Киберпреступность в регионах России: современные тенденции и меры предупреждения[1]

Ольга Романовна АФАНАСЬЕВА,
профессор кафедры криминологии и уголовно-исполнительного права имени Е. В. Эминова Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, доцент
orafanaseva@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Валентина Ивановна ШИЯН,
доцент кафедры правового обеспечения национальной безопасности, законности и правопорядка Российской академии народного хозяйства и государственной службы при Президенте РФ, кандидат юридических наук, доцент
valentina-shiyan@yandex.ru
119571, Россия, г. Москва, просп. Вернадского, д. 82, стр. 1

Аннотация. *В статье представлены результаты исследования современных тенденций киберпреступности в федеральных округах и субъектах РФ. Авторы отмечают, что эффективное предупреждение киберпреступности требует исследования ее характеристик не только на общероссийском, но и на региональном уровне, что позволит определить специфику криминальной пораженности регионов, осуществить их ранжирование, обусловит выявление проблем обеспечения региональной безопасности в различных субъектах РФ и своевременную выработку научно обоснованных рекомендаций по совершенствованию мер, направленных на снижение криминальной пораженности регионов.*

В числе основных современных тенденций киберпреступности авторы называют последовательный рост киберпреступлений как в целом по России, так и во всех ее федеральных округах на фоне общего снижения преступности; высокий уровень латентности и низкий уровень раскрываемости. Отмечается увеличение фактов участия в киберпреступности организованных преступных сообществ, увеличение материального ущерба киберпосягательств и появление новых форм угроз. Установлена выраженная территориальная дифференциация киберпреступности, обусловленная совокупным влиянием демографических, социокультурных, организационных и технологических факторов.

Ключевые слова: *киберпреступность, криминогенная обстановка, регионы России, киберугрозы, состояние преступности, тенденции преступности, меры предупреждения, региональная безопасность*

DOI: 10.17803/2311-5998.2025.129.5.034-047

[1] Данная статья подготовлена в рамках государственного задания РАНХиГС.

Olga R. AFANASIEVA,
Professor of the Chair of Criminology and Executive Law Chair named after E. V. Eminov of the Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Associate Professor
orafanaseva@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Valentina I. SHIYAN,
Associate Professor at the Department of Legal Support of National Security, Legality and Law and Order, Russian Presidential Academy of National Economy and Public Administration, Cand. Sci. (Law), Associate Professor
valentina-shiyan@yandex.ru
82/1, prosp. Vernadsky, Moscow, Russia, 119571

Cybercrime in the Regions of Russia: Current Trends and Preventive Measures

Abstract. *The article presents the results of a study on current trends in cybercrime across federal districts and regions of the Russian Federation. The authors emphasize that effective prevention of cybercrime requires analyzing its characteristics not only at the national level but also at the regional level. This approach makes it possible to identify the specific features of criminal victimization in different regions, rank them accordingly, and uncover problems related to ensuring regional security across various parts of Russia. It also enables the timely development of scientifically grounded recommendations aimed at improving measures to reduce regional criminal victimization.*

Among the main contemporary trends in cybercrime, the authors highlight the steady increase in cybercrime rates both across Russia as a whole and in all federal districts, despite the overall decline in crime. Other noted trends include a high level of latency and a low detection rate. The study also notes an increase in the involvement of organized criminal groups in cybercrime, greater financial damage from cyberattacks, and the emergence of new threat forms. A pronounced territorial differentiation of cybercrime has been identified, driven by the combined influence of demographic, sociocultural, organizational, and technological factors.

Keywords: *cybercrime, criminogenic situation, regions of Russia, cyber threats, crime situation, crime trends, preventive measures, regional security*

На всех этапах развития общества обеспечение региональной безопасности входило в число приоритетных направлений в практике государственных органов и общественных институтов. Вместе с тем усиленное внимание ученых к особенностям региональной преступности началось лишь в конце XIX столетия. Однако этот процесс осуществлялся настолько стремительно и плодотворно, что уже в начале XX в. обусловил появление «региональной

криминологии» — самостоятельного направления в науке. Примечательно, что практически во всех криминологических трудах того времени при исследовании различных видов преступности особое внимание уделялось специфике криминальной пораженности каждой губернии, области и округа Российской империи, которые, как правило, дифференцировали на четыре или шесть типологических групп.

