Научная статья
УДК 34
https://doi.org/10.24412/2073-0454-2025-6-178-182
EDN: https://elibrary.ru/racvex
NIION: 2003-0059-6/25-428
MOSURED: 77/27-003-2025-06-627

Корреляционный анализ преступности в киберпространстве

Армен Жораевич Саркисян
Московская академия Следственного комитета имени А.Я. Сухарева, Москва, Россия

Аннотация. Исследуются факторы, влияющие на состояние и развитие общества и существующих в нем систем и институтов, связанных с предупреждением киберпреступлений. Сделаны основные выводы относительно содержания, возможностей и направлений использования метода корреляционного анализа преступности в киберпространстве.

Ключевые слова: корреляционный анализ, киберпространство, факторный анализ, латентность, информационно-коммуникационные технологии

Для цитирования: Саркисян А. Ж. Корреляционный анализ преступности в киберпространстве // Вестник Московского университета МВД России. 2025. № 6. С. 178–182. https://doi.org/10.24412/2073-0454-2025-6-178-182. EDN: RACVEX.

Original article

Correlation analysis of crime in cyberspace

Armen Zh. Sarkisian
Moscow Academy of the Investigative Committee named after A.Ya. Sukharev, Moscow, Russia

Abstract. The factors influencing the state and development of society and its existing systems and institutions related to the prevention of cybercrime are studied. The main conclusions regarding the content, possibilities and directions of using the method of correlation analysis of crime in cyberspace are highlighted.

Keywords: correlation analysis, cyberspace, factor analysis, latency, information and communication technologies

For citation: Sarkisian A. Zh. Correlation analysis of crime in cyberspace. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2025;(6):178–182. (In Russ.). https://doi.org/10.24412/2073-0454-2025-6-178-182. EDN: RACVEX.

Выявление и изучение связей, закономерностей, тенденций, присущих преступности в киберпространстве, осуществляются посредством применения комплекса различных исследовательских методов, среди которых выделяется корреляционный анализ, представляющий собой распространенный метод аналитической статистики, позволяющий установить наличие и силу взаимосвязи между двумя или более переменными (случайными величинами, показателями), выяснить, как изменения одного показателя влияют на другой показатель [1, с. 71]. Содержание корреляционного анализа составляет определение связи результатов наблюдений с изучаемыми факторами, что выступает основой для оценки того, насколько существенно влияют данные факторы на результаты наблюдений, при этом для характеристики выявленной статистической зависимости между случайными переменными используется коэффициент корреляции, по величине которого судят о степени указанной зависимости [2, с. 29].

Данный метод активно используется в различных областях научного знания, в том числе не связанных с изучением социальных явлений, например, в медицине, при этом отмечается, что наибольшие сложности у исследователей, прибегающих к проведению корреляционного, факторного анализа, возникают именно в тех случаях, когда данный анализ применяется для изучения процессов и явлений, происходящих в обществе, поскольку социальные системы являются сложными, адаптивными и нестабильными, при этом присущее им множество наслаивающихся друг на друга факторов приводит к их взаимодействию, синергии, усиливающей их кумулятивный эффект [3].

Следовательно, в рамках изучения киберпреступности как сложного социально-правового явления важно учитывать специфику как минимум основных факторов, влияющих на состояние и развитие общества и существующих в нем систем и институтов, в том числе связанных с предупреждением данного криминалитета, а также то, что целостное и относительно полное представление о последнем можно сформировать только при использовании комплекса научных методов, позволяющих постичь не только количественные, но и качественные изменения в исследуемом объекте. При этом необходимо исключать выстраивание искусственных связей между случайными переменными, непосредственно не влияющими друг на друга, а также учитывать, что факторы как внешние по отношению к человеку обстоятельства, лежащие в основе корреляционного анализа, воздействуют на уровень преступности именно опосредованно — через создаваемые ими причины, в большей степени связанные с психологическими особенностями людей [4, с. 72].

