

Научная статья

УДК 343.97

EDN QQNJAR

DOI 10.17150/2500-4255.2024.18(6).624-635



## ФАКТОР ЦИФРОВОГО НЕРАВЕНСТВА (РАЗРЫВА) И ЕГО ВЛИЯНИЕ НА ГЕОГРАФИЮ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

**А.А. Комаров***Новосибирский государственный университет экономики и управления, г. Новосибирск, Российская Федерация*

### Информация о статье

Дата поступления

9 сентября 2024 г.

Дата принятия в печать

20 декабря 2024 г.

Дата онлайн-размещения

27 декабря 2024 г.

### Ключевые слова

Интернет; компьютеры; география преступности; цифровое неравенство; цифровой разрыв; тенденции; компьютерная преступность

**Аннотация.** «Цифровой разрыв» отражает неравномерность территориального распространения информационно-коммуникативных технологий. Данное обстоятельство должно влиять на возможность реализации преступных намерений. К сожалению, уже имеющиеся в криминологии работы по вопросам компьютерной преступности (киберпреступности) не устраняют неполноту наших знаний о ее географии.

Вместе с тем в публикациях последних лет наличие цифрового неравенства российских регионов признается условием преступности. Однако это утверждение в своей содержательной части фактологически еще не уточнялось. Наша статья посвящена решению этой задачи.

В результате исследования выявлены недостатки учетно-регистрационной дисциплины, влияющие на полноту наших представлений о географии компьютерной преступности. Приведены расчетные показатели состояния компьютерной преступности по федеральным округам и отдельным регионам. Выстроен ранжир регионов по уровню компьютерной преступности, который далее сличен с ранжирами уровня цифровизации российских регионов. Сделаны обобщающие выводы на этот счет.

### Original article

## THE FACTOR OF DIGITAL INEQUALITY (DIVIDE) AND ITS IMPACT ON THE GEOGRAPHY OF CYBERCRIME

**Anton A. Komarov***Novosibirsk State University of Economics and Management, Novosibirsk, the Russian Federation*

### Article info

Received

2024 September 9

Accepted

2024 December 20

Available online

2024 December 27

### Keywords

Internet; computers; geography of crime; digital inequality; digital divide; trends; cybercrime

**Abstract.** The «digital divide» reflects the uneven territorial distribution of information and telecommunication technologies. This phenomenon ought to have an influence on the opportunities for implementing criminal intentions. Unfortunately, the existing criminological works on computer crime (cybercrime) do not provide enough information on its geography.

At the same time, the publications of recent years recognize that the existence of a digital divide as a condition for crime. However, this statement has not yet been proven by facts. The current work is devoted to solving this problem.

The conducted research revealed some drawbacks in record-keeping and registration that influence the scope of our understanding of the geography of cybercrime. The author presents the calculated values regarding the condition of computer crime in federal districts and specific regions. The article contains a rating of the regions by their level of computer crime, which is then compared to the rating of the regions by their level of digitization. Some generalized conclusions are drawn on this basis.

### Введение

Нетрудно заметить, что внедрение компьютерной техники и информационно-коммуникативных технологий происходит весьма неравномерно, если говорить о конкретном географическом пространстве. Однако относительно «виртуального пространства» в теории уголовного права, а затем и в криминологии,

нет особого единства взглядов. Место совершения компьютерного преступления (особенно с использованием сетевых компьютерных технологий, мобильного доступа) трудно увязать с типом поселений или конкретной географической местностью. Некоторые отечественные [1, с. 415] и зарубежные [2] исследователи отмечают это обстоятельство в качестве одной из осо-

бенностей компьютерной преступности. По вопросу географии авторы высказываются обычно скупое, презюмируя мысль о том, что «виртуальное пространство» лишено географических критериев в материалистическом смысле этого слова. Такие взгляды встречаются в ряде диссертационных работ: Т.Л. Тропиной (2005), Т.М. Лопатиной (2006), А.С. Щуровой (2017), Д.В. Пучкова (2022), В.Ф. Джафарли (2022), М.Н. Туруновой (2022), Е.А. Родиной (2022). Вследствие чего отрицается сама необходимость работы с имеющимся массивом статистических данных о территориальном распределении преступлений.

С такой мыслью, в прикладном ее выражении, трудно согласиться, ибо данное обстоятельство указывает всего лишь на свойство части компьютерной преступности — дистанционный способ совершения, который не стоит абсолютизировать. В уголовном праве и уголовно-процессуальной науке определение места совершения компьютерного преступления сегодня составляет насущную проблему и активно разрабатывается [3, с. 128; 4, с. 165]. Однако криминологическая наука пока еще не имеет надлежащих примеров исследования официальной статистической отчетности на предмет особенностей территориального распределения компьютерной преступности. Работы последних лет устраняют неполноту наших знаний о причинах [5] компьютерной преступности, личности виновных [6] или их жертв [7; 8]. Или в лучшем случае, рассматривая неравномерность информатизации как условие преступности, авторы сразу приступают к функциональному анализу зависимостей, при отсутствии фактического подтверждения свойства массовости в ее статистическом выражении. Вместе с тем правильнее было бы идти в изучении детерминации от простого к сложному. Начиная с факторного анализа, переходить к выявлению функциональных связей и лишь потом — причинно-следственных. Иначе возникает опасность превращения современных криминологических исследований по вопросам компьютерной преступности в консенсуальное социологическое клише на базе суждений о всеместности, неизбежности, поголовной «дигитализации» населения и общественных отношений. В то время как официальная уголовная статистика дает большую эмпирическую базу в распоряжение криминолога для подтверждения или же опровержения подобных утверждений.

Очевидно, что наше исследование, являясь первой попыткой уголовно-статистического анализа закономерностей территориального

распределения компьютерной преступности, не лишено недостатков. Однако ключевые идеи, заложенные в данной работе, могут послужить прологом для дальнейшего исследования географии компьютерной преступности.

### **Проблема фиксации места совершения компьютерного преступления в статистической отчетности**

Для решения этой проблемы существуют два основных практических приема.