Бесспорной является актуальность региональных криминологических исследований, которые в большинстве своем имеют лонгитюдный характер. Результаты подобных изысканий способствуют прежде всего своевременному выявлению криминальных угроз, изучению факторов преступности и учету особенностей их проявления в конкретном регионе, а также осуществлению криминологической классификации и ранжированию регионов, определению закономерностей и специфики видов преступности в них либо фиксации ее эмерджентного характера.

В современном мире геополитическая нестабильность, многочисленные угрозы военно-политического характера, широкое использование новейших информационно-телекоммуникационных технологий во всех сферах общественной жизни, в том числе и криминальной, совершенствование новых технологий цифровизации и роботизации, интеллектуальные системы безопасности и управления обусловили появление и последовательный рост киберпреступлений во всех государствах мира.

Исходя из канонов криминологии, под киберпреступностью целесообразно понимать совокупность киберпреступлений и лиц, их совершивших, на определенной территории, за определенный период времени.

Самая лаконичная дефиниция киберпреступления содержится в Модельном законе о противодействии киберпреступности, принятом на 55-м пленарном заседании Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств (постановление № 55-20 от 14.04.2023): «Киберпреступление — преступление, совершенное в киберпространстве» (ст. 2).

Полный перечень киберпреступлений представлен в указании Генпрокуратуры России и МВД России от 27.12.2024 № 952/11/3 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». Содержание данного нормативного правового акта наглядно свидетельствует, что киберпреступления не ограничены рамками главы 28 «Преступления в сфере компьютерной информации», а выходят далеко за ее пределы.

Рост цифровизации российского общества сопровождается резким увеличением количества и сложности киберпреступлений. Так, в 2024 г. было зарегистрировано 765 365 преступлений[2], совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступлений), что на 13,1 % выше показателя 2023 г. и в 2,59 раза больше значения 2019 г. (всего — 294 409 киберпреступлений). При

[2] Сводные отчеты по России «Сведения о состоянии преступности и результатах расследования преступлений» за 2019—2024 гг. ФКУ «Главный информационно-аналитический центр» Министерства внутренних дел РФ.

этом было выявлено 98 088 лиц, их совершивших, что ниже показателя 2023 г. на 6,6 % (рис. 1).

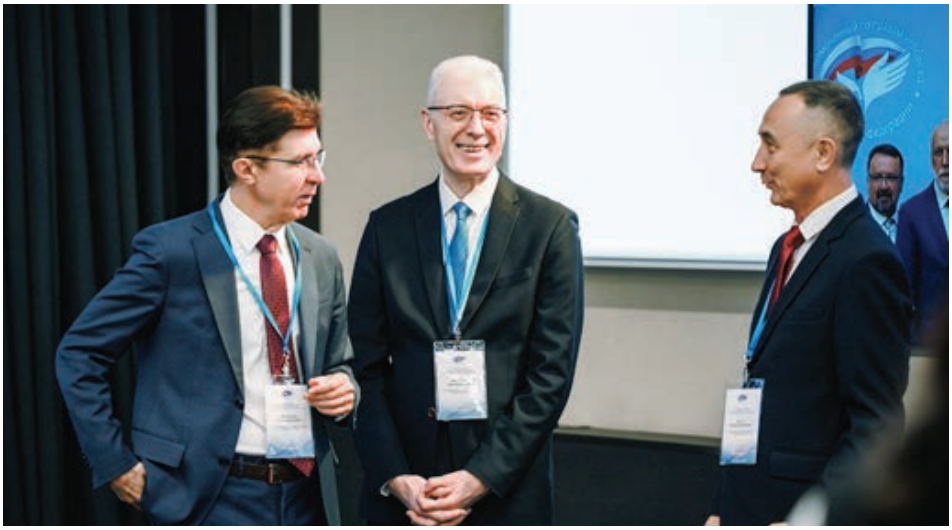

Рис. 1. Динамика количества зарегистрированных киберпреступлений и числа выявленных лиц в Российской Федерации в 2019—2024 гг.

