

Полицейская деятельность

Правильная ссылка на статью:

Комаров А.А. Историческая изменчивость компьютерной преступности: процесс расширения объекта и предмета преступных посягательств и её структура // Полицейская деятельность. 2025. № 2. DOI: 10.7256/2454-0692.2025.2.73704 EDN: GCXRGR URL: [https://nbpublish.com/library\\_read\\_article.php?id=73704](https://nbpublish.com/library_read_article.php?id=73704)

## Историческая изменчивость компьютерной преступности: процесс расширения объекта и предмета преступных посягательств и её структура

Комаров Антон Анатольевич

ORCID: 0000-0002-1330-4236

кандидат юридических наук

доцент, кафедра уголовного права и национальной безопасности; Новосибирский государственный университет экономики и управления

630099, Россия, Новосибирская область, г. Новосибирск, ул. Каменская, 52/1, оф. 503

✉ [reise83@mail.ru](mailto:reise83@mail.ru)



---

[Статья из рубрики "Профилактическая деятельность полиции"](#)

### DOI:

10.7256/2454-0692.2025.2.73704

### EDN:

GCXRGR

### Дата направления статьи в редакцию:

16-03-2025

**Аннотация:** Объектом исследования в данной статье является компьютерная преступность, а предметом — её историческая изменчивость, проявляющаяся в расширении объектов и предметов преступных посягательств, а также в изменении структуры и мотивации преступников. В работе подробно рассмотрены ключевые аспекты темы, такие как влияние экономических и технологических факторов на эволюцию компьютерной преступности, её территориальное распределение и связь с современными вызовами, включая цифровизацию и переход на безналичные расчёты. Особое внимание уделено анализу виктимологических особенностей компьютерных преступлений, а также проблемам правоприменительной практики и недостаткам в расследовании сложных киберпреступлений. В отличие от многих работ, в данной статье акцент сделан на историко-материалистическом подходе, что позволяет глубже понять взаимосвязь между экономическими изменениями и трансформацией преступности. Для

анализа использовались частные методы исследования, включая структурный анализ, метод трендов, расчёт дисперсии и коэффициента вариации, а также сопоставительный анализ данных уголовной статистики и материалов выборочных исследований (на примере 759 уголовных дел за 2022–2023 гг.). В работе систематизированы и ранжированы факторы, влияющие на развитие компьютерной преступности, такие как изменения в экономике, трансформация коммуникативных технологий и сдвиги в массовом сознании. Это позволяет лучше понять механизмы адаптации преступности к новым условиям. Автор подробно исследует, как за последние 30–40 лет объекты преступлений сместились от данных и информационных систем к безналичным средствам, криптовалютам и критической информационной инфраструктуре. Это подчёркивает связь преступности с цифровизацией экономики. В работе выявлены различия между профессиональными киберпреступлениями (ориентированными на крупные суммы и юридических лиц) и общеуголовными мошенничествами (нацеленными на случайных жертв). Это позволяет разработать более адресные меры профилактики. В работе показано, что уровень компьютерной преступности коррелирует с уровнем цифровизации регионов, что позволяет выделить наиболее уязвимые территории и сосредоточить на них усилия по профилактике. Подчёркнута важность открытости данных и взаимодействия между научным сообществом и правоохранительными органами для повышения эффективности борьбы с преступностью.

**Ключевые слова:**

криминология, компьютерная преступность, динамика, уровень преступности, уголовная статистика, интернет-мошенничество, Интернет, исторический материализм, тенденции преступности, методология

**Введение.**

Для начала хотелось бы обратить внимание на то, что компьютерная преступность является наиболее наглядным примером исторической изменчивости преступности. Особенно часто в этом контексте она возникает на страницах учебной литературы. Однако и научные источники зачастую представляют это явление как новое и малоизученное. Мы хотим не просто подчеркнуть наличие такого свойства у преступности, но и углубиться в проблему, указав на то, что компьютерная преступность в её современном состоянии далеко не тождественна тому явлению, которое существовало ещё относительно недавно – те же 30–40 лет назад.

За указанный промежуток времени компьютерная преступность в своём развитии прошла несколько самостоятельных этапов. Изучение свойства исторической изменчивости может углубить наши представления о ней. Изменчивость сводится к описанию состояния преступности и объяснению причин таких изменений по отношению к прошлому периоду её исторического развития. В этой части всё обстоит достаточно благополучно. В последние десять лет написано немало работ, раскрывающих тенденции современной компьютерной преступности: Простосердов (канд. дис., 2016); Мандрыко (канд. дис., 2016); Кузнецова (канд. дис., 2019); Камко (канд. дис., 2020); Родивилин (канд. дис., 2021); Евдокимов (докт. дис., 2021); Пучков (докт. дис., 2022); Конев (канд. дис., 2022); Ильницкий (канд. дис., 2022); Джафарли (докт. дис., 2022); Родина (канд. дис., 2022); Турунова (канд. дис., 2022); Туркулец (канд. дис., 2023); Старостенко (канд. дис., 2023); Шипулин (канд. дис., 2024). Более ранние работы мы решили не приводить в пример, что не умаляет значимости исследований прежних лет. При этом очевидна дальнейшая

дифференциация научных исследований по вопросам компьютерной преступности. Предметная область научных исследований расширяется не случайно. Этот научный процесс соответствует объективным закономерностям развития компьютерной преступности. Однако в этом кроется и серьёзный недостаток: отдельные направления криминологических изысканий остаются самостоятельным почином, интересующихся данной темой. В России отсутствует целенаправленный заказ на криминологические исследования, как и координирующая сила, способная правильно расставлять приоритеты.