Первый прием фиксации реализуется в случае, если место совершения преступления «установлено». Тогда в соответствии со Справочником № 2, составленном ФКУ «Главный информационно-аналитический центр МВД РФ» для заполнения документов первичного учета, в статистическую отчетность попадают сведения о типах поселения и местности. Есть в данных указаниях и сведения об объектах, на которых произошло преступление, но тогда речь будет идти уже о топографии и топонимике преступности. Это были бы весьма ценные сведения, коль скоро при заполнении карточек первичного статистического учета они не указывались произвольно. Произвольность проистекает из того, что в правоприменительной практике и теории не существует однозначной позиции по поводу места совершения компьютерного преступления [9, с. 49]. Подавляющее большинство компьютерных преступлений имеют материальный состав. Одни следователи при квалификации деяния определяют место преступления по совершению действий, а иные — по месту наступления последствий [10, с. 57]. В п. 19 Постановления Пленума Верховного Суда РФ № 37 от 15.12.2022 г. «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» предлагается в качестве такового определить место выполнения объективной стороны состава преступления вне зависимости от места наступления преступных последствий. Но значительное число сотрудников при заполнении статистических документов отождествляет место преступления и место происшествия [11, с. 14]. Исследуя такие данные, мы обретаем представление не о действительном территориальном распределении преступлений, а, скорее, о распределении усилий правоохранительных органов по борьбе с данным видом преступности.

Второй прием тоже не лишен недостатков и применяется в том случае, когда место преступления не установлено. При этом в карточку первичного статистического учета заносится информация о месте его выявления. В этой связи весьма значимым становится поведение самой жертвы. В большинстве случаев потерпевшие обращаются с заявлением о нарушении преступлением своих прав в территориальный орган МВД по месту жительства. Это подтверждается статистическими данными криминалистов, ведь в 97 % случаев поводом к возбуждению уголовного дела становится заявление потерпевшего [12, с. 115]. Зачастую личность виновного так и не удается установить, как и место, откуда он действовал. Учитывая трудности, возникающие на первоначальных этапах расследования, статистика выявленных преступлений в этом случае отражает скорее территориальную активность жертв по подаче заявлений.

Поскольку проблема определения места совершения компьютерного преступления остается не до конца закрытой, то это негативным образом сказывается на качестве собираемых статистических данных.

#### Расчетные показатели географии компьютерной преступности в 2018–2023 гг.

Для обнаружения действительных закономерностей распределения компьютерной преступности мы рассчитали для всех регионов и сгруппировали по федеральным округам Российской Федерации отдельные криминологические показатели преступлений, совершенных в информационно-телекоммуникационной сфере. Данные о состоянии преступности были заимствованы из официальной отчетности Генеральной прокуратуры РФ, размещенной на интернет-портале «Правовая статистика» (crimestat.ru). Отсутствующие в открытом доступе данные за 2023 г. были любезно предоставлены нашими рецензентами, за что им выражаем огромную благодарность. В качестве единицы учета мы брали абсолютное значение числа преступлений, совершенных на определенной территории за отчетный период. Данные о демографии регионов мы почерпнули с официального сайта Росстата (rosstat.gov.ru). Был учтен тот факт, что два региона РФ — Республика Бурятия и Забайкальский край — в 2018 г. перешли в состав Дальневосточного федерального округа. В наших расчетах они сразу перегруппированы на современный лад (табл. 1).

Таблица 1 / Table 1

#### Ранжир федеральных округов относительно медианы уровня преступлений, совершенных в информационно-телекоммуникационной сфере (2018–2023 гг.)

##### Ranging of Federal Districts relative to the median level of cybercrimes (2018–2023)

Регион / Region	К(п) в расчете на 100 тыс. населения (удельный вес, % от числа совершенных преступлений) / Crimes per 100 th. residents (specific weight of the number of committed crimes)					
	2018	2019	2020	2021	2022	2023
Уральский федеральный округ / Ural Federal District	148,9 (13,1)	240,1 (11,8)	372,6 (10,4)	365,4 (10,2)	354,7 (10,0)	457,8 (9,6)
Северо-Западный федеральный округ / Northwestern Federal District	84,7 (8,4)	160,4 (8,9)	358,7 (11,3)	363,0 (11,5)	359,9 (11,4)	472,9 (11,2)
Сибирский федеральный округ / Siberian Federal District	118,5 (14,6)	208,9 (14,2)	357,4 (13,8)	348,5 (13,4)	331,7 (12,8)	474,1 (13,5)
Приволжский федеральный округ / Volga Federal District	113,3 (23,9)	204,6 (23,9)	327,4 (21,6)	315,4 (20,8)	317,7 (20,9)	445,5 (21,9)
Дальневосточный федеральный округ / Far Eastern Federal District	110,1 (6,5)	185,6 (6,0)	302,3 (5,6)	313,1 (5,8)	306,9 (5,7)	426,4 (5,8)
Медиана по РФ / RF Median	91,8 (–)	174,4 (–)	303,7 (–)	295,3 (–)	309,1 (–)	407 (–)
Южный федеральный округ / Southern Federal District	81,1 (9,5)	153,3 (10,2)	269,7 (10,0)	287,4 (10,8)	291,9 (11,0)	375,5 (10,7)
Центральный федеральный округ / Central Federal District	69,5 (19,5)	131,8 (21,1)	266,9 (23,7)	263,7 (23,5)	265,8 (23,7)	334,9 (23,1)
Северо-Кавказский федеральный округ / North Caucasian Federal District	41,4 (2,9)	70,5 (2,8)	126,9 (2,8)	130,8 (3,0)	140,0 (3,2)	178,3 (3,1)
Российская Федерация / Russian Federation	95,4 (100)	170,2 (100)	302,8(100)	301,4(100)	300,8(100)	398,7(100)

Расчет коэффициента вариации и анализ шестилетних значений среднеквадратичного отклонения коэффициентов преступности по всем субъектам РФ указывают на то, что уголовная статистика устоялась и формируется достаточно однородно только с 2020 г. Именно этот небольшой объем исходных данных наиболее пригоден для обследования проблем компьютерной преступности на сегодняшний момент.