Тенденция роста киберпреступлений наблюдается во всех федеральных округах Российской Федерации, при этом наибольшие темпы прироста, превышающие среднероссийское значение, отмечаются в Дальневосточном (+25,9 %), Приволжском (+20,6 %), Северо-Кавказском (+18,1 %) и Южном (+16,2 %) федеральных округах (рис. 2).

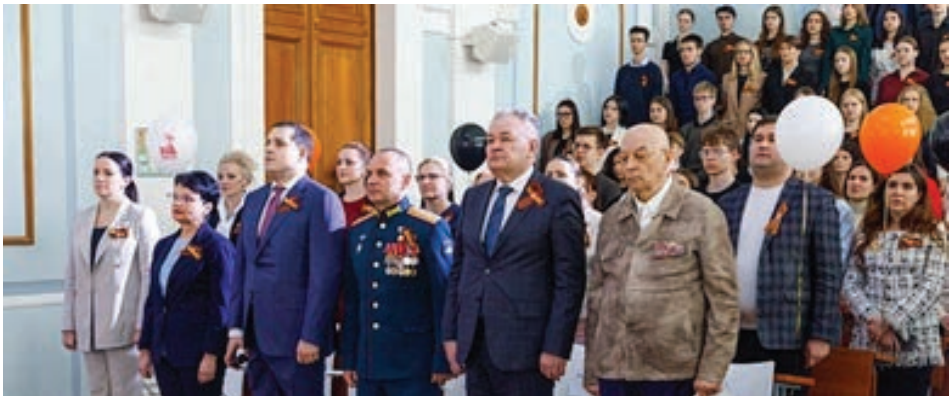

Рис. 2. Динамика зарегистрированных киберпреступлений в федеральных округах Российской Федерации в 2019—2024 гг.

Особенностью территориального распределения преступности в 2024 г. выступает то, что более половины всех зарегистрированных киберпреступлений

приходятся на три федеральных округа (58,7 %) и на 17 субъектов РФ (50,2 %), входящих в различные федеральные округа России (см. рис. 3, табл. 1).

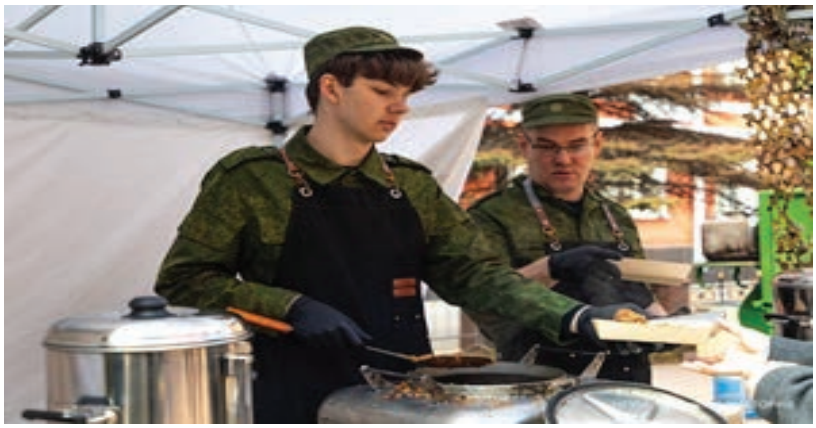

Рис. 3. Киберпреступность в Федеральных округах России в 2024 г.

Таблица 1

Субъекты Российской Федерации, в которых зарегистрировано наибольшее количество киберпреступлений в 2024 г.