Основной акцент работ сделан на том, что развитие компьютерной преступности напрямую связано с технологическими трендами, такими как искусственный интеллект, блокчейн, интернет вещей (IoT) и квантовые вычисления. При этом исследователи всё чаще склоняются к анализу проблем борьбы с современными технологическими вызовами в рамках информационной или кибербезопасности. Мы же видим ситуацию несколько иначе. Полагаем, что рассматривать её следует через призму исторического материализма. Компьютерная преступность – это не только результат технологического прогресса, но и отражение социально-экономических процессов. Экономические кризисы, социальное неравенство и цифровой разрыв между странами создают благоприятную почву для её развития. Это делает её не просто технической проблемой, но и вызовом базисным экономическим отношениям. Задача нашего исследования состоит в том, чтобы показать совокупный объём изменений, произошедших с компьютерной преступностью за последнюю четверть века, на основе статистического материала, определив действительные причины существующих тенденций в материалистическом ключе.

### **Материалы и методы.**

Для начала коснёмся общих вопросов методологии. В изучении проблемы мы стоим на позициях исторического материализма, полагая, что это наиболее продуктивный способ познания окружающей действительности [\[1\]](#). В основе гипотезы лежит предположение о ведущем влиянии базисных экономических отношений на состояние компьютерной преступности. Эта зависимость прослеживается тем полнее, чем глубже мы погружаемся в структурный анализ мотивации современных преступников. Она же возникает не на пустом месте, а является результатом рефлексии на окружающую человека действительность. Но сказанное не следует воспринимать вульгарно-материалистически. Мы, как и ряд наших коллег, склонны диалектически рассматривать процессы, происходящие в историческом контексте [\[2\]](#).

Движение вперёд стоит начинать с малого. К познанию причинно-следственных связей надлежит подходить в последнюю очередь, лишь после обнаружения устойчивой связи состояний, корреляционный анализ которой обеспечит необходимый эмпирический базис для дальнейших утверждений [\[3, с.350\]\[1\]](#). Поэтому необходимо обсудить специально-научный метод нашей статьи. Очевидно, потребуется дать количественную оценку состояния преступности, для чего пригодятся методы расчёта средних значений, темпов роста, структурного анализа отношения части к целому. Достаточная достоверность суждений невозможна без понимания однородности исследуемого статистического массива. Для этого необходимо вычислить значения дисперсии, стандартного отклонения и коэффициента вариации. Наконец, для проверки гипотезы требуется провести сопоставительный анализ результатов, полученных на основе данных уголовной статистики и собственных выборочных исследований.

Особое внимание, а также ряд критических замечаний, следует уделить фактологической базе, формируемой официальной уголовной статистикой. Основой служат извлечения из формы №4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений». Её существование обусловлено Приказом Генеральной прокуратуры РФ от 17 января 2020 г. №30 «Об утверждении формы федерального статистического наблюдения», где наибольший исследовательский интерес представляет раздел 9: «Сведения о преступлениях, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации». Однако, несмотря на интерес научного сообщества к этим данным, с 2023 года их публикация органами прокуратуры прекращена. Управление правовой статистики Главного управления правовой статистики и информационных технологий Генеральной прокуратуры РФ также отказывает в предоставлении запрашиваемой информации. Это напоминает ситуацию пятнадцатилетней давности, описанную В. В. Лунеевым, когда сектор уголовного права ИГП РАН столкнулся с аналогичными отказами [\[4, с.29\]](#). Таким образом, взаимодействие научного сообщества и ведущего ведомства, ответственного за уголовную статистику в России, остаётся неудовлетворительным, что ограничивает привлечение исследователей-волонтеров для решения стоящих перед государством задач по борьбе преступностью.

Имеющиеся в нашем распоряжении данные о состоянии компьютерной преступности охватывают период 2018–2023 гг., поскольку получить полные сведения за 2024 год не представляется возможным. Часть исследовательских задач решена с использованием сводных отчетов о состоянии преступности, публикуемых МВД РФ. Там, где это допустимо, мы дополняли анализ комментариями по итогам прошедшего года.

Недостатки официальной статистики компенсированы результатами выборочного исследования материалов уголовных дел. Нами проанализировано 759 случаев, предусмотренных ст. 159, п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ.

### **Результаты исследования, обнаруженные зависимости.**

В конце XX века в понимании компьютерной преступности было ровно два прочтения – в узком и широком смыслах. В первом случае компьютерная преступность охватывала преступления, предусмотренные гл. 28 УК РФ. В широком смысле – все новые способы совершения преступлений с использованием компьютерной техники. Понятие в узком смысле отличалось от общеуголовной преступности прежде всего объектом преступного посягательства. В тот период нарождающаяся отрасль информационного права, определяя виды охраняемой законом информации (в том числе компьютерной), только создавала основу для разграничения этих категорий. Общеуголовные преступления, напротив, характеризовались более широким спектром объектов и способов совершения [\[5, с. 422\]](#).

В современной действительности количество правоохраняемых объектов и предметов преступных посягательств в сфере компьютерной преступности значительно расширилось. Поскольку мы опираемся на диалектический метод познания, следует признать, что базисные отношения, то есть экономические, предопределяют содержание преступной деятельности. Это позволяет ответить на вопрос, иногда возникающий в криминологии: почему снижается объём регистрируемой уличной преступности? Ведь, в этом отношении, может оказаться прав Я. И. Гилинский, утверждающий, что преступники постепенно уходят в Интернет [\[6, с. 12\]](#). Можно ли это утверждение проверить

статистически? На наш взгляд, ответ должен быть положительным. Для проверки данной гипотезы необходимо исходить из базового тезиса: мотивация компьютерных преступников смещается в сторону корыстных побуждений. В рамках исследования нами обобщены сводные статистические данные о преступлениях, совершённых с применением информационно-коммуникационных технологий, в соответствии с Перечнем №25 Указаний Генеральной прокуратуры России от 25.06.2024 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчётности». Сопоставительный анализ демонстрирует, что ряд деяний, квалифицируемых как компьютерные, либо связан с эффектом расширенного воспроизводства преступности, либо непосредственно сопряжён с иными её видами. Таким образом, структура компьютерной преступности может быть представлена следующим образом:

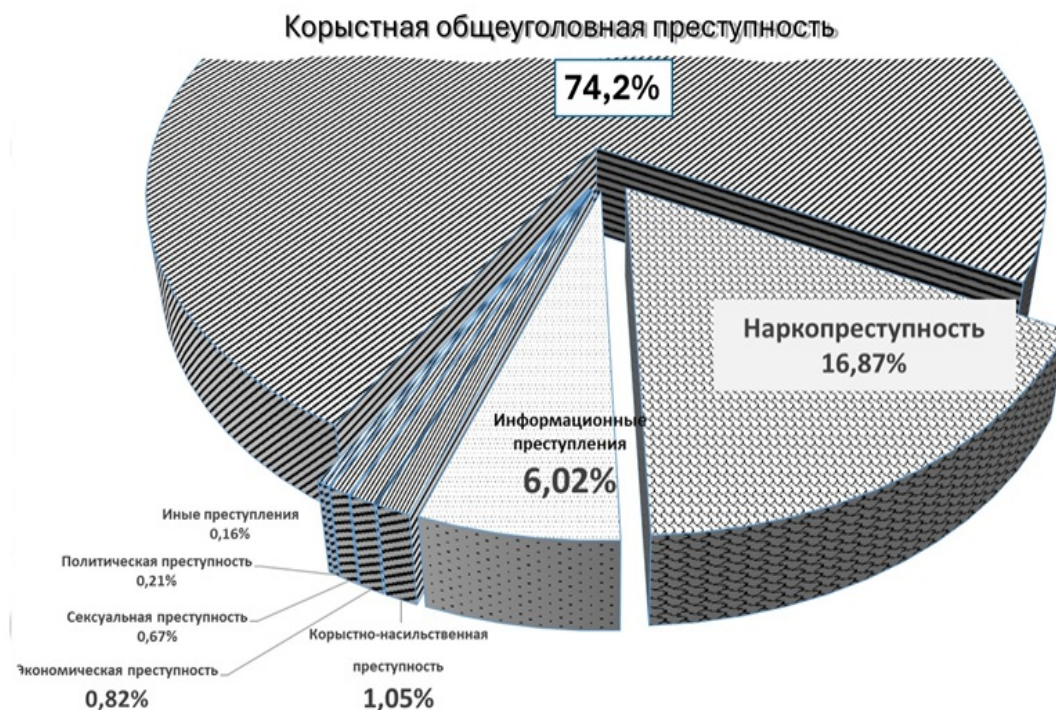


Рис 1. Структура компьютерной преступности.

Основной массив («ядро компьютерной преступности») составляют корыстные имущественные преступления. Наибольшее распространение получили: основная норма об уголовной ответственности за мошенничество – ст. 159 УК РФ (2024 г. – 379,7 тыс.; 2023 г. – 353,2 тыс.; 2022 г. – 249,9 тыс.; 2021 г. – 238,6 тыс.); и кража электронных денежных средств – п. «г» ч. 3 ст. 158 УК РФ (2024 г. – 105,9 тыс.; 2023 г. – 119,2 тыс.; 2022 г. – 113,6 тыс.; 2021 г. – 156,8 тыс.). Близки по объёму к регистрации краж наркопреступления (2024 г. – 118,9 тыс.; 2023 г. – 103,9 тыс.; 2022 г. – 82,6 тыс.; 2021 г. – 52 тыс.). Однако прирост здесь обусловлен изменением дополнительных критериев отнесения к числу компьютерных отдельных видов преступлений. «Ядерным составом» для компьютерных наркопреступлений является ст. 228.1 УК РФ, а именно — сбыт наркотических средств с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), удельный вес которой достигает 78,5 % от всех регистрируемых деяний такого рода.

Иные преступления занимают менее значительный удельный вес. Однако здесь необходимо сделать оговорку. Указанная структура компьютерной преступности была рассчитана на основе совокупности данных о совершённых преступлениях за 2020–2023

гг. Но в 2024 году было зарегистрировано 105 773 преступления в сфере компьютерной информации. Для сравнения: в 2023 году таких преступлений было зарегистрировано порядка 37 101; в 2021 году – 10 027; в 2020 году – 6 869. За последние годы мы наблюдаем кратные темпы прироста данной статистической категории, что равняется максимальным значениям объёма за всю историю наблюдений с момента введения в действие Уголовного кодекса РФ. Необходимо уточнить и структуру данной совокупности, поскольку основной массив приходится исключительно на 272 статью УК РФ. В прошлом году её удельный вес составил 99,6 %. Аналогичная ситуация наблюдалась и в предыдущие годы.

Подобное положение дел в уголовной статистике могло бы проиллюстрировать тезис о детерминации компьютерной преступности внешнеполитическими причинами на фоне специальной военной операции (СВО). Однако здесь существует два возражения.