Сравнение объемов совершенных преступлений указывает на лидерство Центрального и Приволжского федеральных округов (45 % всех преступлений за 2023 г.). Почти половина всех преступлений в Центральном округе приходится на один субъект Российской Федерации — г. Москву, где в 2023 г. было совершено 60,9 тыс. преступлений из общего объема в 159 тыс. В Приволжском федеральном округе особой криминальной пораженностью обладает Республика Татарстан. Показатели объема компьютерных преступлений здесь в 1,5–2 раза превышают значения в иных субъектах РФ этого макрорегиона. Большая часть этих преступлений совершена в столице республики — Казани. Примечательно, что эти два субъекта РФ являются и пионерами по внедрению информационных технологий [13, с. 232]. Из этого может произрасти гипотеза о влиянии типа поселения (и его размера) на состояние компьютерной преступности, о чем мы скажем чуть позднее.

Пока же заметим, что сравнение без перевода в относительные показатели не вполне корректно. После расчета коэффициента преступности картина существенным образом меняется. Первое место занимает Уральский федеральный округ, к которому за последние четыре года вплотную приблизился Северо-Западный. На втором месте находятся Сибирский и Приволжский федеральные округа. С показателями выше среднероссийских на третьем месте располагается Дальневосточный федеральный округ. Значения по нему почти всегда равняются медианным. Остальные федеральные округа все время находятся ниже отметки среднего значения коэффициента компьютерной преступности по России.

Расчетные данные указывают, что показатели распространенности способны меняться в зависимости от масштаба территории. Внутри каждого федерального округа встречаются кратно различающиеся по уровню преступности субъекты РФ. Наибольшей однородностью криминальной активности, с точки зрения раз-

маха вариации, обладают Дальневосточный и Уральский федеральные округа. В них различия коэффициента преступности отдельных регионов не превышает 2, сохраняясь в пределах 1,6–1,8 раза. В иных макрорегионах России такие различия составляют 2,2–2,7 раза. Исключением является Северо-Кавказский федеральный округ, где разница между уровнем преступности в Ставропольском крае и Чеченской Республике составляет 34 раза. Последняя по итогам 2023 г. представляет собой «статистическую аномалию», поскольку это единственный регион, в котором за всю историю статистических наблюдений за компьютерной преступностью отмечен отрицательный темп прироста по отношению к прошлому году. На это накладывается эффект «низкой базы» (в 2022 г. зарегистрировано 214 преступлений, в 2023 г. — 168), который ставит под сомнение возможность объективных замеров динамики, в принципе.

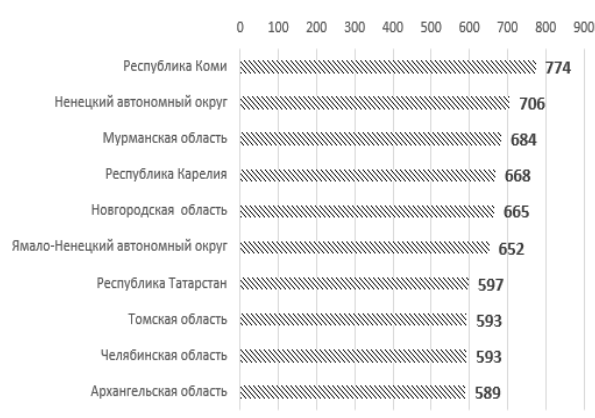
Места локализации компьютерных преступлений зачастую меньше размера отдельно взятого субъекта Федерации. Дисперсия объемов преступлений по территориям слабо отражает известные теории распространения преступности: радиальную, концентрическую [14].

Для наглядности мы выстроили ранжир отдельных регионов по уровню преступлений, связанных с информационно-телекоммуникационными технологиями, за 2023 г. В последующем он будет служить ориентиром читателю для самостоятельного сопоставления с уровнем цифровизации (рис.).

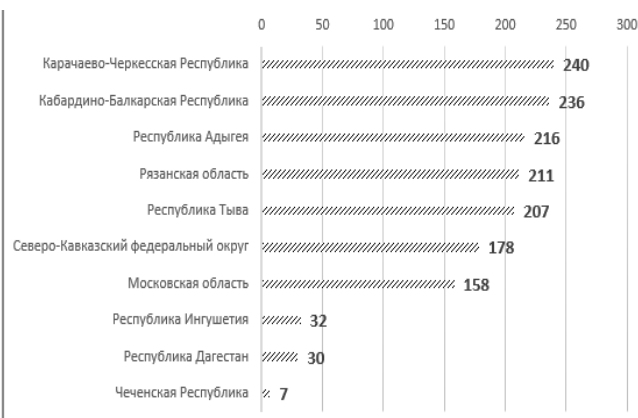
В качестве уточнения хотелось бы указать на то обстоятельство, что динамика компьютерной преступности от года к году непостоянна, т.е. не всегда сообразна представленным на рисунке регионам. Поэтому мы полагаем необходимым усреднить значения, начиная с 2020 г., чтобы выявить регионы с наиболее устойчивыми высокими и низкими показателями коэффициента преступности. Эти данные вошли в табл. 2.

Однако при проведении детальных расчетов выявлена зависимость коэффициента от структуры компьютерной преступности. Причем структура преступности неоднородна по регионам. Составляя ранжиры по другим строкам статистического учета, мы получили иное территориальное распределение коэффициентов преступности по субъектам РФ. Для расчетов мы использовали следующие показатели: преступления, совершенные при помощи сети Интернет; преступления, совершенные при по-





10 регионов с наибольшим уровнем преступлений  
в сфере информационно-коммуникативных  
технологий /  
10 regions with the highest level of cybercrime



10 регионов с наименьшим уровнем преступлений  
в сфере информационно-коммуникативных  
технологий /  
10 regions with the lowest level of cybercrime

### Ранжир регионов по уровню преступности за 2023 г. Ranging of regions by crime level, 2023

Таблица 2 / Table 2

### Средние значения уровня компьютерной преступности в РФ в 2020–2023 гг. Average level of cybercrime in the Russian Federation (RF) in 2020–2023

10 регионов с устойчиво высоким коэффициентом преступности / 10 regions with a stably high crime coefficient		10 регионов с устойчиво низким коэффициентом преступности / 10 regions with a stably low crime coefficient	
Республика Коми	586	Республика Тыва	223
Мурманская область	548	Кабардино-Балкарская Республика	193
Республика Карелия	524	Карачаево-Черкесская Республика	186
Ямало-Ненецкий автономный округ	488	Республика Адыгея	180
Челябинская область	471	Республика Калмыкия	179
Магаданская область	467	Рязанская область	172
Удмуртская Республика	463	Московская область	126
Архангельская область	456	Республика Ингушетия	28
Алтайский край	455	Республика Дагестан	25
Новгородская область	451	Чеченская Республика	7

мощи средств мобильной связи; преступления, совершенные с использованием компьютерной техники.