№ п/п	Российская Федерация и ее субъекты	Федеральный округ РФ	Количество зарегистрированных преступлений	Удельный вес, %	Удельный вес (с нарастающим итогом), %
	Россия		765 365	100	100
1	Москва	ЦФО	63 621	8,3	8,3
2	Краснодарский край	ЮФО	33 489	4,4	12,7
3	Республика Татарстан	ПФО	32 073	4,2	16,9
4	Санкт-Петербург	СЗФО	29 783	3,9	20,8
5	Республика Башкортостан	ПФО	23 823	3,1	23,9
6	Челябинская область	УФО	21 793	2,8	26,7
7	Московская область	ЦФО	19 673	2,6	29,3
8	Пермский край	ПФО	19 396	2,5	31,8

№ п/п	Российская Федерация и ее субъекты	Федеральный округ РФ	Количество зарегистрированных преступлений	Удельный вес, %	Удельный вес (с нарастающим итогом), %
9	Красноярский край	СФО	18 055	2,4	34,2
10	Ростовская область	ЮФО	17 941	2,3	36,5
11	Свердловская область	УФО	17 419	2,3	38,8
12	Самарская область	ПФО	16 868	2,2	41,0
13	Волгоградская область	ЮФО	14 396	1,9	42,9
14	Ханты-Мансийский автономный округ	УФО	14 283	1,9	44,8
15	Алтайский край	СФО	14 236	1,9	46,6
16	Нижегородская область	ПФО	13 654	1,8	48,4
17	Новосибирская область	СФО	13 454	1,8	50,2

Несмотря на сохраняющуюся общероссийскую тенденцию к росту количества зарегистрированных преступлений в сфере информационных технологий, в отдельных регионах наблюдаются признаки обратной динамики. Так, в десяти субъектах РФ в 2024 г. зафиксировано снижение числа киберпреступлений (табл. 2). Вместе с тем данное сокращение не свидетельствует об ослаблении киберугроз как таковых. Наоборот, в ряде случаев наблюдается рост степени их общественной опасности, выраженный в увеличении размера причиненного материального ущерба. Так, по данным МВД по Республике Коми, несмотря на сокращение количества зарегистрированных преступлений в сфере кибербезопасности на 20,6 %, совокупный ущерб от них возрос на 17 % и превысил 1,3 млрд рублей[3]. Это может свидетельствовать как о смещении фокуса киберпреступной активности в сторону более сложных, целенаправленных схем, характеризующихся высокой эффективностью и значительными экономическими последствиями, так и о деятельности правоохранительных органов по выявлению и расследованию подобных фактов преступной активности.

[3] Доклад руководителя МВД Коми за 2024 год // URL: https://uhta.bezformata.com/listnews/komi-za-2024-god/144219358/ (дата обращения: 29.03.2025).

Таблица 2

Субъекты Российской Федерации, в которых зафиксировано снижение количества зарегистрированных киберпреступлений в 2024 г.

№ п/п	Субъекты РФ	Всего	Абсолютный прирост	Темп прироста, %
1	Челябинская область	—	–936	–4,1
2	Новосибирская область	13 454	–943	–6,5
3	Кемеровская область	12 923	–670	–4,9
4	Воронежская область	9 324	–376	–3,9
5	Ленинградская область	8 071	–568	–6,6
6	Ярославская область	6 166	–365	–5,6
7	Республика Коми	5 068	–1315	–20,6
8	Смоленская область	4 990	–368	–6,9
9	Ямало-Ненецкий автономный округ	3 307	–551	–14,3
10	Орловская область	3 241	–18	–0,6

В большинстве субъектов Российской Федерации наблюдается нарастание преступной активности в сфере использования информационно-телекоммуникационных технологий или компьютерной информации. В частности, в 50 регионах страны темпы относительного прироста числа зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, превысили среднероссийский показатель. Наиболее выраженная динамика зафиксирована в республиках Южного и Северо-Кавказского федеральных округов, а также в отдельных регионах Приволжья и Сибири.

Так, наибольшие темпы прироста в 2024 г. отмечаются в Чеченской Республике (+154,8 %), Республике Мордовия (+76,7 %), Республике Марий Эл (+67,1 %), Республике Адыгея (+60,6 %), Карачаево-Черкесской Республике (+59,7 %), Республике Дагестан (+57,3 %), Ханты-Мансийском автономном округе (+54,7 %), Республике Северная Осетия — Алания (+49,5 %), Еврейской автономной области (+43,5 %) и Псковской области (+42,0 %) (рис. 4).

