государственными разведывательными и контрразведывательными службами, и т.д.);

- экономические (экономическая преступность, уровень цифровизации экономики, доступность дистанционных банковских и финансовых услуг, использование электронных средств платежа, в т.ч. криптовалют; интернет-коммерция);

- научно-технические (существующая система научных и образовательных учреждений, технопарков, высокотехнологических производств по разработке программного обеспечения; производства чипов и микросхем, сборки компьютерных устройств, рынок инновационных продуктов в сфере использования IT-технологий).

- социально-бытовые (социальные сети, интернет вещей, детские электронные гаджеты и др.);

- образовательно-культурные (уровень технической образованности общества, уровень правовой культуры общества, существование различных криминальных субкультур и идеологий);

- юридические (особенности национального законодательства, недостатки судебной и пенитенциарной системы, уровень индивидуального и общественного правосознания, уровень правовой защищенности и доступности юридических (правоохранительных) услуг для граждан);

5) по кругу лиц на:

- общие (корыстная преступность, увеличение количества компьютерных пользователей, пользователей социальных сетей, получателей информационно-коммуникационных услуг);

- групповые (организованная преступность, профессиональная преступность, преступность несовершеннолетних, женская преступность);

- индивидуальные (пол, возраст, образование, технические навыки, индивидуальное правосознание, преступная специализация компьютерного преступника: вирусмейкер, крэкер, майнер, кардер и т.д.).

В результате исследования, автор приходит к выводу, что самодетерминация компьютерной преступности как способность автономно репродуцировать в социальной среде компьютерные преступления, является одной из основных детерминант ее генезиса и трансформации в технотронную преступность.

В параграфе 3 «Эволюция вредоносных компьютерных программ как базовый фактор генезиса компьютерной преступности» обращается внимание на то, что вредоносные компьютерные программы как орудия и средства совершения преступных деяний постоянно совершенствуются и усложняются, а процесс их противоправного генезиса является одной из основных детерминант компьютерной преступности и ее эволюционирования в технотронную преступность.

Проведенный автором анализ экспертных отчетов (Group-IB, Dr.Web, Symantec, «Лаборатория Касперского», ПАО Сбербанк и др.) показал, что количество выявленных компьютерных вирусов постоянно увеличивается (ежегодно детектируется несколько десятков миллионов новых объектов) и растет число совершенных ими в автоматическом режиме кибератак

(исчисляются каждый год несколькими миллиардами). При этом в отличие от простейших компьютерных вирусов конца 1990-х – начала 2000-х годов, современные вирусы уже представляют многофункциональные сложные вредоносные компьютерные программы с повышенным уровнем мимикрирования (маскировки, адаптации), скрытности и способности к самоуничтожению.

Эволюция вредоносных компьютерных программ привела к тому, что в настоящее время компьютерные вирусы возникают уже целыми семействами (штаммами). Данный факт позволяет прийти к выводам, что производство такого количества вирусов и программ становится физически невозможным для отдельных «вирусмейкеров», что компьютерные вирусы в таком количестве моделируются специальными вредоносными компьютерными программами-генераторами, программами-конструкторами (иногда с элементами искусственного интеллекта), изначально написанными для этих целей вирусмейкерами (вирусописателями). Как следствие, процесс создания и размножения «штаммов» компьютерных вирусов стал практически полностью автоматизированным и часто осуществляется без вмешательства человека.

При этом вирусмейкер, создавший подобные программы для производства компьютерных вирусов не всегда знает полный цифровой код модификаций последних, а, следовательно, способов их блокирования либо уничтожения.

Это приводит к неконтролируемости процесса размножения указанных модификаций вирусов и как следствие к глобальным эпидемиям компьютерных устройств, причиняющих обществу огромный материальный ущерб.

Ярким примерами являются случаи с вирусописателями Чэнь Инхао, Баситом Фаруком Алви, Робертом Моррисом, Крисом Пайлом, Дэвидом Смитом, Яном де Витом и др., создавшими и распространившими вирусы, что привело к масштабным компьютерным эпидемиям и многомиллионным убыткам владельцев компьютеров. Вирусмейкеры вынуждены были добровольно сдаваться и идти на сотрудничество с

правосудием, в надежде на смягчение наказания, т.к. самостоятельно уже не могли предотвратить распространение компьютерного вируса (соответствующий антивирус ими не создавался).

Таким образом, эволюция вредоносных компьютерных вирусов в искусственный интеллект, т.е. автономную и самообучающуюся компьютерную программу, по мнению автора, приводит к становлению неконтролируемой технотронной преступности и процессу ее самодетерминации.

Глава 3 «Организация и система мер противодействия компьютерной преступности» состоит из четырех параграфов, в которых исследуется организационно-правовая основа и система мер противодействия компьютерной преступности в условиях ее технологической трансформации как на международном уровне, так и в Российской Федерации.

В параграфе 1 «Организационно-правовые основы противодействия компьютерной преступности в России» расматриваются понятие, цели, задачи, принципы, субъекты системы противодействия компьютерной преступности, правовые основы их деятельности, анализируется состояние существующей системы противодействия компьютерной преступности.

Для повышения эффективности системы противодействия компьютерной преступности, автором обосновывается необходимость расширения сферы деятельности негосударственных правоохранительных организаций: народных дружин (кибердружин), частных охранных предприятий, частных детективных агентств по выявлению, предупреждению, пресечению компьютерных преступлений путем обеспечения необходимым программно-аппаратным оборудованием и техническими специалистами, законодательного закрепления полномочий по охране компьютерной информации и информационно-коммуникационных сетей физических и юридических лиц, поиску утраченной компьютерной информации, выявлению и блокированию противоправного контента в информационно-коммуникационных сетях, включая сеть Интернет.

В частности, предлагается дополнить Федеральный закон от 2 апреля 2014 года № 44-ФЗ «Об участии граждан в охране общественного порядка» положениями о «кибердружинах» и «кибердружинниках», уравняв последних по правовому статусу с народными дружинниками, предусмотрев государственную регистрацию «кибердружин» и включение их в региональные реестры общественных объединений правоохранительной направленности.

Также, расширить содержание статьи 3 Закона Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации», включив в перечень видов охранных и сыскных услуг такие услуги как «охрана компьютерной информации, находящейся в собственности, во владении, в пользовании, хозяйственном ведении, оперативном управлении или доверительном управлении физических и (или) юридических лиц» и «поиск утраченной гражданами или предприятиями, учреждениями, организациями компьютерной информации».

Кроме того, автор приходит к выводу, что правовая основа компьютерной преступности состоит из большого количества нормативных правовых актов.

В связи с чем, требуется систематизация последних путем принятия кодифицированного Федерального закона «О противодействии компьютерной преступности в Российской Федерации», который бы определил понятийно-терминологический аппарат, правовые основы противодействия компьютерной преступности; систему субъектов профилактики, борьбы и нейтрализации проявлений компьютерных преступлений, их полномочия и ответственность; общие и специальные меры противодействия компьютерной преступности.