Это обстоятельство указывает на то, что уровень преступности слабо связан с фактическим размещением информационно-телекоммуникационной инфраструктуры. Большинство вычислительных мощностей сосредоточено в Москве и Санкт-Петербурге<sup>1</sup>. Такая несообразность объясняется тем, что уголовная статисти-

ка, как мы уже писали выше, учитывает местонахождение жертвы или преступника. При этом отдельные составы преступлений, связанные с нарушением правил эксплуатации информационной инфраструктуры, должны иметь более тесную привязку к месту нахождения оной. К таким преступлениям относятся посягательства на критически важную информационную инфраструктуру Российской Федерации или нарушения правил эксплуатации ЭВМ на конкретных объектах (предприятиях). Однако уголовная статистика страдает неполнотой. За пятилетие (2018–2023 гг.) было зарегистрировано 16 преступлений по ст. 274 УК РФ, а по ч. 3 ст. 274.1

<sup>1</sup> Российский рынок коммерческих дата-центров 2023 : аналит. отчет // IKS Consulting. 2024. URL: <https://survey.iksconsulting.ru/page30265406.html> (дата обращения: 28.04.2024).

УК РФ — 30 фактов. Выстроить какую-либо статистическую закономерность на основе приведенных данных не представляется возможным.

Географически зависимым оказывается распространение мошенничеств, связанных с дистанционной торговлей товарами и обманом потребителей, в том числе на вторичном рынке посредством электронных досок объявлений («Авито», «Юла» и иные) и социальных сетей. Среди 15 лидеров ранжира по преступлениям, совершенным посредством сети Интернет, достаточно много географически отдаленных регионов: Магаданская область, Ямало-Ненецкий автономный округ, Республика Коми, Ханты-Мансийский автономный округ, Удмуртская Республика, Амурская область, Республика Карелия, Еврейская автономная область, Мурманская область. Для жителей этих регионов дистанционный способ совершения сделки является если не единственным, то наиболее удобным способом приобрести необходимый товар. В результате чего в этих местностях растет количество потерпевших и заявлений о совершении преступления.

Но территориальное распределение преступлений, совершенных с использованием информационно-телекоммуникационных технологий, связано не только с закономерностями компьютерной преступности.

Перечень № 25 совместных указаний Генеральной прокуратуры и МВД РФ, регламентирующий порядок учета преступлений в информационно-телекоммуникационной сфере, предусматривает в качестве таковых наркопреступления. В структуре они занимают значимый удельный вес (15,4 %). Однако особенности их территориального распределения отвечают более закономерностям наркопреступности. По состоянию на 2023 г. в 10 регионов с наиболее высоким уровнем наркопреступлений, совершаемых посредством сети Интернет, входят: Ямало-Ненецкий автономный округ (205,1 на 100 тыс. населения); Челябинская область (168,8); Курганская область (122,4); Тюменская область (120,4); Кемеровская область (118,9); Омская область (112,7); Томская область (104,9); Мурманская область (104,3); Республика Татарстан (103,9); Ханты-Мансийский автономный округ — Югра (98,9); Пермский край (94). Большинство этих регионов отличает приграничное положение с Республикой Казахстан. Поэтому предупредительная работа, пресечение нарко-traфика для субъектов правоохранительной де-

ятельности становится в этой местности первоочередной задачей.

Свои особенности распределения в пространстве имеют «телефонные мошенничества», удельный вес которых составляет порядка 44,7 % от всех выявленных за 2023 г. информационно-телекоммуникационных преступлений. Они носят ярко выраженный общеуголовный характер, отличаясь от компьютерных преступлений, предусмотренных гл. 28 УК РФ. Значительная часть таких деяний относится к феномену пенитенциарной преступности. В этом случае они должны быть связаны с местоположением учреждений, исполняющих наказание в виде лишения свободы. Однако сопоставление 15 регионов-лидеров по численности «тюремного населения» с ранжиром уровня преступности, связанного с телефонным мошенничеством, не показывает какой-либо статистически значимой связи. Условное совпадение наблюдается только по пяти регионам: Республика Коми, Челябинская, Кемеровская, Архангельская области и Красноярский край. Подобное положение дел может объясняться тем обстоятельством, что связь в данном случае является функциональной. То есть имеет смысл добавлять в выборку и исследовать только конкретные объекты, на которых в большей степени наблюдаются нарушения установленного режима отбывания наказания. Проблема же состоит в том, что у нас фактически отсутствуют надлежащие статистические критерии для такого параллельного сравнения. Ибо нарушения режима различны по своему содержанию. Необязательно они связаны с использованием средств мобильной связи на территории исправительного учреждения. С другой стороны, нужно учитывать, что в большинстве случаев место нахождения преступника территориально не совпадает с местом жительства потерпевшего [15, с. 66], где оно по заявлению последнего и регистрируется. Мониторинг Всероссийского центра изучения общественного мнения указывает, что мошеннические звонки чаще поступают жителям крупных городов<sup>2</sup>. Еще одной причиной несоответствия территориального распределения может служить активизация борьбы с пенитенциарной преступностью в 2022 г., в результате которой число телефонных

<sup>2</sup> Телефонное мошенничество: мониторинг // ВЦИОМ. 2024. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring> (дата обращения: 28.04.2024).

мошенничеств, совершаемых из мест лишения свободы, снизилось<sup>3</sup>.