Кроме того, при осуществлении корреляционного анализа преступности в киберпространстве необходимо принимать во внимание ее особенности, в том числе высокий уровень латентности, включение в ее объем практически всех видов преступлений, при совершении которых используются информационно-коммуникационные технологии, а также публичный, транснациональный и организованный характер значительной части таких уголовно наказуемых деяний. В связи с этим такой анализ, относящийся ко всей преступности в киберпространстве, преимущественно связан с оперированием примерными числами и пропорциональными значениями, которые вместе с тем позволяют составить общее представление о закономерностях и тенденциях, присущих этому криминалитету в целом, и его отдельным проявлениям в частности.

Для полного установления и исследования закономерностей и тенденций, присущих развитию преступности в киберпространстве, необходимо сформировать систему переменных, изменения которых во взаимосвязи друг с другом будут указывать на наличие определенных особенностей актуального состояния и генезиса этого негативного социально-правового явления.

В частности, в отдельную, основную группу взаимосвязанных переменных полагаем целесообразным включить факторы, способствующие определенным трансформациям структуры криминалитета, например, перемещению все большего числа различных видов уголовно наказуемых деяний в компьютерную, цифровую среду. Данные направления и тенденцию развития преступности, как правило, обозначают как ее цифровизацию, происходящую во взаимосвязи с цифровизацией многих видов общественных отношений и легальных сфер деятельности, в том числе банковской, предпринимательской или иной экономической деятельности [5; 6; 7].

Цифровизацию как таковую преимущественно рассматривают в контексте позитивных, прогрессивных изменений, происходящих в различных областях социальных отношений, вместе с тем одновременно обозначают и те риски, которые таят в себе такие изменения, включая появление новых либо качественную и (или) количественную трансформацию «традиционных» видов уголовно наказуемых деяний, образующих современное явление преступности в киберпространстве.

В Доктрине информационной безопасности РФ, в частности, указано, что расширение областей, в которых применяются информационные технологии, хотя и способствует генезису экономики и повышению эффективности функционирования институтов общества и государства, тем не менее, одновременно приводит к появлению новых информационных угроз, в том числе способных подорвать международную безопасность и стратегическую стабильность. Поэтому внедрение информационных технологий вне связи с обеспечением безопасности их использования и защищенности информационных ресурсов еще более повышает вероятность возникновения таких угроз и увеличения масштабов их потенциальных негативных последствий [8].

В Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, также обращается внимание на цифровизацию практически всех сфер жизни общества и государства, в том числе существующих систем и институтов управления ими, а также отмечается важный аспект, касающийся широкого распространения и доступности мобильных устройств, беспроводных технологий и сетей связи. Одновременно указывается, что в 2024 г. число пользователей российского сегмента «Интернета» превысило 130 млн человек, что составило примерно 90 % всего населения государства, при этом социальными сетями активно пользовались 106 млн человек (свыше 81 % от всех пользователей сети «Интернет» в России). Следовательно, указанные сети и технологии стали элементами повседневной жизни для подавляющего числа российских граждан, которые привыкли пользоваться различными электронными возможностями и сервисами, в том числе, связанными с оказанием государственных и муниципальных услуг. Вместе с тем формирование информационного общества с неизбежностью связано с тем, что те же сети и технологии активно используются лицами, замышляющими, подготавливающими и совершающими различного рода преступления в киберпространстве [9].

С учетом изложенного можно выделить первую

закономерность преступности в киберпространстве, заключающуюся в ее развитии, идущем параллельным или даже опережающим курсом с цифровизацией общественных отношений и непрерывным развитием и совершенствованием информационно-коммуникационных технологий, часть которых разрабатывается и используется специально для повышения эффективности противодействия различным преступлениям, совершаемым в киберпространстве.

М. Г. Решняк обращает внимание на трансформирующий эффект цифровизации, проявляющийся в последние годы в изменении не только общественных отношений, охраняемых уголовным законом, а также способов, средств, обстановки совершения преступных деяний, но еще и во внесении дополнений в законодательство в целях создания эффективных правовых средств противодействия новым формам преступности, прежде всего, существующей в киберпространстве [7, с. 55–56].

В частности, имеется корреляционная связь между миграционными процессами и совершаемыми в их рамках нарушениями, с одной стороны, и увеличением количества видов киберпреступлений и фактов их совершения, равно как и числа участвующих в них лиц, с другой стороны, в том числе в рамках криминальной деятельности по организации незаконной миграции. Эта связь с течением времени приобрела настолько очевидный характер, что нашла свое отражение в уголовном законе в виде дополнения ч. 2 ст. 322.1 УК РФ пунктом «д», содержащим новый для состава организации незаконной миграции квалифицирующий признак, заключающийся в использовании информационно-телекоммуникационных сетей, включая сеть «Интернет» [10].