Такие показатели могут свидетельствовать как о реальном росте преступной активности в указанных субъектах РФ, так и о повышении эффективности работы правоохранительных органов по выявлению киберпреступлений. Кроме того, данные тенденции требуют отдельного анализа с точки зрения факторов цифрового развития регионов, уровня интернет-проникновения и степени правовой осведомленности населения.

По итогам 2024 г. уровень криминальной нагрузки, обусловленный киберпреступностью, в Российской Федерации составил 523,68 преступления на 100 тыс. населения. Указанный показатель превышает значение 2023 г. на 13,27 % и в 2,6 раза превосходит уровневое значение 2019 г. Рост уровня киберпреступности отмечается во всех федеральных округах. Наибольшие значения уровня

Рис. 4. Субъекты Российской Федерации
с наибольшими темпами прироста киберпреступности в 2024 г.

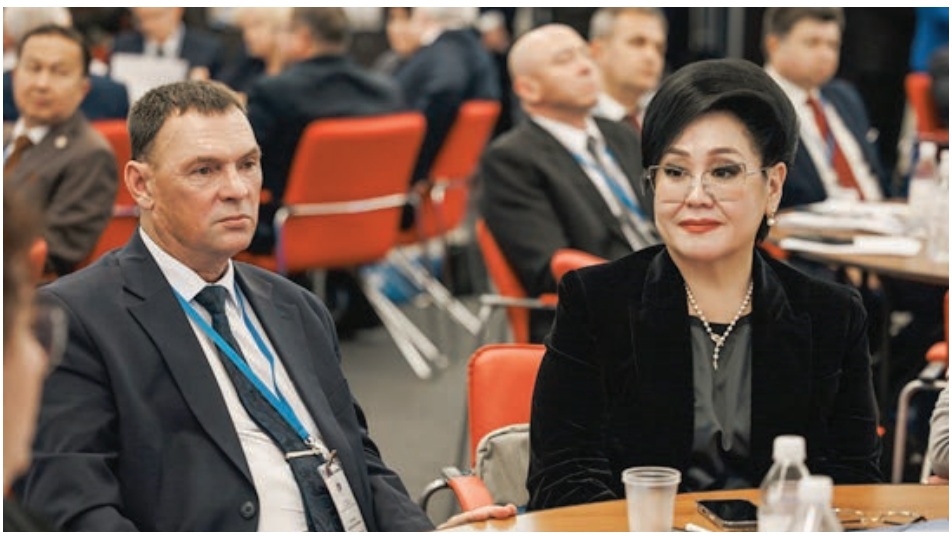

Рис. 5. Динамика уровня киберпреступности и коэффициента криминальной активности населения в Российской Федерации в 2019—2024 гг. (на 100 тыс. населения)

преступности, превышающие среднероссийский показатель, отмечены в Дальневосточном (623,7), Приволжском (622,8), Уральском (587,1), Северо-Западном (596,2) и Сибирском (575,9) федеральных округах (рис. 5, 6).

В 48 субъектах РФ уровень преступности превышает общероссийский, при этом в Ненецком автономном округе он выше общероссийского в два раза (1068,11 на 100 тыс. населения), в связи с чем данный регион отнесен к числу регионов с худшей криминальной ситуацией в сфере киберпреступности.

Столь высокий показатель уровня киберпреступности объясняется географической удаленностью и ограниченной доступностью традиционных форм финансового и потребительского обслуживания, высокой цифровой активностью населения, включая широкое распространение онлайн-сервисов, что, в свою очередь,

Рис. 6. Уровень киберпреступлений в федеральных округах в 2024 г. (на 100 тыс. населения)

расширяет потенциальные возможности для совершения киберпреступлений. Так, в 2024 г. в Ненецком АО уровень киберпреступлений составил (далее приведены данные на 100 тыс. населения):

— с использованием компьютеров — 423,93 преступления при среднероссийском показателе 28,97;
— с использованием сети Интернет — 1 006,54 преступления при среднероссийском показателе 444,1;
— с использованием средств мобильной связи — 532,87 преступления при среднероссийском показателе 236,76 преступления.

Негативное влияние на состояние киберпреступности может оказывать также недостаточная оснащенность правоохранительных органов региона специализированными техническими и кадровыми ресурсами для оперативного выявления и пресечения преступлений в цифровой среде.