*Первое из них* связано с тем, что защите критически важной информационной инфраструктуры Российской Федерации посвящена отдельная статья Уголовного кодекса – ст. 274.1 УК РФ. По каковой регистрируется мало преступлений. Пик преступной активности «иностранных агентов» пришёлся именно на 2022 год. Так, в 2023 г. было зарегистрировано 114 преступлений; в 2022 г. – 519; в 2021 г. – 159; в 2020 г. – 22. Сходная ситуация наблюдается и в отношении нормы, предусмотренной ст. 274.2 УК РФ. Существенное влияние на регистрируемость этого деяния оказывает административная преюдиция (ст. 13.42 и 13.42.1 КоАП РФ). Для большей сопоставимости данных обратимся к судебной статистике и форме № 1-АП «Отчёт о работе судов общей юрисдикции по рассмотрению дел об административных правонарушениях». В 2023 году было рассмотрено 34 административных дела, в которых фигурировали 32 правонарушителя. В первой половине 2024 года было рассмотрено 22 дела, и к ответственности привлечено 18 лиц. Очевидно, что динамика правонарушаемости положительная. В истекшем году логично ожидать увеличение числа дел и лиц, выявленных за совершение административных правонарушений. К сожалению, на момент написания работы Судебным департаментом ещё не сведена статистика за полный отчётный период. За тот же отрезок времени (1,5 года) данные о судимости отсутствуют, поскольку никто не был привлечён к уголовной ответственности. Сопоставление данных позволяет предположить, что преюдиция может оказаться относительно эффективной профилактической мерой. Принятию решения о привлечении к административной ответственности, как правило, предшествует вынесение предостережения о недопустимости нарушений закона индивидуальным предпринимателем или представителем юридического лица из числа операторов связи. Косвенно это подтверждается результатами прокурорских проверок. Начальник отдела по надзору за исполнением законов в сфере информационных технологий и защиты информации Генеральной прокуратуры О. В. Кипкаев в публичном выступлении указал, что за последние 2,5 года только на объектах критической информационной инфраструктуры выявлено более 155 тыс. нарушений. Однако для более обстоятельной проверки необходимы статистические данные за ряд будущих лет. В ретроспективе интересующие нас данные о судимости и административной правонарушаемости несопоставимы или вовсе отсутствуют, поскольку нормы об уголовной и административной ответственности были приняты относительно недавно.

Тем не менее, данная совокупность охранительных норм, как показала практика, способна обеспечить эффективный контроль за трафиком информации, распространяемой в Интернете. При отсутствии таких норм крупные инфраструктурные проекты по ограничению доступа к информации (например, блокировка YouTube) были



бы невозможны. Не опасаясь уголовно-правовых санкций, индивидуальные предприниматели и юридические лица в погоне за прибылью не стали бы соблюдать запреты информационного права и распоряжения Роскомнадзора.

*Второе возражение* связано с изучением материалов конкретных уголовных дел. Создаётся впечатление, что за 2024 год никаких изменений в преступном поведении и правилах квалификации по сравнению с прошлыми годами не произошло. Если рассматривать практику применения ст. 272 УК РФ, то в основном это посягательства на персональные данные лицами, уполномоченными работодателем на их обработку. Трудно предположить, что за год объём подобных преступлений увеличился в 3,5 раза. Скорее, уменьшается их латентная часть. Но об этом мы писали в предыдущей нашей работе [\[7\]](#). Чего действительно можно ожидать в области уголовной статистики, так это перераспределения статистической совокупности в силу изменения правил квалификации компьютерных преступлений, связанных с оборотом персональных данных россиян, в связи с введением в действие ст. 272.1 УК РФ Федеральным законом № 421 от 30.11.2024.

С учётом корыстной направленности большинства таких преступных посягательств мы можем констатировать, что персональные данные россиян мало полезны для иностранных преступников. Информацию на русском языке ещё нужно суметь использовать для совершения хищения. После начала специальной военной операции Россия была отключена от системы международных платежей SWIFT. Поэтому вывести похищенное за пределы Российской Федерации становится затруднительно.

Завершив нашу оговорку, вернёмся к основной идее статьи. Казалось бы, из представленного структурного анализа неизбежно следует вывод о том, что компьютерные технологии влияют на содержание общественных отношений. Однако приведённые данные можно интерпретировать и с точностью до наоборот. Современная компьютерная преступность всё более напоминает общеуголовную, замещая, где это возможно, традиционные способы совершения корыстных, корыстно-насильственных, сексуальных и наркопреступлений. Информатизация выступает в качестве производной детерминанты, поскольку её интенсивность и сама возможность реализации определяются состоянием экономики.

Таким образом, в соответствии с тенденциями развития экономических отношений меняются и сами предметы преступных посягательств, особенно если уточнить их содержание в рамках объектов гражданских прав. Всё чаще предметом компьютерного хищения становятся безналичные денежные средства, что отражается на содержании действующего уголовного законодательства [\[8\]](#). На рисунке №2 представлена гистограмма, иллюстрирующая динамику удельного веса безналичных расчётов физических лиц за оказанные услуги и приобретённые товары.



Рис.2. Безналичные расчёты в России.

В случае совершения уличного мошенничества или карманной кражи у современной жертвы практически нечего изъять и обратить в свою пользу, кроме банковских карт. А поскольку желаемым результатом является завладение денежными средствами, то цель преступления отдалается, как и момент его окончания. Снижается эффективность преступной деятельности. Увеличивается вероятность разоблачения и взятия с поличным при попытке «обналичивания», и дело доходит до того, что Г. Э. Бицадзе такие преступления перестал относить к категории «уличных».

Иными словами, всё чаще вместо вещных прав (денег) предметом преступления «вынужденно» выступают иные имущественные права обязательственного характера (криптовалюта, безналичные денежные средства). Такие тенденции развития финансовой системы имеют предпосылки антикриминогенного свойства, коль скоро мы говорим о корыстной общеуголовной преступности.

Но в то же время наличие у преступности свойства исторической изменчивости позволяет ей подстроиться и под эту систему социального контроля с большей или меньшей эффективностью. Это приводит к тому, что статистическая совокупность имущественных преступлений уже долгие годы перераспределяется от краж в пользу мошенничеств. Подтверждение чему находится в таблице №1.

Таблица 1. Перераспределение в пользу мошенничеств.