Автор приходит к выводу, что реальное состояние системы противодействия компьютерной преступности показывает ее неэффективность в профилактике, борьбе и нейтрализации проявлений преступлений, совершенных с использованием компьютерных. информационно-коммуникационных и иных высоких технологий, требуя серьезной модернизации ее организационно-правовых основ.

В параграфе 2 «Общие меры противодействия компьютерной преступности в России» рассматриваются цели, задачи и система общих мер по противодействию компьютерной преступности.

Автор приходит к выводу, что общие меры противодействия компьютерных преступлений носят всеобщий политический, экономический, социальный, научно-технический, духовно-культурный характер, и направлены на противодействие, как компьютерной преступности в частности, так и технотронной преступности в целом.

Данные меры закреплены в нормативных правовых актах, регулирующих общественные отношения в сферах национальной безопасности, информационной безопасности, научно-технологического развития, развития искусственного интеллекта.

По мнению автора пристальное внимание необходимо уделять общим научно-техническим мерам противодействия компьютерной преступности: развитию информационной и коммуникационной инфраструктуры Российской Федерации; созданию и применению российских информационных и коммуникационных технологий; средств по обработке больших объемов данных; развитию технологий в сфере искусственного интеллекта, облачных и туманных вычислений; интернета вещей и индустриального интернета; проведению научно-исследовательских и опытных работ по созданию новых информационных технологий и средств обеспечения информационной безопасности.

Наряду с этим, важная роль в механизме противодействия компьютерной преступности отводится институтам гражданского общества, которые во взаимодействии с государственными органами являются серьезным инструментом для выявления и блокирования противоправного контента в киберпространстве. Кроме того, вышеуказанные институты могут осуществлять общественный контроль за эффективностью противодействия компьютерной преступности в деятельности правоохранительных органов и

соблюдению последними общеправовых принципов: уважения прав и свобод человека и гражданина, законности, гласности и др.

Параграф 3 «Система специальных мер противодействия компьютерной преступности» посвящен исследованию специальных мер противодействия компьютерной преступности.

Автором предложена система мер, направленных на противодействие компьютерной преступности в условиях ее преобразования в технотронную преступность:

- правовых (совершенствование действующего уголовного и информационного законодательства, судебно-следственной практики, активизация и совершенствование международно-правового сотрудничества в сфере предупреждения и борьбы с компьютерными преступлениями);

- духовно-культурных (активное привлечение средств массовой информации в предупреждении компьютерных преступлений, правовое воспитание молодежи, формирование индивидуальной и общественной культуры информационной безопасности),

- организационно-управленческих и технических (подготовка специалистов для правоохранительных органов, формирование в технических и ведомственных ВУЗах специализированных научно-исследовательских лабораторий по созданию и модификации программных систем компьютерной защиты с правом реализации (продажи) своей продукции заинтересованным физическим и юридическим лицам и криминалистических; курсы обучения и повышения квалификации для сотрудников служб безопасности банков, предприятий, учреждений, либо заинтересованных компьютерных пользователей; взаимодействие органов правоохранительных органов со средствами массовой информации в рамках межведомственных рабочих групп, комиссий, координационных советов и т.д.; создание национальной операционной системы для компьютерных устройств, а также общенациональной системы фиксации, анализа компьютерных преступлений, учета компьютерных преступников, выбора оптимальных решений и т.д.),

- криминалистических (совершенствование уголовно-процессуального законодательства; создание новых и совершенствование существующих методик выявления, пресечения, раскрытия, расследования компьютерных преступлений; привлечение к расследованию сложных преступлений экспертов в области информационной безопасности из «Лаборатории Касперского», «Dr.Web», «Group-IB» и др.).

При этом предложенная система специальных мер противодействия компьютерной преступности, по мнению автора, даст положительный эффект при реализации его правоохранительными органами во взаимодействии с институтами гражданского общества.

В параграфе 4 «Международное сотрудничество в сфере противодействия компьютерной преступности» автор на основе проведенного исследования приходит к выводу о том, что Российская Федерация в последние годы усилила международное сотрудничество по противодействию компьютерной преступности в рамках межгосударственных организаций СНГ, БРИКС и ШОС, G-20, что связано как с совершенствованием взаимодействия с крупнейшими странами мира (Китай, Индия, Пакистан, Бразилия и др.), так и созданием альтернативы деятельности межгосударственных организаций «G-7», НАТО, ЕС и др., в которых США и большинство европейских государств проводят в отношении нашей страны политику «международной изоляции», путем введения политических, экономических, научно-технических и иных санкций.

Поэтому СНГ, ШОС и БРИКС стали для Российской Федерации новыми международными платформами для эффективного взаимодействия в области противодействия компьютерной и технотронной преступности, которое осуществляется в рамках ранее принятых международно-правовых актов.

Необходимо отметить, что серьезное значение по противодействию компьютерной преступности имеет участие Российской Федерации в Международной организации уголовной полиции (Интерпол), которое осуществляется с 1996 года.

Оптимальным решением вопроса международного сотрудничества в

сфере противодействия компьютерной преступности, по мнению автора, является принятие специальной конвенции Организации Объединенных Наций, которая должна содержать понятийно-терминологический аппарат; общие организационно-правовые принципы; комплекс криминологических, криминалистических и организационно-технических мер по противодействию компьютерной преступности; механизм международного взаимодействия правоохранительных органов в указанной сфере.

В рамках научного исследования диссертантом по данному вопросу был проведен соответствующий социологический опрос и проанкетировано две группы респондентов: экспертов (410 прокурорских работников) и компьютерных пользователей (410 студентов юридических ВУЗов г. Иркутска). Результаты анкетирования подтвердили научную позицию автора. За необходимость принятия вышеуказанного международного правового акта высказалось 79,5% прокурорских работников и 79,8 % компьютерных пользователей, т.е. подавляющее большинство опрошенных.

Раздел II «Уголовно-правовые меры противодействия компьютерной преступности» состоит из трех глав.

Глава 1 «Международно-правовые и компаративистские аспекты уголовно-правового противодействия компьютерной преступности» посвящена сравнительно-правовому анализу норм международного и зарубежного уголовного права в части регламентации ответственности за совершение компьютерных преступлений, включает два параграфа.

В параграфе 1 «Международные уголовно-правовые меры противодействия компьютерной преступности» анализируются нормы международного права, образующие правовой механизм уголовно-правового противодействия компьютерной преступности в условиях ее трансформации в высокотехнологическую – технотронную преступность. На основе этого анализа формулируется вывод автора о необходимости принятия на уровне Организации Объединенных Наций специальной Конвенции о противодействии компьютерной и технотронной преступности, которая бы

стала международно-правовым фундаментом предупреждения, борьбы, минимизации и ликвидации последствий компьютерных преступлений.