Шесть регионов (Республика Марий Эл (977,53), Республика Карелия (952,17), Томская область (923,53), Новгородская область (907,69), Республика Удмуртия (888,43) и Кировская область (870,4)) образуют группу с высоким уровнем киберпреступности. Высокие показатели коэффициента киберпреступности, зафиксированные в таких субъектах РФ, требуют комплексного анализа с учетом социально-экономических, демографических, организационных и технологических факторов. Между тем возможно предположить, что одной из причин высокого уровня регистрируемых киберпреступлений является активное распространение цифровых технологий в условиях слабой цифровой гигиены и недостаточной правовой грамотности населения. Кроме того, в таких регионах, как Республика Удмуртия и Томская область, функционируют крупные промышленные и образовательные центры, что обеспечивает высокий уровень интернет-активности и широкой вовлеченности населения в дистанционные формы занятости, обучения и потребления.

Отмеченные значения уровня преступности могут быть следствием высокой активности органов внутренних дел по выявлению и регистрации киберпреступлений, в том числе благодаря функционированию специализированных подразделений в региональных управлениях МВД России.

В группу регионов с уровнем преступности выше среднего входят десять субъектов РФ: Мурманская область (837,7), Ханты-Мансийский автономный округ (811,82), Республики Татарстан (801,22) и Мордовия (798,28), Архангельская область (796,57), Пермский край (777,31), Амурская область (760,71), Еврейская автономная область (737,3), Псковская область (726,67) и Республика Коми (703,3).

61 субъект РФ образует группу регионов со средним уровнем киберпреступности. Это преимущественно субъекты РФ, входящие в состав Центрального, Приволжского, Северо-Западного и Южного федеральных округов.

Группу регионов с коэффициентом преступности ниже среднего значения составляют четыре субъекта РФ: Кабардино-Балкарская Республика (317,4), Рязанская область (286,4), Республика Тыва (271,7) и Московская область (227,4).

К регионам с низким коэффициентом преступности отнесены Республики Ингушетия (82,1), Дагестан (64,6) и Чеченская (27,6). Между тем в 2024 г. в Чеченской Республике отмечается наибольший темп прироста киберпреступности. Сложившаяся криминальная ситуация, существенно отличающаяся от среднероссийских значений, может быть интерпретирована посредством анализа влияния демографических, социокультурных и институциональных факторов.

Прежде всего необходимо учитывать ограниченный уровень цифровизации и относительно низкую вовлеченность населения данных регионов в электронную коммерцию, онлайн-сервисы и дистанционные формы социальной активности. Несмотря на активное развитие инфраструктуры связи, в отмеченных республиках сохраняются низкие показатели охвата населения Интернетом по сравнению с другими субъектами РФ, особенно в сельских и горных районах регионов. Это объективно снижает как потенциальную вовлеченность в цифровую среду, так и возможности для реализации преступных схем с использованием информационных технологий.

На состояние преступности оказывают влияние также социокультурные особенности и высокая степень семейной и общинной сплоченности, характерная для республик Северного Кавказа. В таких условиях преступления, особенно в отношении местных жителей, зачастую регулируются внеформальными механизмами социальной регуляции, что, безусловно, сказывается на показателях регистрируемой преступности.

О повышенной степени общественной опасности киберпреступлений свидетельствует широкое использование информационно-телекоммуникационных технологий в деятельности организованных групп, преступных сообществ (преступных организаций), что позволяет говорить о ее наукоемкости. По итогам 2024 г. только число преступлений в сфере компьютерной информации, совершенных организованными группами или преступными сообществами (преступными организациями), увеличилось в 9,5 раза, прирост составил +853,8 %.

Все чаще достижения научно-технического прогресса применяются при совершении преступлений экономической направленности, преступлений террористического характера, в сфере незаконного оборота наркотиков.

Глобализация информационных процессов обусловила появление новых форм терроризма и экстремизма — кибертерроризма и киберэкстремизма.

Отметим, что данные официальной статистики не отражают реальное состояние киберпреступлений, поскольку исследуемый вид преступности продолжает оставаться высоколатентным. По мнению экспертов, этот показатель составляет от 60 до 90 % и даже более[4].