	2003 год	2013 год	2023 год
Объём зарегистрированных преступлений в отчётный период:	2 756 398	2 206 249	1 947 161
Объём мошенничеств;	87 471	164 629	433 708
(их удельный вес):	(3,2%)	(7,5%)	(22,3%)
Объём краж;	1 150 772	922 562	583 343
(их удельный вес):	(41,7%)	(41,8%)	(30%)

Несомненно, это утверждение может быть подвергнуто критике с той точки зрения, что



изменения уголовного законодательства поспособствовали перераспределению статистической совокупности. Мы, конечно же, не отрицаем такой вариант. Это оказывает прямое влияние на состояние уголовной статистики в части формирования перечней составов преступлений, учитываемых в качестве совершённых с использованием информационно-коммуникативных технологий. Но получаемые на протяжении четверти века данные могут указывать и на то, что это не следствие неких внутренних закономерностей учётно-регистрационной дисциплины, а действительное изменение качественных показателей преступности. Невозможно объяснить такое перераспределение простым изменением правил квалификации, поскольку объём регистрируемых деяний тогда бы оставался неизменным. Он же прирастает за счёт мошенничеств, а не краж, при снижающемся уровне преступности. Получается, прав был И. Я. Фойницкий, утверждая, что с развитием и усложнением экономических отношений увеличивается распространённость мошенничеств [\[9, с.22\]](#).

Несколько противоречиво при всём этом выглядит ситуация с регистрацией компьютерных мошенничеств и преступных схем, связанных с использованием электронных средств платежа. Их объёмы выказывают отрицательные темпы прироста. В 2024 году по ст. 159.3 УК РФ было зарегистрировано 273 преступления; в 2023 – 2 461; в 2022 – 7 288; в 2021 – 10 258. По ст. 159.6 УК РФ за тот же промежуток времени наблюдалась следующая динамика: в прошлом году – 309 преступлений; в 2023 – 417; в 2022 – 334; в 2021 – 431. Казалось бы, в текущей экономической ситуации количество подобных деяний обязано неуклонно возрастать. Здесь нужно рассмотреть два контраргумента.

*Первый* состоит в том, что данные преступления относятся к категории высокопрофессиональных, совершаемых только в случае, если преступник обладает достаточными познаниями в области информатики. В результате таких преступлений остаётся довольно много «цифровых» следов. Нахождение и фиксация которых в современной криминалистической науке хоть и вызывают некоторые затруднения, но всё-таки совершенствуются довольно быстрыми темпами. Отчего преступники, совершающие исключительно вышеописанные преступления, просто вынуждены уметь скрывать следы совершённых ими преступлений. Уголовные дела, конечно же, возбуждаются, особенно по статье 159.3 УК РФ. Внимательное прочтение уголовной статистики наводит на мысль, что все они приостанавливаются в силу невозможности установления лица, совершившего преступление, либо ограниченности юрисдикции Российской Федерации в отношении скрывшихся от следствия и суда. Так, в 2023 году по ч. 1 ст. 208 УПК РФ было приостановлено 2 890 уголовных дел, ещё 5 уголовных дел было приостановлено по части 2 вышеуказанной статьи и одно уголовное дело по части 3. Математически получается, что ежегодно по статье 159.3 УК РФ уголовных дел приостанавливается даже больше, чем регистрируется фактов преступлений.

Что же касается применения ст. 159.6 УК РФ, то здесь ситуация складывается ещё более причудливым образом. До принятия Постановления Пленума Верховного Суда РФ №48 от 30.11.2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» часто встречалась неправильная квалификация общеуголовных мошенничеств (ст. 159 УК) в качестве компьютерных [\[10, с.34\]](#). После, в 2018 году, уровень регистрации таковых снизился до современных нам значений. Наиболее логичной гипотезой, объясняющей происходящее, является предположение о том, что он всегда был таковым, начиная с 2012 года. А в деле выявления и расследования мошенничеств с использованием электронных средств платежа и компьютерного мошенничества наблюдаются большие сложности. Причём проблема заключается не просто в недостатке криминалистических

методик, а в разрыве между практикой и теорией.

*Второй момент* состоит в размере причиняемого такими преступлениями ущерба в соотношении со способом завладения имуществом или правами на него. Подобный эффект мы уже наблюдали в случае перераспределения статистической совокупности от уличной преступности к компьютерной и от краж к мошенничествам. Проиллюстрируем это данными (см. рис. 3) о распределении имущественного ущерба, причинённого преступлениями, предусмотренными ст. 159, п. «г» ч. 3 ст. 158, ст. 159.6, ст. 159.3 УК РФ. Всего в случайной выборке оказалось 759 уголовных дел за 2022–2023 гг. Значения дисперсии, стандартного отклонения и коэффициента вариации дают нам основание утверждать, что в данной статистической совокупности наблюдается не одно явление, а несколько разных. Ущерб, причиняемый сложными мошенническими схемами с использованием специальных познаний в области информатики для совершения хищения, и банальный общеуголовный обман существенно отличаются по размеру. Более того, в первом случае деятельность преступников хорошо организована и целенаправлена. Размер похищенного, как правило, известен им заранее и является их преступной целью. А вот для мошенников, особенно телефонных, сумма причиняемого материального ущерба будет зависеть от платёжеспособности конкретной жертвы и зачастую определяется случайным образом. Подобная особенность уже отмечалась ранее другими исследователями [\[11\]](#).

В силу этих обстоятельств уместно будет говорить о возможности статистического анализа только в разрезе средних значений причиняемого ущерба (моды и медианы). Так, анализ данных уголовных дел показал, что средний размер ущерба составляет 574 тыс. рублей. При этом модой (наиболее часто встречаемым ущербом в материалах дела) является относительно небольшая сумма – 15 тыс. Стоит также заметить, что половина причиняемого ущерба лежит ниже медианы в 25 тыс. рублей.



Рис. 3. Суммы материального ущерба.