В настоящее время международные уголовно-правовые основы противодействия компьютерной преступности основываются на Конвенции Совета Европы о компьютерных преступлениях от 23 ноября 2001 года (далее – Конвенция о киберпреступности), которая не ратифицирована Российской Федерацией, и соответствующих декларациях Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, носящих рекомендательный характер.

По мнению автора, для совершенствования международного механизма противодействия компьютерной преступности, обеспечения международной информационной безопасности и укрепления уголовно-правовых основ борьбы с компьютерными преступлениями, а также разграничения уголовно-правовых и политических аспектов в указанных сферах, требуется принятие двух международных правовых актов: Конвенции Организации Объединённых Наций по противодействию компьютерной и технотронной преступности, а также Конвенции Организации Объединённых Наций по обеспечению международной информационной безопасности.

Автор приходит к выводу, что Конвенция Организации Объединённых Наций по противодействию компьютерной и технотронной преступности в отличие от Конвенции Организации Объединённых Наций по обеспечению международной информационной безопасности должна носить специальный уголовно-правовой и уголовно-процессуальный характер, включая: понятийно-терминологический аппарат; общие организационно-правовые принципы; перечень преступных деяний, подлежащих криминализации в законодательстве стран-участниц; систему уголовно-правовых и уголовно-процессуальных норм, регламентирующих наказание за компьютерные преступления и общую процедуру привлечения виновных к уголовной ответственности; комплекс криминологических, криминалистических и организационно-технических мер по противодействию компьютерной преступности; систему и механизм

международного взаимодействия правоохранительных органов в указанной сфере (например, выполнение совместных следственных и оперативно-розыскных мероприятий, предоставление информации по запросам стран-участниц, порядок и процедуру экстрадиции компьютерных преступников, обмен данными о компьютерных преступлениях и лицах их совершающих, ведение общей криминалистической базы данных, проведение совместных, либо по запросам сторон судебно-компьютерных экспертиз и иных криминалистических экспертиз, а также иные виды международного сотрудничества).

В параграфе 2 «Зарубежный опыт уголовно-правового противодействия компьютерной преступности» проводится сравнительно-правовой анализ зарубежного уголовного законодательства в части регламентации составов компьютерных преступлений и ответственности за их совершение для определения уголовно-правовых основ противодействия компьютерной преступности и ее новой эволюционной форме – технотронной преступности.

В результате сравнительно-правового исследования уголовного законодательства Великобритании, Германии, Дании, Италии, Китая, Нидерландов, США, Франции, Швеции, стран СНГ и Балтии, автор приходит к выводу о необходимости снижения возраста привлечения к уголовной ответственности компьютерных преступников с 16 до 14 лет (в случае наступления тяжких последствий), введения в Уголовный кодекс Российской Федерации института уголовной ответственности юридических лиц и новых составов преступлений, а также ужесточения наказания за совершение компьютерных преступлений (в случае, если деяние повлекло наступление тяжких последствий) до 15 лет лишения свободы.

Глава 2 «Уголовно-правовая характеристика компьютерных преступлений» содержит четыре параграфа, где проводится анализ составов компьютерных преступлений, регламентированных Уголовным кодексом Российской Федерации, в частности, преступлений в сфере компьютерной

информации и деяний, совершенных с использованием информационно-телекоммуникационных технологий.

В параграфе 1 «Объект и предмет компьютерных преступлений» исследуются объект и предмет преступлений в сфере компьютерной информации, деяний, совершенных с использованием информационно-телекоммуникационных сетей, т.к. уголовное законодательство Российской Федерации не содержит понятия «компьютерные преступления».

В диссертации автор приходит к выводу о множественности объектов компьютерного преступления, что связано масштабным проникновением IT-технологий во многие сферы общественных отношений, охраняемых уголовным законом.

В преступлениях в сфере компьютерной информации и деяний, совершенных с использованием информационно-телекоммуникационных сетей, наряду с основным непосредственным объектом преступного посягательства могут присутствовать также дополнительный и факультативный объекты преступления (например, общественные отношения в сфере собственности, интересы службы, конституционные права человека на информацию, достоинство, тайну частной, семейной жизни, переписки и др.).

По мнению автора, непосредственным объектом преступлений в сфере компьютерной информации выступают охраняемые законом права и интересы собственников (владельцев) компьютерной информации в сфере безопасной обработки, распространения, защиты компьютерной информации, а также безопасного функционирования компьютерных устройств, информационно-телекоммуникационных сетей и иных средств создания, использования, распространения компьютерной информации.

Непосредственным объектом преступления, предусмотренного ст. 274^1 УК РФ, будут выступать охраняемые законом права и интересы собственников (владельцев) компьютерной информации в сфере безопасной обработки, распространения, защиты компьютерной информации, а также безопасного функционирования информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления и иных

объектов критической информационной инфраструктуры Российской Федерации.

Понятие компьютерной информации, сформулированное в примечании к ст. 272 УК РФ автор, с учетом дальнейшего развития высоких технологий, предлагает изложить в следующей редакции: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме любых сигналов физического характера (механических, электрических, квантовых, гравитационных, молекулярных и т.п.), независимо от средств их создания, хранения, обработки и передачи».

При этом предмет преступного посягательства, предусмотренный ст. ст. 272-274[1] УК РФ, автор полагает возможным рассматривать в широком и узком смысле.

В узком смысле предметом преступления выступают: соответственно охраняемая законом компьютерная информация; средства ее хранения, обработки, передачи и защиты, а также информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, оконечное оборудование, в том числе относящиеся к объектам критической информационной инфраструктуры Российской Федерации.

В широком смысле предметом преступлений в сфере компьютерной информации будут являться IT-технологии (информационные технологии), находящиеся в законном владении, распоряжении, пользовании физических и юридических лиц.

Специфика объекта и предмета преступного посягательства, а также использование высоких технологий в качестве орудий и средств совершения различного вида преступлений, обуславливает, по мнению автора, необходимость переименования главы № 28 Уголовного кодекса Российской Федерации с «Преступления в сфере компьютерной информации» на «Технотронные преступления».

В параграфе 2 «Объективная сторона компьютерных преступлений» анализируется объективная сторона преступлений в сфере компьютерной информации, предусмотренных ст. ст. 272-274[1] УК РФ, а также деяний, совершенных с использованием информационно-телекоммуникационных сетей и технологий (ст. ст. 128[1], 137, 138, 146, 147, 158, 159, 159[1]-159[6], 163, 171[2], 183, 187, 228[1], 230, 242-242[2], 280, 282 УК РФ и др.).