Думается, что латентизация киберпреступлений обусловлена анонимностью интернет-пользователей, т.е. возможностью создавать скрытые ресурсы на псевдодоменах, транснациональным характером, скоротечностью, отсутствием материальных следов и другими обстоятельствами. В результате латентности и низкой раскрываемости (в 2024 г. было раскрыто 23,2 % киберпреступлений, в 2023 г. — 26,6 %) невозможно говорить о надлежащей реализации принципа неотвратимой ответственности и эффективной деятельности по предупреждению этого вида преступлений.

В криминологической науке традиционно низкую раскрываемость связывают с латентным характером киберпреступлений. Справедливости ради необходимо отметить, что на уровне ряда регионов раскрываемость киберпреступлений выше общероссийского показателя. В частности, в Республике Дагестан раскрываемость в 2024 г. составляла 48,6 %, в Свердловской области — 37,6 %, в Республике Ингушетия — 36,8 %, в Чеченской Республике — 34,0 %, в Рязанской области — 32,9 %, в Тамбовской области — 32,3 %, в Брянской области — 32,2 %, в Кемеровской области — Кузбассе — 31,7 %, в Московской области — 31,3 %, в Кабардино-Балкарской Республике — 31,1 %.

Соответственно, в указанных субъектах РФ в большинстве случаев растет количество лиц, выявленных за совершение киберпреступлений, и отмечается увеличение уровня (коэффициента) исследуемого вида преступности.

Например, в 2024 г. по сравнению с 2023 г. на территории Республики Дагестан раскрываемость киберпреступлений повысилась на 0,3 %, уровень (коэффициент) — на 23,2, темпы прироста количества лиц, выявленных за совершение киберпреступлений, увеличились на 46,2 %. Высокая раскрываемость обусловила рост последних двух показателей в Московской области, соответственно, на 33,7 и 4,2 %, в Чеченской Республике — на 16,0 и 123,3 %.

Самое низкое значение раскрываемости киберпреступлений зарегистрировано в Ненецком автономном округе — 9,6 %.

---

[4] См., например: Латентность киберпреступности превысила 60 % — Сидоренко // РАПСИ — Российское агентство правовой и судебной информации. URL: https://rapsinews.ru/digital_law_news/20240424/309839280.html (дата обращения: 29.03.2025) ; *Линников А. С.* Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. 2017. № 5. С. 19—29 ; *Бойко О. А., Унукович А. С.* Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридический вестник Самарского университета. 2020. Т. 6. № 3. С. 53—59 ; *Ki Hong (Steve) Chon*. Cybercrime Precursors: Towards a Model of Offender Resources // The Australian National University Journal. 2018. № 1. P. 66—81.

В качестве сравнения обозначим, что раскрываемость преступлений экономической направленности зафиксирована на отметке 80,9 %, экстремистской направленности — 92,7 %, коррупционной направленности — 97,2 %.

Результаты проведенного исследования позволяют констатировать, что в целях обеспечения региональной безопасности осуществляется реализация комплекса следующих мер. В соответствии с поручением Президента России В. В. Путина ФСБ России и МВД России были разработаны дополнительные меры по блокировке телефонных вызовов, осуществляемых с территорий Украины и других недружественных иностранных государств в преступных целях, а также иные необходимые меры по защите прав и законных интересов граждан Российской Федерации от преступных посягательств, совершаемых с использованием современных информационно-коммуникационных технологий[5]. В результате значительно сократилось количество мошеннических звонков россиянам[6].

Распоряжением Правительства РФ от 30.12.2024 № 4154-р была утверждена Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий. Настоящий документ определяет принципы, цели, задачи и функции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение ее создания и функционирования.

Особый акцент сделан на создании государственной системы противодействия киберпреступлениям, на взаимодействии федеральных государственных органов и органов государственной власти субъектов РФ, Центрального банка РФ, финансовых и иных организаций в сфере противодействия киберпреступности, на прогнозировании и выявлении противоправных деяний, совершенствовании инструментов и механизмов противодействия киберпреступлениям, развитии цифровой грамотности населения, правосознания граждан, на укреплении международного сотрудничества и др.