Поэтому совершение общеуголовного корыстного преступления – это более простая и рациональная практика реализации корыстных мотивов. А в случае с профессиональными компьютерными преступниками речь может идти о конкуренции (борьбе) корыстных мотивов с иными. На этот счёт также существуют специальные

исследования [\[12, с. 67\]](#).

Гипотезу о тесной связи базисных экономических отношений и состояния современной компьютерной преступности подтверждает и анализ её территориального распределения. Расчёты коэффициента преступности по отдельно взятым регионам за последние 3 года свидетельствуют о том, что преступления, связанные с дистанционной торговлей, мошенническими схемами, недоставкой товаров и обманом потребителей, довольно распространены в тех регионах нашей страны, что достаточно удалены в географическом отношении. На рисунке №3 мы видим 10 регионов-лидеров по распространённости интернет-мошенничества в нашей стране. Все они находятся на севере и северо-востоке России, куда товары доставляются почтой и курьерскими службами, потому что купить их дистанционно удобнее.

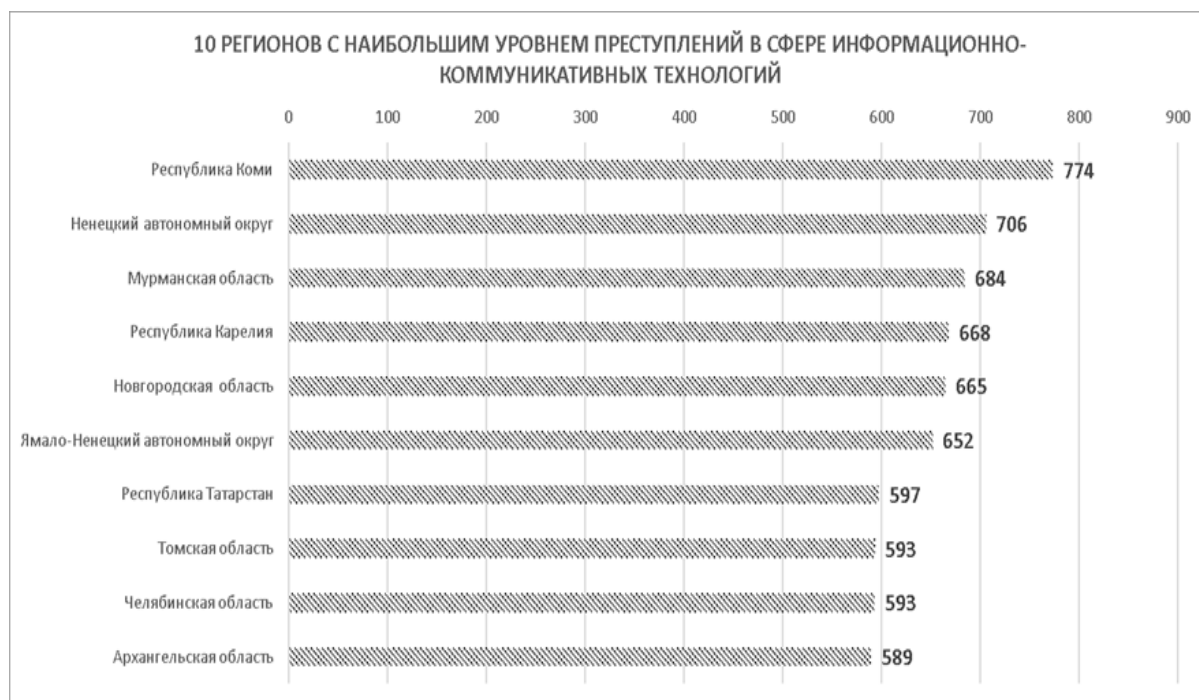


Рис. 4. Ранжир регионов по уровню интернет-мошенничества.

По большей части данное обстоятельство совпадает с ранжированием регионов по распространённости и применимости живущими там людьми безналичных расчётов. Данные Сберегательного банка России на сайте [сбериндекс.ru](http://сбериндекс.ru) говорят, что самыми «безналичными» регионами страны в 2023 г. остались Ненецкий АО (76,5 %), Республика Саха (73,8 %) и Чукотский АО (73,4 %). При этом рост к прошлому году наблюдался во всех регионах. Наиболее активно безналичный торговый оборот развивался в Чукотском АО (+5,9 п.п.), Карачаево-Черкесской Республике (+5,6 п.п.) и Ямало-Ненецком АО (+5 п.п.).

Таким образом, становится очевидным, что вектор мотивационной направленности компьютерных преступников меняется в зависимости от объективной экономической действительности, а не идеалистических представлений о массовой цифровизации сознания россиян. Общественное бытие, определившее общественное сознание на конкретном периоде времени, вступает в новую фазу исторического развития. Когда уже само общественное сознание в некоторой степени детерминирует развитие иных общественных отношений, в том числе и экономических. В данный момент времени именно такое положение дел мы наблюдаем. Но значение этого обстоятельства не стоит абсолютизировать и переставлять местами причину и следствие.

### **Выводы.**

Проделанная нами работа позволяет сформулировать ряд ключевых выводов:

#### *1. Историческая изменчивость как ключевая характеристика компьютерной преступности.*

Компьютерная преступность демонстрирует яркий пример исторической изменчивости, эволюционируя вместе с развитием технологий и социально-экономических условий. За последние 30–40 лет объекты и предметы преступных посягательств значительно расширились. Однако ранжир факторов, обуславливающих её состояние, следует изложить в следующем порядке:

а) изменения в экономике, создающие конкурентные преимущества для субъектов предпринимательской деятельности при использовании компьютерных технологий и побуждающие их к развитию цифровых платформ (цифровой экономики);

б) трансформация коммуникативных технологий, спонсированных бизнес-структурами;

в) корреспондирующие изменения в общественных отношениях и массовом сознании.