Исследование российского и зарубежного законодательства, научных работ, материалов судебно-следственной практики, экспертных данных и других источников приводит автора к выводам:

– о пробеле российского уголовного законодательства в части регламентации хищения компьютерной информации и ее физических носителей с целью неправомерного доступа к информации ограниченного доступа, что обуславливает необходимость криминализации указанного деяния и дополнения главы 28 УК РФ статьей 272[1] «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации» и статьей 272[2] «Перехват компьютерной информации с целью ее незаконного уничтожения, блокирования, модификации, копирования или нейтрализации средств защиты»;

– о необходимости криминализации нового состава преступления – создания, приобретения, использования и распространения в преступных целях инфицированных вредоносными компьютерными программами и объединенных в общую сеть компьютеров либо иных компьютерных устройств, удаленно используемых преступниками для совершения различного вида противоправных деяний, что требует дополнения главы 28 УК РФ статьей 273[1] «Создание, приобретение, использование и распространение вредоносной компьютерной сети (ботнета)».

Существующая в научном сообществе дискуссия о размере крупного ущерба, причиненного преступлением в сфере компьютерной информации и коллизия уголовно-правовых норм, устанавливающих различный размер крупного ущерба для смежных видов преступлений, уровень доходов

населения и коммерческих организаций, позволяет автору предложить снизить размер причиненного крупного ущерба с одного миллиона рублей до ста тысяч рублей.

В связи атрибутивностью существующего в российском уголовном праве института соучастия в преступлении, предлагается криминализировать деяние в виде «приобретения» вредоносных компьютерных программ для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, внеся соответствующее дополнение в диспозицию уголовно-правовой нормы, предусмотренной ч. 1 ст. 273 УК РФ.

В параграфе 3 «Субъект компьютерных преступлений» проводится анализ признаков субъекта преступлений в сфере компьютерной информации (ст. ст. 272-274[1] УК РФ), а также деяний, совершенных с использованием информационно-телекоммуникационных технологий (ст. ст. 128[1], 137, 138, 146, 147, 158, 159, 159[1]-159[6], 163, 171[2], 183, 187, 228[1], 242-242[2], 280, 282 УК РФ и др.), с учетом того, что российское уголовное законодательство не выделяет такой вид преступных деяний как «компьютерные преступления».

В результате проведенного исследования, автор приходит к выводам:

– о необходимости снижения возраста привлечения к уголовной ответственности с 16 до 14 лет, для вменяемых физических лиц совершивших преступления в сфере компьютерной информации, которые повлекли наступление тяжких последствий;

– о неизбежности и целесообразности введения в российское уголовное право института ответственности юридических лиц, поддерживая принятие находящегося с 2015 г. на рассмотрении в Государственной Думе Российской Федерации проекта Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с введением института уголовной ответственности юридических лиц» № 750443-6.

Параграф 4 «Субъективная сторона состава компьютерных преступлений» посвящен рассмотрению особенностей субъективной стороны состава преступлений в сфере компьютерной информации и деяний,

совершенных с использованием информационно-телекоммуникационных технологий.

С целью всесторонней и полной квалификации рассматриваемых деяний, эффективной и объективной дифференциации уголовной ответственности за преступления в сфере компьютерной информации, предлагается криминализировать ряд преступных мотивов, дополнив диспозиции ст. ст. 272 - 274^1 УК РФ новыми квалифицирующими признаками: «те же деяния, совершенные из хулиганских побуждений», «те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и (или) местного самоуправления, государственных и (или) муниципальных учреждений, предприятий».

В главе 3 «Проблемы совершенствования уголовного законодательства и практики его применения в сфере противодействия компьютерной преступности» исследуются проблемы квалификации компьютерных преступлений при расследовании и судебном рассмотрении уголовных дел, предлагаются основные направления совершенствования Уголовного кодекса Российской Федерации в части регламентации составов компьютерных преступлений и ответственности за их совершение.

В параграфе 1 «Проблемы квалификации компьютерных преступлений при расследовании и судебном рассмотрении уголовных дел» проводится анализ сложившейся в Российской Федерации судебно-следственной практики по уголовным делам о компьютерных преступлениях, основу которых составляют преступления в сфере компьютерной информации.

В результате автор приходит к выводу, что при квалификации хищений денежных средств с помощью IT-технологий, хищений денежных средств из банкоматов и платежных терминалов, незаконном использовании поддельных платежных карт, целенаправленных DDoS-атак на информационные ресурсы органов власти, организаций, предприятий, учреждений и др., нередко допускаются ошибки в юридической оценке совершенных деяний.

Отсутствие единообразной судебно-следственной практики при рассмотрении и расследовании, в первую очередь, уголовных дел о преступлениях в сфере компьютерной информации, требует доведения до судов соответствующих разъяснений со стороны Верховного Суда Российской Федерации по вопросам правильной квалификации вышеуказанных деяний.

С целью совершенствования судебно-следственной практики по уголовным делам о компьютерных преступлениях, предлагается авторский проект постановления Пленума Верховного Суда Российской Федерации «О некоторых вопросах судебной практики при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации».

Параграф 2 «Основные направления совершенствования Уголовного кодекса Российской Федерации в части регламентации составов компьютерных преступлений и ответственности за их совершение» посвящен разработке основных путей совершенствования российского уголовного законодательства в части регламентации составов компьютерных преступлений и ответственности за их совершение в условиях трансформации компьютерной преступности в высокотехнологическую – технотронную преступность.

Автором разработан проект Федерального закона «О внесении изменений в Уголовный Кодекс Российской Федерации», который содержит соответствующие изменения и дополнения как в Общую, так и в Особенную часть УК РФ.

В частности, с точки зрения пенализации и дифференциации уголовной ответственности, диссертант предлагает дополнить пункт «к» части 1 статьи 63 УК РФ новым обстоятельством, отягчающим наказание: «с использованием компьютерных, информационно-телекоммуникационных, космических, когнитивных и иных высоких технологий».

Обосновывается необходимость изменения названия главы № 28 УК РФ с «Преступлений в сфере компьютерной информации» на «Технотронные преступления» и включение новых составов технотронных преступлений, внесение изменений в формулировку текста ст. 272, 273, 274, 274^1 УК РФ и

дополнение диспозиций имеющихся норм новыми квалифицирующими признаками.

В **заключении** изложены основные выводы и предложения диссертанта по результатам проведенного исследования.

В **приложениях** представлены авторские проекты: Федерального закона «О внесении изменений в Уголовный Кодекс Российской Федерации», Федерального закона «О внесении изменений в статью 151 Уголовно-процессуального кодекса Российской Федерации», Федерального закона «О внесении изменений в Закон Российской Федерации «Об организации страхового дела в Российской Федерации» и отдельные законодательные акты Российской Федерации», проект постановления Пленума Верховного Суда Российской Федерации «О некоторых вопросах судебной практики при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации», анкета и результаты анкетирования компьютерных пользователей и прокурорских работников по вопросам противодействия технотронной преступности, программа изучения уголовных дел и аналитическая справка о личности технотронного преступника (по результатам изучения материалов уголовных дел).