Вместе с тем существует гипотеза о территориальном перераспределении или «миграции телефонного мошенничества» на территорию современной Украины, где против россиян действуют организованные преступные группы<sup>4</sup>. Это отчасти способно объяснить существенный прирост подобных посягательств в прошлом году. Но фактологически, к сожалению, подобная гипотеза пока не может быть подтверждена.

### **Корреляция цифрового неравенства с состоянием компьютерной преступности**

Учитывая отсутствие универсальной методики рейтингования российских регионов в научной литературе, мы предлагаем опробовать несколько ранжиров из области социально-экономических исследований наших коллег.

По мнению Я.Ю. Бондаревой, используя методику Росстата, можно обозначить 15 регионов-лидеров и 15 регионов-аутсайдеров [16, с. 491]. При анализе состояния компьютерной преступности в этих регионах прямой зависимости не просматривается. В группе «лидеров» пять регионов имеют уровень преступности ниже, чем по федеральному округу. Можно выделить только шесть регионов, в которых он существенно (> 30 %) выше аналогичного показателя по соответствующему федеральному округу. При этом из группы аутсайдеров неожиданно высоким уровнем преступности выделяются три региона: Костромская область, Ненецкий автономный округ, Кировская область. Он превышает таковой даже относительно большинства регионов-лидеров из ранжира Бондаревой. Семь регионов-аутсайдеров согласуются с гипотезой, имея более низкий уровень преступности, чем соседние, более информационно развитые регионы.

На конечный результат могло повлиять то обстоятельство, что регионы в рейтинге Рос-

стата неустойчивы. В списках «лидеров» 2019 г. и 2021 г. совпадают только восемь регионов: Магаданская область, Ставропольский край, Новосибирская область, Свердловская область, Нижегородская область, Белгородская область, Сахалинская область, г. Санкт-Петербург. В большинстве из них (за исключением Магаданской области и Ставропольского края) уровень преступности равен или даже чуть ниже окружного. Ставропольский край является своеобразной «аномалией» Южного федерального округа, выказывая общероссийский уровень компьютерной преступности. На фоне соседних республик он действительно выглядит высоким.

Л.И. Власюк, стремясь преодолеть методические недостатки Росстата, предлагает собственный интегративный критерий цифровизации российских регионов [17, с. 59]. Однако ее группировка для наших целей представляется не вполне удачной. К группе «аутсайдеров» относится всего 12 субъектов РФ. В то время как к группе лидеров — целых 32 региона, которые разбиваются еще на два кластера. Эти кластеры отличаются экономическими параметрами. 20 регионов, ориентированных на коммерческое использование информационно-коммуникативных технологий. 12 регионов — с приоритетом на домашнем (бытовом) их применении. По 12 регионам-лидерам прямой зависимости не отмечается. Шесть регионов отличаются в большую сторону (> 30 %) от среднего по их федеральному округу. Три региона в значительно меньшую (< 30 %).

Более или менее слитное единство образуют только регионы-аутсайдеры. Они демонстрируют более низкий уровень преступности в своих федеральных округах. Исключение из правил составляют ряд республик Северного Кавказа (Республика Северная Осетия — Алания, Кабардино-Балкарская Республика, Карачаево-Черкесская Республика), где уровень преступности выше среднего по округу. При этом в Дагестане, Чеченской, Ингушской республиках выявлен аномально низкий уровень компьютерной преступности. Это сильно занижает показатели Северо-Кавказского федерального округа в целом. Поэтому справедливо было бы сравнивать их со средними показателями рассчитанного нами коэффициента преступности для России. В таком случае он однозначно будет ниже среднероссийского.

Но выявленная зависимость для регионов-аутсайдеров довольно очевидна. Отсутствие

<sup>3</sup> Клинический психолог назвал фразу, которая может нейтрализовать телефонных мошенников // Московская газета. 2023. 9 марта. URL: <https://msgazeta.ru/obshchestvo/klinicheskij-psiholog-nazval-frazu-kotoraya-mozhet-nejtralizovat-telefonnyh-moshennikov-11711.html> (дата обращения: 28.04.2024).

<sup>4</sup> Из интервью заместителя председателя Сберегательного банка С. Кузнецова // Известия. 2024. 4 июня. URL: <https://iz.ru/1706227/natalia-ilina/na-ukraine-protiv-rossii-rabotaet-350-400-moshennicheskikh-kollecenrov> (дата обращения: 04.11.2014).

технологий равняется отсутствию возможности совершать компьютерные преступления. Обратная же закономерность для передовых в информационном плане регионов статистически не может быть подтверждена.

В качестве гипотезы стоит принять во внимание и специфику современного сверхкрупного города. Его эффективное развитие сегодня немыслимо без широкого внедрения в жизнь компьютерных технологий. Влияние «Интернета вещей», скоростного мобильного интернета должно более интенсивно отражаться на жизни и поведении его жителей. Любопытно, что в одном из исследований Московской школы управления «СКОЛКОВО» делается акцент на независимости показателей темпов информатизации и размера города<sup>5</sup>. В 2014 г. ими впервые

<sup>5</sup> Цифровая жизнь российских регионов, 2020: стат. сб. URL: [https://iems.skolkovo.ru/downloads/documents/SKOLKOVO\\_IEMS/Research\\_Reports/SKOLKOVO\\_IEMS\\_Research\\_Digital\\_life\\_of\\_russian\\_regions\\_2020-06-09\\_ru.pdf](https://iems.skolkovo.ru/downloads/documents/SKOLKOVO_IEMS/Research_Reports/SKOLKOVO_IEMS_Research_Digital_life_of_russian_regions_2020-06-09_ru.pdf) (дата обращения: 15.03.2024).

было проанализировано состояние информатизации в городах-миллионниках, а в последующие годы в выборку добавились менее крупные города. Верна ли эта закономерность для территориального распределения компьютерной преступности?

Наши замеры уровня компьютерной преступности в регионах с городами-миллионниками зависимости от размера города также не выявляют. Свериться с данными можно по табл. 3, где регионы ранжированы по состоянию преступности и числу жителей их столиц на 2023 г.