Если в конце XX века объектом компьютерной преступности были преимущественно данные и информационные системы, то сегодня туда вошли безналичные денежные средства, криптовалюты, электронные платёжные системы, персональные данные и даже критическая информационная инфраструктура. Это свидетельствует о том, что преступность адаптируется к новым реалиям цифровой экономики.

#### *2. Изучение свойства исторической изменчивости.*

Изучение свойства исторической изменчивости по отношению к преступлениям, связанным с посягательствами на охраняемую законом компьютерную информацию, показывает, что и в данном случае экономические причины являются более значимыми. Иные факторы, такие как политические, не соответствуют данным о территориальном распределении этого вида преступлений и преимущественной мотивации компьютерных преступников, изученной по материалам уголовных дел. При этом специфическая часть профессиональных компьютерных преступлений (в том числе корыстной направленности – ст. 159.3 и 159.6 УК РФ) в последние годы регистрируется хуже. Данное обстоятельство стоит увязать с переориентацией деятельности правоохранительных органов на выявление и расследование общеуголовных преступлений. Даже создание специализированных управлений по организации борьбы с противоправным использованием информационно-коммуникативных технологий в структуре Министерства внутренних дел в 2023 году существенным образом ситуацию не изменило. Конечно, увеличивается выявляемость и раскрываемость. Однако эти показатели улучшаются за счёт наиболее простых мошеннических схем. Опыт правоохранительной деятельности у переаттестованных на службу в эти подразделения, позволяет им эффективно реализовывать правоохранительную функцию только таким способом. Очевидно, что экстенсивная регистрация компьютерных преступлений дальше невозможна, поскольку экспоненциальный рост числа регистрируемых преступлений приведёт к непропорциональному росту загруженности. Сейчас как никогда важно установить целевые показатели, а также их индикаторы. Это послужит цели объективизации и большей открытости сводных данных о результатах деятельности соответствующих подразделений. А научное сообщество сможет проанализировать эти результаты и предложить практике верные решения по основным направлениям противодействия компьютерной преступности с учётом закономерностей её исторического развития. Пока

же между общественностью и правоохранительными органами наблюдается обратная ситуация, когда имеющиеся сводные данные не публикуются и не представляются для независимого анализа. Тем самым они фактически не используются для принятия каких-либо управленческих решений по организации борьбы с преступностью, или же эффективность последних малообоснованна. Ведь на изучение материала зачастую не хватает штатных ресурсов аналитических подразделений. В связи с этим управления правовой статистики прокуратуры перестали выкладывать в свободный доступ какую-либо аналитическую информацию, а в сводных отчётах Министерства внутренних дел содержатся лишь выборочные сведения при наличии всей полноты исходных первичных данных.

### *3. Влияние экономических и технологических факторов.*

Влияние экономических и технологических факторов проявляется в расширении объектов и предметов преступных посягательств, что напрямую связано с развитием экономических отношений и технологий. Переход на безналичные расчёты, распространение электронной торговли и цифровых активов создали новые возможности для преступников, что привело к смещению акцентов в структуре преступности. Историческая изменчивость компьютерной преступности проявляется в её постепенном замещении традиционных форм преступности, таких как уличные кражи и мошенничества. Преступники всё чаще используют цифровые технологии, что делает их действия более скрытыми и сложными для расследования. В силу недостатков, связанных с невозможностью фактического расследования сложных высокопрофессиональных компьютерных преступлений, видится сомнительным участие в Конвенции ООН «Против киберпреступности» 2024 года. Если мы унифицируем законодательство в соответствии с этой ней, то вряд ли мы сможем её исполнять в должном объёме. Понятно, что изменение структуры компьютерной преступности требует постоянного обновления уголовного законодательства и методов правоприменения. Введение в действие новых статей, таких как ст. 272.1 УК РФ, отражает попытки законодателя адаптироваться к новым вызовам, однако эффективность этих мер остаётся ограниченной. При этом стоит учитывать, что отдельные нормы уголовного закона имеют важный антикриминогенный потенциал. Статью 228.1 УК РФ даже можно назвать нормой двойной превенции, поскольку практика её применения свидетельствует о том, что сотрудники, выявляя сайты и каналы в мессенджерах или группы в социальных сетях, прекращают их деятельность, тем самым сокращая возможность потребления наркотиков конечными потребителями. И при успешном её применении сам феномен наркомании можно даже несколько сократить.

### *4. Анализ дисперсии причиняемого материального ущерба.*

Такой анализ помог установить некоторые виктимологические особенности совершаемых преступлений. Деятельность профессиональных преступников ориентирована на крупные суммы и юридических лиц в качестве потерпевших, а общеуголовное мошенничество ориентировано больше на случайную жертву, характеристики платёжеспособности которой преступнику заранее неизвестны.

Анализ территориального распределения компьютерной преступности показывает, что её структура и объекты преступных посягательств зависят от уровня цифровизации и экономического развития регионов. В удалённых регионах, где активно используются дистанционные услуги и электронные платежи, преступность чаще связана с мошенничеством и недоставкой товаров.