Основные положения диссертации отражены в следующих работах автора:

Статьи, опубликованные в ведущих рецензируемых журналах и изданиях, указанных в перечне Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации:

1. Евдокимов, К. Н. Вопросы уголовно-правовой квалификации неправомерного доступа к компьютерной информации и его отграничения от смежных составов преступлений [Текст] / К. Н. Евдокимов // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2009. – № 2 (10). – С. 42-46. – 0,5 п.л.

2. Евдокимов, К. Н. Субъективная сторона неправомерного доступа к компьютерной информации [Текст] / К.Н. Евдокимов // Вестник Академии

Генеральной прокуратуры Российской Федерации. – 2009. – № 4 (12). – С. 53-58. – 0,5 п.л.

3. Евдокимов, К. Н. К вопросу об объекте преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Сибирский юридический вестник. – 2009. – № 4. – С. 39-44. – 0,5 п.л.

4. Евдокимов, К. Н. К вопросу об объективной стороне создания, использования и распространения вредоносных программ для ЭВМ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2010. – № 4 (18). – С.51-55. – 0,5 п.л.

5. Евдокимов, К. Н. Субъект преступления при неправомерном доступе к компьютерной информации [Текст] / К. Н. Евдокимов // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2010. – № 5 (18). – С.52-56. – 0,5 п.л.

6. Евдокимов, К. Н. К вопросу о причинах компьютерной преступности в России [Текст] / К. Н. Евдокимов // Известия Иркутской государственной экономической академии. – 2010. – № 5 (73). – С.167-170. – 0,5 п.л.

7. Евдокимов, К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) [Текст] / К. Н. Евдокимов // Сибирский юридический вестник. – 2011. – № 1. – С.86-90. – 0,5 п.л.

8. Евдокимов, К. Н. Актуальные проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Российский следователь. – 2012. – № 6. – С.18-21. – 0,5 п.л.

9. Евдокимов, К. Н. К вопросу о совершенствовании уголовной ответственности за создание, использование, распространение вредоносных программ для ЭВМ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Известия Иркутской государственной экономической академии. – 2012. – № 3 (83). – С.136-140. – 0,5 п.л.

10. Евдокимов, К. Н. К вопросу об объекте состава преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Российский следователь. – 2012. – № 12. – С.24-27. – 0,5 п.л.

11. Евдокимов, К. Н. Актуальные проблемы совершенствования субъекта состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Сибирский юридический вестник. – 2013. – № 3. – С. 69-75. – 0,5 п.л.

12. Евдокимов, К. Н. К вопросу о совершенствовании объективной стороны состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Российский следователь. – 2013. – № 7. – С. 18-24. – 0,5 п.л.

13. Евдокимов, К. Н. К вопросу о субъективной стороне состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Российский следователь. – 2013. – № 8. – С. 22-26. – 0,5 п.л.

14. Евдокимов, К. Н. О конституционно-правовых гарантиях информационных прав и свобод человека и гражданина [Текст] / К. Н. Евдокимов // Известия Иркутской государственной экономической академии. – 2013. – № 3. – С. 106-109. – 0,5 п.л.

15. Евдокимов, К. Н. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. – 2014. – № 4 (19). – С. 33-36. – 0,5 п.л.

16. Евдокимов, К. Н. Причины компьютерной преступности в современной России [Текст] / К. Н. Евдокимов // Российский следователь. – 2015. – № 3. – С. 33-37. – 0,5 п.л.

17. Евдокимов, К. Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации [Текст] / К. Н.

Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 21-31. – 0,5 п.л.

18. Евдокимов, К.Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Российский следователь. – 2015. – № 10. – С. 24-29. – 0,5 п.л.

19. Евдокимов, К. Н. К вопросу о криминализации политических мотивов и целей при совершении преступлений в сфере компьютерной информации в Российской Федерации [Текст] / К. Н. Евдокимов // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2016. – № 1. – С. 88-91. – 0,5 п.л.

20. Евдокимов, К. Н. К вопросу о понятии, структуре и сущности компьютерной преступности в Российской Федерации [Текст] / К. Н. Евдокимов // Библиотека криминалиста. Научный журнал. – 2016. – № 1 (24). – С. 128-139. – 1 п.л.

21. Евдокимов, К. Н. Структура и состояние компьютерной преступности в Российской Федерации [Текст] / К. Н. Евдокимов // Юридическая наука и правоохранительная практика. – 2016. – № 1 (35). – С. 86-94. – 0,8 п.л.

22. Евдокимов, К. Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями [Текст] / К. Н. Евдокимов // Вестник Казанского юридического института МВД России. – 2016. – № 2 (24). – С. 62-66. – 0,5 п.л.

23. Евдокимов, К. Н. К вопросу о криминализации деяний, направленных на создание, использование и распространение «ботнетов» [Текст] / К. Н. Евдокимов // Библиотека уголовного права и криминологии. – 2016. – № 3 (15). – С.61-67. – 0,6 п.л.

24. Евдокимов, К. Н. Криминологическая характеристика личности компьютерного преступника в современной России [Текст] / К. Н. Евдокимов // Библиотека криминалиста. Научный журнал. – 2016. – № 4 (27). – С. 85-93. – 0,8 п.л.

25. Евдокимов, К. Н. Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела [Текст] / К. Н. Евдокимов // Российский следователь. – 2017. – № 4. – С. 39-44. – 0,5 п.л.

26. Евдокимов, К. Н. Особенности уголовно-правовой квалификации преступлений, предусмотренных статьями 159^6, 272 УК РФ, на стадии возбуждения уголовного дела [Текст] / К. Н. Евдокимов // Библиотека уголовного права и криминологии. – 2017. – № 2 (20). – С. 161-173. – 1 п.л.

27. Евдокимов, К. Н. Проблемные вопросы международного сотрудничества России в сфере противодействия компьютерной преступности [Текст] / С. В. Скляров, К. Н. Евдокимов // Библиотека криминалиста. Научный журнал. – 2017. – № 4 (33). – С. 269-275. (авторство не разд.). – 0,6 п.л.

28. Евдокимов, К. Н. Актуальные вопросы определения объекта преступного посягательства при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) [Текст] / К. Н. Евдокимов // Ученые записки Крымского федерального университета имени В.И. Вернадского. – 2018. – Т.12. – № 4. – С. 187-195. – 0,5 п.л.

29. Евдокимов, К. Н. Актуальные вопросы определения понятия компьютерной преступности в современной России (криминологические аспекты) [Текст] / К. Н. Евдокимов // Российский следователь. – 2018. – № 5. – С. 48-51. – 0,5 п.л.

30. Евдокимов, К. Н. Актуальные вопросы противодействия компьютерной преступности в Российской Федерации (криминологическое исследование) [Текст] / К. Н. Евдокимов // Российский следователь. – 2018. – № 10. – С. 56-61. – 0,5 п.л.