При этом наблюдается любопытная зависимость, складывающаяся в области учетно-регистрационной дисциплины, как минимум, последние два календарных года. Различия в показателях «окружных» коэффициентов и «региональных» всегда складываются в одну и ту же сторону. То есть субъект Федерации из года в год отличается по коэффициенту либо в большую, либо в меньшую сторону. «Смены ролей» не происходит или происходит весьма редко,

Таблица 3 / Table 3

**Уровень компьютерной преступности в регионах с городами-миллионниками в 2023 г.**  
**Cybercrime levels in the regions with cities having over 1 mln. residents in 2023**

Субъект РФ в составе с городом-миллионником / Subject of the RF with a city having over 1 mln. residents	Коэффициент компьютерной преступности в расчете на 100 тыс. населения / Cybercrime coefficient per 100 th. residents	Среднее значение коэффициента компьютерной преступности по соответствующему федеральному округу РФ / Average coefficient of cybercrime in the corresponding Federal District of the RF	Различие в показателях (+/-) / Difference in indicators		Удельный вес города в численности населения региона, % / Specific weight of the city in the number of residents in the region, %
			за 2023 г. / for 2023	за 2022 г. / for 2022	
Москва / Moscow	388,5	334,9	+53,6	+55,81	98,3
Санкт-Петербург / Saint Petersburg	406,7	472,9	-66,2	-39,57	100
Новосибирская область / Novosibirsk Region	432,6	474,1	-41,5	-60,86	58
Свердловская область / Sverdlovsk Region	303,5	457,8	-154,3	-111,87	35
Республика Татарстан / Tatarstan Republic	597,3	445,5	+151,8	+66,89	31
Нижегородская область / Nizhni Novgorod Region	373,7	445,5	-71,8	-18,48	40
Челябинская область / Chelyabinsk Region	592,7	457,8	+134,9	+80,59	34



Окончание табл. 3 / The End of the table 3

Субъект РФ в составе с городом-миллионником / Subject of the RF with a city having over 1 mln. residents	Коэффициент компьютерной преступности в расчете на 100 тыс. населения / Cybercrime coefficient per 100 th. residents	Среднее значение коэффициента компьютерной преступности по соответствующему федеральному округу РФ / Average coefficient of cybercrime in the corresponding Federal District of the RF	Различие в показателях (+/-) / Difference in indicators		Удельный вес города в численности населения региона, % / Specific weight of the city in the number of residents in the region, %
			за 2023 г. / for 2023	за 2022 г. / for 2022	
Самарская область / Samara Region	400,9	445,5	-44,6	-16,93	36
Республика Башкортостан / Bashkortostan Republic	414,0	445,5	-31,5	-36,23	28
Ростовская область / Rostov Region	353,4	375,5	-22,1	-8,38	27
Омская область / Omsk Region	491,8	474,1	+17,7	+6,63	61
Красноярский край / Krasnoyarsk Region	494,1	474,1	+20	+12,66	39
Воронежская область / Voronezh Region	374,2	334,9	+39,7	+35,08	46
Пермский край / Perm Region	527,1	445,5	+81,6	+6,55	41
Волгоградская область / Volgograd Region	388,3	375,5	+12,8	+16,77	40

что свидетельствует об устойчивости территориального распределения компьютерной преступности вне зависимости от ее динамики.

Таким образом, прирост в 2023 г. (+29,7 % по отношению к прошлому году) обеспечен не столько улучшением выявляемости таких преступлений в крупных городских агломерациях, сколько усилением борьбы с компьютерной преступностью в менее крупных регионах.

В целом ряде федеральных округов существенный вклад в число совершаемых преступлений вносят более мелкие муниципальные образования. А уровень и качество жизни в них мало отличаются с точки зрения возможности реализации преступных наклонностей. В отдельных регионах с крупными региональными центрами уровень компьютерной преступности превышает таковой у городов-миллионников и средний по федеральному округу. Например, Алтайский край при численности краевого центра (г. Барнаул) 623 тыс. жителей имеет коэффициент компьютерной преступности 583,5. Курганская область (г. Курган — 305 тыс.) имеет коэффициент 457,7.

Поэтому гипотеза о большей степени информатизации и криминогенности крупных городских агломераций не подтверждается фактическими данными. С учетом того, что наши коллеги из «СКОЛКОВО» не находят прямой зависимости между спросом на информационные технологии и их предложением со стороны бизнес-структур, мы вынуждены констатировать внеэкономическую природу информатизации российского общества. Драйвером роста информатизации выступают государственный и муниципальный секторы, иницирующие частно-государственное партнерство. Поэтому уровень ее распространения не зависит исключительно от экономических возможностей того или иного региона.

Более того, благодаря принимаемым административно-командным решениям органов федеральной власти, цифровой разрыв в развитии отдельных регионов Российской Федерации теряет былую актуальность. При реализации многих федеральных целевых

программ устраняется неравномерность развития информационных технологий, увеличивается доступность интернета и средств мобильной связи. Следовательно, определяющего воздействия данное условие на развитие компьютерной преступности на современном этапе не оказывает.

### Заключение

Подводя итоги нашего исследования, резюмируем следующие выводы.

1. Существующая проблема фиксации места совершения компьютерного преступления налагает серьезные ограничения на исследовательские возможности по изучению географии преступности. Как показывает практика, в большинстве случаев при заполнении документов первичного статистического учета место преступления отождествляется с местом происшествия. А активность жертв преступлений вынуждает фиксировать эти деяния в уголовной статистике по месту выявления.

2. Коэффициент вариации и анализ пятигодичных значений среднеквадратичного отклонения коэффициентов преступности по всем субъектам РФ показали, что наиболее пригоден для обследования проблем компьютерной преступности лишь объем данных, накопленных с 2020 г. Полагаем, что далее в официальной уголовной статистике массив данных будет только накапливаться. В том числе имеются признаки его качественно-го улучшения, детализации отдельных строк учета. Однако выбранная Генеральной прокуратурой с 2023 г. политика «отказа от раскрытия информации» на портале «Правовая статистика», сокращает возможности для добровольного участия научной общественности в информационно-консультативном обеспечении деятельности по предупреждению.