К сожалению, указанная Концепция не имеет нормативного характера, поскольку в соответствии со ст. 5 Федерального конституционного закона от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» «акты Правительства Российской Федерации, имеющие нормативный характер, издаются в форме постановлений Правительства Российской Федерации. Акты по оперативным и другим текущим вопросам, не имеющие нормативного характера, издаются в форме распоряжений Правительства Российской Федерации».

Особое внимание уделяется укреплению кадрового потенциала подразделений, осуществляющих противодействие киберпреступности, их обучению и переподготовке, которые проводятся на базе Краснодарского университета МВД

[5] Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 14.01.2024 № Пр-64) // URL: http://www.kremlin.ru/acts/assignments/orders/73277 (дата обращения: 10.03.2025).

[6] Сбер: число звонков мошенников россиянам удалось уменьшить до 6—7 млн в сутки // URL: https://tass.ru/ekonomika/21775745 (дата обращения: 10.03.2025).

России (создан профильный факультет) и Московского университета МВД России имени В. Я. Кикотя (создана профильная кафедра).

Учитывая современные тенденции киберпреступности, можно констатировать, что, несмотря на принимаемые превентивные меры, повышение эффективности деятельности органов внутренних дел в рассматриваемой сфере, говорить о полной результативности и достаточности пока не приходится.

Проведенное исследование позволяет заключить, что киберпреступность в Российской Федерации в период с 2019 по 2024 г. демонстрирует устойчивую тенденцию к росту при низких значениях выявляемости виновных лиц и раскрываемости преступности. При этом киберпреступность охватывает все федеральные округа, проявляясь с разной степенью интенсивности на уровне субъектов РФ. Установлена выраженная территориальная дифференциация уровня киберпреступности, обусловленная совокупным влиянием демографических, социокультурных, организационных и технологических факторов.

Характерной особенностью современного этапа является не только количественный рост зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, но и повышение их качественной сложности, наукоемкости и степени общественной опасности. Это проявляется в усилении участия организованных преступных сообществ, возрастании финансовых последствий киберпосягательств и появлении новых форм угроз, таких как кибертерроризм и киберэкстремизм.

Особую озабоченность вызывает высокая латентность и низкий уровень раскрываемости киберпреступлений (менее 25 %), что указывает на сохраняющуюся неэффективность существующих механизмов уголовно-правового реагирования и превентивной деятельности. Вместе с тем зафиксированы отдельные позитивные сдвиги, выражающиеся в разработке государственной концепции противодействия преступлениям в ИКТ-среде, росте кадрового обеспечения и развитии цифровой грамотности населения.

Однако, учитывая отсутствие нормативного характера утвержденных стратегических документов и сохраняющиеся пробелы в межведомственном взаимодействии, можно заключить, что предпринимаемые меры по предупреждению киберпреступности на текущем этапе являются недостаточно эффективными, что требует комплексной корректировки подходов как на федеральном, так и региональном уровне.

БИБЛИОГРАФИЯ

1. *Бойко О. А., Унукович А. С.* Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридический вестник Самарского университета. — 2020. — Т. 6. — № 3. — С. 53—59.
2. Доклад руководителя МВД Коми за 2024 год // URL: https://uhta.bezformata.com/listnews/komi-za-2024-god/144219358/ (дата обращения: 29.03.2025).

3. Латентность киберпреступности превысила 60 % — Сидоренко // РАПСИ — Российское агентство правовой и судебной информации. URL: https://rapsinews.ru/digital_law_news/20240424/309839280.html (дата обращения: 29.03.2025).
4. *Линников А. С.* Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. — 2017. — № 5. — С. 19—29.
5. Сбер: число звонков мошенников россиянам удалось уменьшить до 6—7 млн в сутки // URL: https://tass.ru/ekonomika/21775745 (дата обращения: 10.03.2025).
6. *Ki Hong (Steve) Chon.* Cybercrime Precursors: Towards a Model of Offender Resources // The Australian National University Journal. — 2018. — № 1. — P. 66—81.