31. Евдокимов, К. Н. Некоторые уголовно-правовые аспекты определения субъекта преступления, предусмотренного статьей 274 УК РФ [Текст] / К. Н. Евдокимов // Российский следователь. – 2019. – № 5. – С.37-40. – 0,5 п.л.

32. Евдокимов, К. Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) [Текст] / К. Н. Евдокимов // Российский следователь. – 2020. – № 11. – С.41-44. – 0,5 п.л.

33. Евдокимов, К. Н. К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации [Текст] / К. Н. Евдокимов // Российский следователь. – 2021. – № 10. – С.69-72. – 0,5 п.л.

Статьи в изданиях, входящих в международные реферативные базы данных и системы цитирования:

34. Евдокимов, К. Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации [Текст] / Д. А. Липинский, К. Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9. – № 1. – С. 101-110. – 0,9 п.л.

35. Евдокимов, К. Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы [Текст] / С. В. Пархоменко, К. Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9. – № 2. – С. 265-276. – 1,1 п.л.

36. Евдокимов, К. Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации [Текст] / С. В. Скляров, К. Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. – 2016. – Т. 10. – № 2. – С. 322–330. – 0,9 п.л.

37. Евдокимов, К. Н. Регулятивная функция уголовной ответственности: понятие, структура и взаимосвязь с предупреждением преступности [Текст] / Д. А. Липинский, К. Н. Евдокимов // Всероссийский криминологический журнал. – 2017. – Т. 11. – № 3. – С. 520-530. – 1,1 п.л.

38. Евдокимов, К. Н. Проблемные вопросы квалификации преступлений, предусмотренных статьей 273 УК РФ, на стадии возбуждения уголовного дела

[Текст] / К. Н. Евдокимов, Н. Н. Таскаев // Всероссийский криминологический журнал. – 2018. – Т. 12. – № 4. – С. 590–600. – 1 п.л.

39. Evdokimov, K. N. Regulation of Criminal Responsibility for Cyber Crimes in Countries with Different Legal Systems [Text] / Dmitry A. Lipinsky, Konstantin N. Evdokimov, and Aleksandra A. Musatkina // Advances in Intelligent Systems and Computing. – 2019. – Т. 726. – P.P. 409–422. – 1,2 п.л.

40. Evdokimov, K. N. Actual problems of international cooperation of Russia in the sphere of cyber security [Text] / D. A. Lipinsky, A. A. Musatkina, K. N. Evdokimov // The Future of the Global Financial System: Downfall or Harmony «Lecture Notes in Networks and Systems» Cham, Switzerland, 2019. – P.P. 495-504. – 0,9 п.л.

41. Evdokimov, K. N. The modern technetronic society and computer crimes [Text] / Dmitry A. Lipinsky, Konstantin N. Evdokimov, and Aleksandra A. Musatkina // Advances in Intelligent Systems and Computing. – 2020. – P.P. 852-857. – 0,5 п.л.

Монографии, научно-практические и учебные пособия:

42. Евдокимов, К. Н. Проблемы противодействия неправомерному доступу к компьютерной информации: уголовно-правовые и криминологические аспекты. Монография / К. Н. Евдокимов. – Иркутск: ФГОУ ВПО «Восточно-Сибирский институт МВД РФ», 2007. – 110 с. – 5,6 п.л.

43. Евдокимов, К. Н. Проблемы квалификации и предупреждения компьютерных преступлений: монография / К. Н. Евдокимов. – Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, 2009. – 171 с. – 8,7 п.л.

44. Евдокимов, К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография / К. Н. Евдокимов. – Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2013. – 275 с. – 15,6 п.л.

45. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография / И. Г. Смирнова, К. Н. Евдокимов, О. А. Егерева, В. В. Коломинов, С. А. Машков, Д. И. Сачков, Т. М. Судакова, Е. М. Якимова; Научный редактор И. Г. Смирнова. – Москва: Издательство «Юрлитинформ», 2016. – 312 с. – 19,5 п.л. – 19,5/8,6 п.л. – С. 42-180 (раздел 3 «Криминологический анализ киберпреступности», раздел 4 «Уголовно-правовая характеристика преступлений в сфере компьютерной информации»).

46. Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография / Агапов П. В., Антонов-Романовский Г. В., Артеменков В. К., Бажанов С. В., Боголюбова Т. А., Борисов С. В., Васькина И. А., Винокуров С. И., Воеводина Т. Г., Воронцов А. А., Диканова Т. А., Евдокимов К. Н., Евланова О. А., Ережипалиев Д. И., Жидких А. А., Жубрин Р. В., Илий С. К., Капинус О. С., Коимшиди Г. Ф., Красникова Е. В. и др.; под общ. ред. Р. В. Жубрина; Академия Генеральной прокуратуры Российской Федерации. – Москва: Проспект, 2016. – 656 с. – 41,0/3,1 п.л. – С. 383-425 (глава 11 «Предупреждение компьютерной преступности» раздела 2 «Особенности предупреждения отдельных видов преступности»).

47. Евдокимов, К. Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты: монография / К. Н. Евдокимов. – Иркутск: Иркутский юридический институт (филиал) Акад. Ген. прокуратуры Рос. Федерации, 2016. – 267 с. – 15,58 п.л.

48. Криминология. Особенная часть. В 2 т. Т. 2 : учебник для академического бакалавриата / под общ. ред. О. С. Капинус. — Москва: Издательство Юрайт, 2016. – 311 с. – Серия : Бакалавр. Академический курс. – 24,1/2,2 п.л. – С. 235-243, 250-260 (параграф 19.1 «Понятие, структура, состояние и динамика компьютерной преступности в Российской Федерации», параграф 19.3 «Особенности личности преступника, совершающего преступления в сфере компьютерной информации» главы 19 «Криминологическая характеристика компьютерной преступности»).

49. Евдокимов К. Н. Проблемы квалификации и предупреждения нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): монография / К. Н. Евдокимов. – Иркутск : Иркутский юридический институт (филиал) Акад. Ген. прокуратуры Рос. Федерации, 2018. – 223 с. – 13 п.л.

50. Комментарий к Уголовному Кодексу Российской Федерации / Под общей редакцией О. С. Капинус; науч. ред. В. В. Меркурьев. – Первое издание – Москва, Академия Генеральной прокуратуры Российской Федерации, 2018. – 1 376 с. – 86/0,3 п.л. – С. 674-677, 1299-1307 (комментарий к статье 159.6 и главе 28 Уголовного кодекса Российской Федерации в соавторстве с М. А. Ефремовой).

51. Криминология: учебник для бакалавриата, специалитета и магистратуры / под общ. ред. О. С. Капинус; под науч. ред. В. В. Меркурьева. – 2-е изд., пер. и доп. – Москва: Издательство Юрайт, 2019. – 1132 с. – (Серия: Бакалавр. Специалист. Магистр). – 87,83/3,7 п.л. – С. 986-997, 1009-1042 (параграф 19.1 «Понятие, структура, состояние и динамика компьютерной преступности в Российской Федерации», параграф 19.3 «Личность компьютерного преступника», параграф 19.4 «Предупреждение компьютерной преступности в Российской Федерации» главы 19 «Криминологическая характеристика компьютерной преступности»).