3. Обобщенные показатели преступлений, совершенных в информационно-телекоммуникационной сфере, не отражают состояния какого-либо отдельного вида преступности. Ранжиры распространенности тех или иных групп преступлений, обособленных в качестве строк статистического учета, указывают на независимость географии таких видов преступности, как «телефонное» общеуголовное мошенничество, интернет-преступность, компьютерная информационная преступность.

4. Показатели распространенности преступлений, совершенных при помощи инфор-

мационно-телекоммуникационных технологий, зависят от масштаба рассматриваемой территории. Наибольшей однородностью криминальной активности обладают Дальневосточный и Уральский федеральные округа. Однако даже на их примере не соблюдаются закономерности известных теорий распространения преступности: радиальной, концентрической.

5. Корреляция цифрового неравенства с состоянием компьютерной преступности проявляется неоднозначно, поскольку в социально-экономических исследованиях имеются собственные методологические сложности с определением надлежащих индикаторов и построением ранжиров регионов. Мы с большей уверенностью можем констатировать наличие такой зависимости среди регионов-аутсайдеров по части информатизации, нежели у регионов-лидеров. Отсутствие технологий равняется отсутствию возможности совершать компьютерные преступления. Обратная же закономерность — для передовых в информационном плане регионов — статистически не может быть подтверждена.

6. Гипотеза о большей степени информатизации и криминогенности крупных городских агломераций не подтверждается фактическими данными. В целом ряде федеральных округов существенный вклад в число совершаемых преступлений вносят более мелкие муниципальные образования. А уровень и качество жизни в них мало отличаются с точки зрения возможности реализации преступных наклонностей.

7. Благодаря принимаемым административно-командным решениям органов федеральной власти цифровой разрыв в развитии отдельных регионов Российской Федерации теряет былую актуальность. При реализации многих федеральных целевых программ устраняется неравномерность развития информационных технологий, увеличивается доступность интернета и средств мобильной связи. Полагаем, что ни дальнейшее увеличение компьютерного парка, ни увеличение количества пользователей не способно существенным образом повлиять на развитие компьютерной преступности. Увеличение числа регистрируемых преступлений обеспечивается за счет улучшения деятельности правоохранительных органов и сокращения латентной части компьютерной преступности.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ


1. Евдокимов К.Н. Противодействие компьютерной преступности : дис. ... д-ра юрид. наук : 12.00.08. / К.Н. Евдокимов. — Москва, 2021. — 557 с.
2. Exploring the global geography of cybercrime and its driving forces / S. Chen, M. Hao, F. Ding [et al.]. — DOI 10.1057/s41599-023-01560-x // *Humanities and social sciences communications*. — 2023. — Vol. 10, no. 1. — P. 71–81.
3. Овсюков Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации : дис. ... канд. юрид. наук : 5.1.4 / Д.А. Овсюков. — Москва, 2022. — 231 с.
4. The criminal law influence on the modern electronic and information society of the Russian Federation / A.A. Komarov, E.A. Dorozhinskaya, V.I. Krupnitskaya, I.V. Rozuman. — EDN WZGTJD // *International Review of Management and Marketing*. — 2016. — Vol. 6, no. 6. — P. 165–168.
5. Кобец П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения / П.Н. Кобец. — DOI 10.37523/SUI.2022.47.1.007. — EDN PHOALB // *Вестник Самарского юридического института*. — 2022. — № 1 (47). — С. 52–58.
6. Джафарли В.Ф. Личность преступника в механизме преступлений, совершаемых в сфере информационных технологий / В.Ф. Джафарли. — Москва : КноРус, 2017. — 108 с. — EDN BMXHCJ.
7. Родина Е.А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве : дис. ... канд. юрид. наук : 5.1.4 / Е.А. Родина. — Саратов, 2022. — 217 с. — EDN MYDGRO.
8. Старостенко О.А. Виктимологическое предупреждение хищений, совершаемых дистанционно : дис. ... канд. юрид. наук : 5.1.4 / О.А. Старостенко. — Краснодар, 2023. — 232 с. — EDN CETPEL.
9. Грибанова Д.В. Место совершения хищения безналичных денег и территориальная подсудность уголовного дела / Д.В. Грибанова, П.П. Степанов. — DOI 10.52390/20715870\_2023\_9\_49. — EDN ZZGNHQ // *Уголовное право*. — 2023. — № 9. — С. 49–62.
10. Есаков Г.А. Место совершения преступления при хищении: новый подход судебной практики / Г.А. Есаков. — DOI 10.52390/20715870\_2023\_3\_54. — EDN TEXRBT // *Уголовное право*. — 2023. — № 3. — С. 54–60.
11. Степанова М.А. Проблемы определения места совершения хищения денежных средств с использованием информационно-телекоммуникационных технологий / М.А. Степанова, Е.В. Царёв. — EDN COYGXC // *Вестник Белгородского юридического института МВД России имени И.Д. Путилина*. — 2021. — № 1. — С. 12–16.
12. Старостенко Н.И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий : дис. ... канд. юрид. наук : 5.1.4 / Н.И. Старостенко. — Краснодар, 2023. — 230 с. — EDN BCNHDY.
13. Асалханова С.А. Проблемы цифрового неравенства регионов России / С.А. Асалханова, Т.А. Селищева. — EDN JINNNM // *Проблемы современной экономики*. — 2019. — № 3 (71). — С. 230–234.
14. Piscitelli A. The Geography of Crime: Placing Geographers in the Space of Criminologists : theses and dissertation / A. Piscitelli. — Milton, 2019. — 153 p.
15. Шатилов А.В. Особенности криминологической характеристики и предупреждения мошенничества, совершаемого организованными преступными формированиями : дис. ... канд. юрид. наук : 12.00.08 / А.В. Шатилов. — Саратов, 2019. — 210 с. — EDN FZPSXJ.
16. Бондарева Я.Ю. Влияние цифрового неравенства на пространственное развитие и сетевое взаимодействие регионов: актуальные исследования и подходы к оценке / Я.Ю. Бондарева. — EDN IQYXGM // *Экономика. Информатика*. — 2023. — Т. 50, № 3. — С. 491–500.
17. Власюк Л.И. Цифровое неравенство российских регионов: стратегические возможности и угрозы / Л.И. Власюк. — DOI 10.17073/2072-1633-2023-1-59-68. — EDN YIUJES // *Экономика промышленности*. — 2023. — Т. 16, № 1. — С. 59–68.