## Библиография

1. Бабаев М. М., Пудовочкин Ю. Е. Криминология и история: на пути междисциплинарного сближения // Всероссийский криминологический журнал. 2023. Т. 17, № 4. С. 312-322.
2. Лепс А., Спиридонов Л. И. Диалектическая криминология. Москва: Юрлитинформ, 2016. 232 с.
3. Ленин В. И. Статистика и социология / Полное собрание сочинений. 55 томов. 5-е изд. Москва: Гос. изд-во полит. лит., 1969. Т. 30. 562 с.
4. Исследования латентной преступности: материалы круглого стола / отв. ред. С. М. Иншаков; Акад. Ген. Прокуратуры РФ. М., 2010. 141 с.
5. Анисимов С. Л., Ситников К. А. К вопросу о понятии "преступления в сфере высоких технологий" // Евразийский юридический журнал. 2024. № 2(189). С. 421-424.
6. Гилинский Я. И. Девиантология постмодерна // Российский девиантологический журнал. 2022. № 1. С. 10-16.
7. Комаров А.А. Измерение латентности преступлений, совершённых при помощи информационно-коммуникативных технологий, по матрице индексов наказуемости А.А. Конева // Вопросы безопасности. 2024. № 4. С. 31-48. DOI: 10.25136/2409-7543.2024.4.72451 EDN: DNARAJ URL: [https://nbpublish.com/library\\_read\\_article.php?id=72451](https://nbpublish.com/library_read_article.php?id=72451)
8. Мира К. А., Першин А. Н. Механизм хищений чужого имущества с использованием информационных технологий. Москва: Юрлитинформ, 2024. 184 с.
9. Фойницкий И. Я. Мошенничество по русскому праву: сравнительное исследование. С.-Петербург: тип. т-ва "Обществ. Польза", 1871. 256 с.
10. Харина Е. А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис... канд. юрид. наук. Краснодар, 2024. 248 с.
11. Жмуров Д. В. Кибервиктимология: концептуальные основы учения о жертве киберпреступлений: Издание 2-е, исправленное и дополненное. Санкт-Петербург: Научное издание, 2024. 410 с.
12. Евдокимов К. Н. Противодействие технотронной преступности: теория, законодательство, практика: монография. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры РФ, 2023. 171 с.

## Результаты процедуры рецензирования статьи

*В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.*

*Со списком рецензентов издательства можно ознакомиться [здесь](#).*

**Предмет исследования.** В рецензируемой статье «Историческая изменчивость компьютерной преступности: процесс расширения объекта и предмета преступных посягательств и её структура» предметом исследования являются нормы права, устанавливающие уголовную ответственность за киберпреступления.

**Методология исследования.** Методологический аппарат составили следующие диалектические приемы и способы научного познания: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация и обобщение. Отмечается применение современных методов, таких как: историко-юридический, теоретико-юридический, формально-логический, сравнительно-правовой, статистический, метод анализа конкретных правовых ситуаций и др. Применение современных научных методов позволило автору сформировать собственную аргументированную позицию по заявленной тематике.



Актуальность исследования. Актуальность темы рецензируемой статьи не вызывает сомнения. Происходящая в настоящее время цифровая трансформация всех сфер жизнедеятельности людей обуславливает необходимость обновления правового регулирования. Особую озабоченность государства и общества вызывает стремительный рост киберпреступности. Правовое регулирование, в том числе его охранительная составляющая, отстает от стремительной динамики общественных отношений. «...Развитие компьютерной преступности напрямую связано с технологическими трендами, такими как искусственный интеллект, блокчейн, интернет вещей (IoT) и квантовые вычисления». Автор статьи правильно отмечает, что «...компьютерная преступность в её современном состоянии далеко не тождественна тому явлению, которое существовало ещё относительно недавно – те же 30–40 лет назад». Доктринальные разработки по данной проблематике необходимы в целях совершенствования уголовного законодательства и практики его правоприменения.

Научная новизна. Не подвергая сомнению важность проведенных ранее научных исследований, послуживших теоретической базой для данной работы, тем не менее, можно отметить, что в этой статье сформулированы заслуживающие внимания положения, которые указывают на важность этого исследования для юридической науки и его практическую значимость: «Влияние экономических и технологических факторов проявляется в расширении объектов и предметов преступных посягательств, что напрямую связано с развитием экономических отношений и технологий. Переход на безналичные расчёты, распространение электронной торговли и цифровых активов создали новые возможности для преступников, что привело к смещению акцентов в структуре преступности. Историческая изменчивость компьютерной преступности проявляется в её постепенном замещении традиционных форм преступности, таких как уличные кражи и мошенничества». В статье содержатся и другие положения, которые отличаются научной новизной. Несомненно это исследование можно расценивать как вклад в отечественную юриспруденцию.

Стиль, структура, содержание. Тема раскрыта. Статья по содержанию соответствует своему названию. Автором соблюдены требования к объёму материала. Статья написана научным стилем, грамотно использована специальная терминология, в том числе и юридическая. Автором предпринята попытка структурировать статью. Так, статья состоит из введения, основной части и заключения. Введение отвечает установленным требованиям, в нем обоснована актуальность темы исследования, определена его методология. В основной части материал изложен последовательно и ясно. Теоретические положения дополнены актуальными статистическими данными. Для улучшения восприятия материала автор использовал таблицы, рисунки. В заключении сформулированы конкретные итоги исследования.

Замечания технического характера следующие:

- 1.Скорректировать название статьи, поскольку оно должно быть более кратким.
- 2.При упоминании других ученых в тексте статьи необходимо указывать фамилию и инициалы (а не только фамилию).

Других замечаний нет.

Библиография. Автором использовано достаточное количество доктринальных источников. Ссылки на источники оформлены с соблюдением требований библиографического ГОСТа.

Апелляция к оппонентам. По спорным вопросам заявленной тематики представлена научная дискуссия, обращения к оппонентам корректные. Все заимствования оформлены ссылками на автора и источник опубликования.

Выводы, интерес читательской аудитории. Статья «Историческая изменчивость компьютерной преступности: процесс расширения объекта и предмета преступных

посягательств и её структура» может быть рекомендована к опубликованию. Статья отвечает редакционной политике журнала «Полицейская деятельность». Статья написана на актуальную тему, отличается научной новизной и имеет практическую значимость. Данная статья могла бы представлять интерес для широкой читательской аудитории, прежде всего, специалистов в области уголовного права, а также, была бы полезна для преподавателей и обучающихся юридических вузов и факультетов.