Статьи в иных изданиях:

52. Евдокимов, К. Н. К вопросу о конституционно-правовых гарантиях информационных прав и свобод человека и гражданина [Текст] / К. Н. Евдокимов // Конституции, уставы субъектов Российской Федерации: проблемы интеграции с Конституцией и федеральным законом : материалы Всероссийской научно-практической конференции. – Иркутск : Изд-во ИГУ, 2012. – С.46-51. – 0,4 п.л.

53. Евдокимов, К. Н. Информационные права и свободы человека и гражданина в Российской Федерации: проблемы теории и практики [Текст] / К. Н. Евдокимов // Правозащитная деятельность органов государственной власти: проблемы и перспективы. Материалы круглого стола с международным участием. – Иркутск: Изд-во БГУЭП, 2012. – С. 39-43. – 0,3 п.л.

54. Евдокимов, К. Н. К вопросу о совершенствовании уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) [Текст] / К. Н. Евдокимов // Деятельность правоохранительных органов в современных условиях: материалы Международ. науч.- практ. конф. – Иркутск: ФГКОУ ВПО ВСИ МВД России, 2012. – С.227-230. – 0,3 п.л.

55. Евдокимов, К. Н. К вопросу о совершенствовании юридической терминологии в российском уголовном законодательстве (на примере преступлений в сфере компьютерной информации) [Текст] / К. Н. Евдокимов // Правовая политика современной России: реалии и перспективы: материалы Международной науч.- практ. конф., посвященной 95-летию Иркутского гос. ун-та. – Иркутск: Изд-во ИГУ, 2013. – С.49-54. – 0,5 п.л.

56. Евдокимов, К. Н. Сравнительно-правовой анализ регламентации уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ в законодательстве России и зарубежных стран [Текст] / К. Н. Евдокимов // «Европа - Россия - Азия: диалог континентальных культур (история, право, гражданское общество, геополитика)»: сб. материалов 3-й всерос. науч.- практ. конф.; под ред. С. А. Рязанцева, М. А. Мушинского. – Иркутск: Иркутский государственный технический университет, 2013. – С.69-84. – 0,9 п.л.

57. Евдокимов, К. Н. Основные причины компьютерной преступности в современной России [Текст] / К. Н. Евдокимов // The Journal of Siberian and Far Eastern Studies. – Vol. X. – July 2014 (Institute of Russian Studies, Hallim University). – С.45-89. – 1,2 п.л.

58. Евдокимов, К. Н. Проблемные вопросы квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Информационные технологии в обществе и правовой сфере: Сб. науч. ст. – Вып. 2. – Калининград: Калининградский филиал СПбУ МВД России, 2014. – С.66-75. – 0,5 п.л.

59. Евдокимов, К. Н. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Правовая политика современной России: реалии и перспективы : материалы Междунар.науч.-практ. конф., посвящ. 150-летию земской и судебной реформ в России. – Иркутск : Изд-во ИГУ, 2014. – С.95-97. – 0,2 п.л.

60. Евдокимов, К. Н. Политические факторы компьютерной преступности в России [Текст] / К. Н. Евдокимов // Информационное право. – 2015. – № 1. – С. 41-47. – 0,5 п.л.

61. Евдокимов, К. Н. К вопросу о конституционно-правовых гарантиях информационных прав и свобод человека и гражданина [Текст] / К. Н. Евдокимов // ГлаголЪ правосудия. – 2015. – № 2 (10). – С.62-64. – 0,4 п.л.

62. Евдокимов, К. Н. Проблемные вопросы квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Прокуратура и судебная система России: история и современность. К 150-летию Судебной реформы 1864 года. Материалы научно-практической конференции / Под общ. ред. Г. В. Штадлера. – Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2015. – С.93-98. – 0,4 п.л.

63. Евдокимов, К. Н. Актуальные вопросы взаимодействия органов государственной власти, органов местного самоуправления и общественных объединений в обеспечении национальной безопасности России от современных киберугроз [Текст] / К. Н. Евдокимов, П. Н. Саганов // Проблемы организации органов государственной власти и местного самоуправления: история, теория, практика и перспективы: материалы Международной научно-

практической конференции. – Иркутск: Байкальский Государственный Университет Экономики и Права, 2015. – С.75-81. – 0,5 п.л.

64. Евдокимов, К. Н. Актуальные проблемы противодействия информационным правонарушениям в Российской Федерации: конституционно-правовой аспект [Текст] / К. Н. Евдокимов, А. Т. Нагуслаев // Проблемы организации органов государственной власти и местного самоуправления: история, теория, практика и перспективы: материалы Международной научно-практической конференции. – Иркутск: Байкальский Государственный Университет Экономики и Права, 2015. – С.69-75. – 0,5 п.л.

65. Евдокимов, К. Н. Актуальные вопросы совершенствования уголовной ответственности за совершение преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Проблемы современного российского законодательства: материалы III Всерос. науч.- практ. конф. – Иркутск; М.: РПА Минюста России, 2015. – С.255-257. – 0,21 п.л.

66. Евдокимов, К. Н. К вопросу об определении понятия «компьютерная преступность в Российской Федерации» [Текст] / К. Н. Евдокимов // Деятельность правоохранительных органов в современных условиях: сб. материалов 20-й международ. науч.- практ. конф. В 2 т. Т.1. – Иркутск: ФГКОУ ВПО ВСИ МВД России, 2015. – С. 36-39. – 0,21 п.л.

67. Евдокимов, К. Н. К вопросу о совершенствовании уголовно-правовой квалификации преступлений в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы Всероссийского круглого стола. – Иркутск: ФГКОУ ВПО ВСИ МВД России, 2015. – С.113-120. – 0,5 п.л.

68. Евдокимов, К. Н. К вопросу о совершенствовании уголовно-правового механизма противодействия преступлениям в сфере компьютерной информации [Текст] / К. Н. Евдокимов // Криминалистические чтения на Байкале – 2015: материалы Международ. науч.-практ. конф. ФГБОУВО

«Российский государственный университет правосудия» Восточно-Сибирский филиал; отв. ред. Д. А. Степаненко. – Иркутск, 2015. – С.158-163. – 0,5 п.л.

69. Evdokimov, K. N. On the issue of criminal responsibility for the creation, use and distribution of «botnets» [Text] / K. N. Evdokimov // European science review. – 2015. – № 11-12. – P.P. 229-230. – 0,2 п.л.

70. Evdokimov, K. N. Personality traits of computer criminals in modern Russia [Text] / K. N. Evdokimov // European Journal of Law and Political Sciences. – 2016. – № 2. – P.P. 42-45. – 0,25 п.л.