## REFERENCES


1. Evdokimov K.N. *Countering Computer Crime. Doct. Diss.* Moscow, 2021. 557 p.
2. Shuai Chen, Mengmeng Hao, Fangyu Ding, Dong Jiang, Jiping Dong, Shize Zhang, Qiquan Guo, Chundong Gao. Exploring the Global Geography of Cybercrime and its Driving Forces. *Humanities and Social Sciences Communications*, 2023, vol. 10, no. 1, pp. 71–81. DOI: 10.1057/s41599-023-01560-x.
3. Ovsyukov D.A. *Mercenary Crimes against Property with the Use of Information-telecommunication Networks: Questions of Qualification. Cand. Diss.* Moscow, 2022. 231 p.
4. Komarov A.A., Dorozhinskaya E.A., Krupnitskaya V.I., Rozuman I.V. The Criminal Law Influence on the Modern Electronic and Information Society of the Russian Federation. *International Review of Management and Marketing*, 2016, vol. 6, no. 6, pp. 165–168. EDN: WZGTJD.
5. Kobets P.N. Cybercrime: Modern Types, Causes Generating and Features of Prevention. *Vestnik Samarskogo yuridicheskogo instituta = Bulletin of the Samara Law Institute*, 2022, no. 1, pp. 52–58. (In Russian). EDN: PHOALB. DOI: 10.37523/SUI.2022.47.1.007.
6. Dzhafarli V.F. *The Identity of the Offender in the Mechanism of Crimes Committed in IT Sphere*. Moscow, KnoRus Publ., 2017. 108 p. EDN: BMXHCJ.
7. Rodina E.A. *Countering Criminal Victimization of Internet Users in Cyberspace. Cand. Diss.* Saratov, 2022. 217 p. EDN: MYDGRO.
8. Starostenko O.A. *Victimological Prevention of Theft Committed Remotely. Cand. Diss.* Krasnodar, 2023. 232 p. EDN: CETPEL.
9. Stepanov P.P., Griбанова D.V. Locus Delicti of Theft of Non-Cash Funds and Territorial Jurisdiction of a Criminal Case. *Ugolovnoe pravo = Criminal Law*, 2023, no. 9, pp. 49–62. (In Russian). EDN: ZZGNHQ. DOI: 10.52390/20715870\_2023\_9\_49.
10. Esakov G.A. Locus Delicti in Misappropriation: the New Approach in Judicial Practice. *Ugolovnoe pravo = Criminal Law*, 2023, no. 3, pp. 54–60. (In Russian). EDN: TEXRBT. DOI: 10.52390/20715870\_2023\_3\_54.

11. Stepanova M.A., Tsarev E.V. Problems of Determining the Place of Embezzlement of Funds Using Information and Telecommunications Technologies. *Vestnik Belgorodskogo yuridicheskogo instituta MVD Rossii imeni I.D. Putilina = Vestnik of Putilin Belgorod Law Institute of Ministry of the Interior of Russia*, 2021, no. 1, pp. 12–16. (In Russian). EDN: COYGXC.
12. Starostenko N.I. *Initial Stage of Investigation of Thefts Committed Using Methods of Social Engineering and Information and Telecommunication Technologies: Cand. Diss.* Krasnodar, 2023. 230 p. EDN: BCNHDY.
13. Selishcheva T.A., Asalkhanova S.A. Problems of Digital Inequality of Russia's Regions (Russia, St. Petersburg). *Problemy sovremennoi ekonomiki = Problems of Modern Economy*, 2019, no. 3, pp. 230–234. (In Russian). EDN: JINHNM.
14. Piscitelli A. *The Geography of Crime: Placing Geographers in the Space of Criminologists. Theses and Dissertation.* Milton, 2019. 153 p.
15. Shatilov A.V. *Specifics of Criminological Description and Prevention of Fraud Committed by Organized Criminal Groups. Cand. Diss.* Saratov, 2019. 210 p. EDN: FZPSXJ.
16. Bondareva Ya.Yu. The Impact of the Digital Divide on Spatial Development and Networking of Regions: Current Research and Assessment Approaches. *Ekonomika. Informatika = Economics. Information Technologies*, 2023, vol. 50, no. 3, pp. 491–500. (In Russian). EDN: IQYXGM.
17. Vlasyuk L.I. Digital Inequality of the Russian Regions: Strategic Opportunities and Threats. *Ekonomika promyshlennosti = Economy of Industry*, 2023, vol. 16, no. 1, pp. 59–68. (In Russian). EDN: YIUJES. DOI: 10.17073/2072-1633-2023-1-59-68.

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

Комаров Антон Анатольевич — доцент кафедры уголовного права и национальной безопасности Новосибирского государственного университета экономики и управления, кандидат юридических наук, г. Новосибирск, Российская Федерация; e-mail: reise83@mail.ru;  <https://orcid.org/0000-0002-1330-4236>.

#### INFORMATION ABOUT THE AUTHORS

Komarov, Anton A. — Ass. Professor, Department of Criminal Law and National Security, Novosibirsk State University of Economics and Management, Ph.D. in Law, Novosibirsk, the Russian Federation; e-mail:  reise83@mail.ru; <https://orcid.org/0000-0002-1330-4236>.

#### ДЛЯ ЦИТИРОВАНИЯ

Комаров А.А. Фактор цифрового неравенства (разрыва) и его влияние на географию компьютерной преступности / А.А. Комаров. — DOI 10.17150/2500-4255.2024.18(6).624-635. — EDN QQNJAR // Всероссийский криминологический журнал. — 2024. — Т. 18, № 6. — С. 624–635.

#### FOR CITATION

Komarov A.A. The Factor of Digital Inequality (Divide) and Its Impact on the Geography of Cybercrime. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 6, pp. 624–635. (In Russian). EDN: QQNJAR. DOI: 10.17150/2500-4255.2024.18(6).624-635.