71. Evdokimov, K. N. Comparative legal analysis of the legislation of Russia and foreign countries, regulating the criminal liability for committing computer crimes [Text] / K. N. Evdokimov // The collection includes the 9th International Scientific Conference «Science and Society» (London, 24-29 November 2016). – 2016. – № 3-1. – P.P. 104-121. – 0,5 п.л.

72. Евдокимов, К. Н. Актуальные вопросы противодействия компьютерной преступности в Российской Федерации [Текст] / К. Н. Евдокимов // Деятельность правоохранительных органов в современных условиях: сборник материалов XXI международной научно-практической конференции. – Иркутск: ФГКОУ ВПО ВСИ МВД России, 2016. – С. 54-58. – 0,25 п.л.

73. Евдокимов, К. Н. Криминологические особенности личности компьютерного преступника в Российской Федерации [Текст] / К. Н. Евдокимов // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: Материалы всероссийской научно-практической конференции. – Иркутск: ФГКОУ ВПО ВСИ МВД России, 2016. – С. 116-121. – 0,3 п.л.

74. Евдокимов, К. Н. Особенности уголовно-правовой квалификации и ответственности за компьютерные преступления в законодательстве России и зарубежных стран [Текст] / К. Н. Евдокимов // Проблемы современного законодательства России и зарубежных стран материалы V Международной

научно-практической конференции; отв. ред. С. И. Суслова, А. П. Ушакова. – Иркутск; М.: РПА Минюста России, 2016. – С. 80-84. – 0,2 п.л.

75. Евдокимов, К. Н. Актуальные вопросы обеспечения информационной безопасности Российской Федерации: уголовно-правовые и криминологические аспекты [Текст] / К. Н. Евдокимов, Н. Н. Таскаев // Обеспечение национальной безопасности России в современном мире: материалы международной научно-практической конференции. Министерство образования и науки РФ; Байкальский государственный университет, 2016. – С. 66-74. – 0,5 п.л.

76. Евдокимов, К. Н. Сравнительно-правовой анализ законодательства России и зарубежных стран, регламентирующего уголовную ответственность за совершение компьютерных преступлений [Текст] / К. Н. Евдокимов // Юридический мир. – 2017. – № 3. – С. 45-49. – 0,5 п.л.

77. Евдокимов, К. Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о хищении чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации (ст. 159^6 УК РФ) [Текст] / С. В. Скляров, К. Н. Евдокимов // Российский судья. – 2017. – № 7. – С. 28-32. (авторство не разд.). – 0,5 п.л.

78. Евдокимов, К. Н. Актуальные вопросы международно-правового сотрудничества России в сфере противодействия компьютерной преступности [Текст] / К. Н. Евдокимов, Н. Н. Таскаев // Проблемы обеспечения национальной безопасности в контексте изменения геополитической ситуации: материалы международной научно-практической конференции, Иркутск: Байкальский государственный университет, 2017. – С. 41-49. – 0,5 п.л.

79. Evdokimov, K. Comparative legal analysis of responsibility for the commission of computer crimes in the criminal law systems of Russia and foreign countries [Text] / D. Lipinsky, K. Evdokimov // Kazan University Law Review. – 2017. – Т. 3. – № 3. – С. 83-98. – 0,5 п.л.

80. Евдокимов, К. Н. Анекселенктотичная технотронная преступность (частная теория) [Текст] / К. Н. Евдокимов // Российский судья. – 2018. – № 4. – С. 35-39. – 0,5 п.л.

81. Евдокимов, К. Н. Правовые меры предупреждения компьютерной преступности в Российской Федерации [Текст] / К. Н. Евдокимов // Инновационные внедрения в области юриспруденции : сб. науч. тр. Междунар. науч.-практ. конф. - Москва: Издательство: Федеральный центр науки и образования «Эвенсис», 2018. – С. 29-32. – 0,21 п.л.

82. Евдокимов, К. Н. Новые угрозы информационной безопасности России: от компьютерной преступности к анекселенктотичной технотронной преступности (частная научная теория) [Текст] / К. Н. Евдокимов // Основные направления государственной политики России в сфере обеспечения национальной безопасности: Материалы международной научно-практической конференции. Отв. ред. Е.М. Якимова. Иркутск, 2018. – С. 57-65. – 0,65 п.л.

83. Евдокимов, К. Н. К вопросу о совершенствовании объективной стороны состава преступления при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [Текст] / К. Н. Евдокимов // Российская юстиция. – 2019. – № 3. – С. 10-13. – 0,5 п.л.

84. Евдокимов, К. Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) [Текст] / К. Н. Евдокимов // Российский судья. – 2019. – № 2. – С. 12-16. – 0,5 п.л.

85. Евдокимов, К. Н. Особенности субъективной стороны состава преступления при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) [Текст] / К. Н. Евдокимов // Мировой судья. – 2019. – № 6. – С. 28-32. – 0,5 п.л.

86. Евдокимов, К. Н. К вопросу определения объективной стороны нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) [Текст] / К. Н. Евдокимов // Конституция Российской

Федерации и современный правопорядок: Материалы международной научно-практической конференции. В 5 ч. Ч. 5. – Москва, 2019. – С. 42-46. – 0,4 п.л.

87. Евдокимов, К. Н. Вредоносные компьютерные программы как орудие и средство совершения преступлений: онтологические и гносеологические аспекты [Текст] / К. Н. Евдокимов // Российская юстиция. – 2020. – № 3. – С. 56-58. – 0,5 п.л.

88. Евдокимов, К. Н. Самодетерминация технотронной преступности в Российской Федерации [Текст] / К. Н. Евдокимов // Российский судья. – 2020. – № 7. – С. 48-53. – 0,5 п.л.

89. Евдокимов, К. Н. Самодетерминация компьютерной преступности в условиях ее трансформации в технотронную преступность [Текст] / К. Н. Евдокимов // Правовые средства обеспечения национальной безопасности Российской Федерации: история и современность. Материалы международной научно-практической конференции. Отв. редактор Е.М. Якимова. – Иркутск: Байкальский государственный университет, 2020. – С. 26-33. – 0,5 п.л.

90. Евдокимов, К. Н. Противодействие компьютерной преступности в Российской Федерации (по результатам социологического исследования) [Текст] / К. Н. Евдокимов // Научный компонент. – 2020. – № 3 (7). – С. 192-200. – 0,5 п.л.

91. Евдокимов, К. Н. Проблемы квалификации киберпреступлений при расследовании и судебном рассмотрении уголовных дел в Российской Федерации [Текст] / К. Н. Евдокимов // Противодействие киберпреступности: современное состояние и пути повышения эффективности : сборник статей. – Минск : Следственный комитет Республики Беларусь, ЮрСпектр, 2020. – С.92-96. – 0,24 п.л.

Общий объем опубликованных работ составляет 120,0 п. л.