Кроме того, в п. 18 Концепции государственной миграционной политики РФ на 2026–2030 гг. указано, в частности, что для профилактики, предупреждения, выявления и пресечения нарушений миграционного законодательства следует использовать современные цифровых технологии и информационно-технические средства; в подп. «б» п. 27 данной Концепции к задачам миграционной политики отнесено «развитие цифровой среды государственного управления и внедрение современных информационных технологий для обеспечения контроля в сфере миграции»; в подп. «а» п. 28 в качестве одного из основных направлений реализации миграционной политики названо «расширение практики использования цифровых технологий», в том числе искусственного интеллекта, позволяющего эффективно анализировать большие массивы данных; в подп. «а» п. 32 в рамках определения основных составляющих информационно-аналитического обеспечения реализации данной политики закреплено расширение использования актуальных цифровых технологий, в том числе обеспечивающих генезис межведомственных систем мониторинга и оценки миграционной ситуации, контроля за выполнением и результатами мероприятий по координации деятельности различных органов власти [11].

Расширение «цифрового компонента» уголовного и иного законодательства, а также документов стратегического планирования также можно назвать их цифровизацией, являющейся, на наш взгляд, фактором, способным ослабить корреляционные связи между рассмотренными и другими факторами и преступностью в киберпространстве.

При анкетировании 262 практических сотрудников органов внутренних дел, в том числе 145 сотрудников оперативных и 117 сотрудников следственных подразделений, задавался вопрос относительно факторов, способствующих росту или снижению числа фактически совершенных и регистрируемых киберпреступлений значительная часть респондентов (77 сотрудников — 29,39 %) в своих ответах обратила внимание на прогрессирующий кадровый дефицит, являющийся фактором, обусловливающим снижение числа регистрируемых киберпреступлений, и одновременно фактором, способствующим росту фактически совершенных уголовно наказуемых деяний данной группы. Т. е. нехватка личного состава в ключевых подразделениях ОВД и постепенное ухудшение данной ситуации прямо коррелирует с ростом фактически совершаемых киберпреступлений и находится в обратной корреляции в случае регистрируемой части преступности в киберпространстве.

Приведенная выше особенность присуща состоянию так называемых выявляемых преступлений, количество которых, попадающее в ведомственные учеты и в официальную статистику, зависит от усилий правоохранительных органов, в том числе от количества занятых в противодействии данной части криминалитета сотрудников, интенсивности, профессионализма и интенсивности их служебной деятельности, направленной на выявление и раскрытие этих преступлений. Принимая во внимание рассмотренные особенности киберпреступлений, эффективное противодействия таковым предполагает наличие у данных сотрудников дополнительных компетенций, в связи с чем простое замещение соответствующих вакантных должностей не представляется возможным. Для этого нужно время, достаточное для подготовки и (или) повышения квалификации сотрудников, при этом негативные тенденции с кадровым обеспечением органов внутренних дел только нарастают.

Так, по данным Министра внутренних дел РФ, озвученным им в марте 2025 г., в 39 из 96 территориальных органов имеет место нехватка свыше 20 % сотрудников, причем в отдельных подразделениях некоторых субъектов РФ кадровый дефицит составляет 40 % и количество вакантных мест продолжает увеличиваться. Только за 1 год из ОВД уволилось более 33 тысяч сотрудников, вследствие чего число вакантных должностей выросло до 172 тысяч [12].

Если же обратиться к статистике ГИАЦ МВД России, то можно увидеть подтверждение мнения респондентов, увидевших корреляционную связь между сокращением числа сотрудников органов внутренних дел и уменьшением количества зарегистрированных преступлений, совершаемых в гиперпространстве. Так, за январь-сентябрь 2025 г. количество преступлений, совершенных с использованием информационно-коммуникационных технологий, уменьшилось на 7,4 % по сравнению с аналогичным периодом 2024 г. В частности, количество так называемых дистанционных краж стало ниже на 19,2 %, число «дистанционных мошенничеств» — на 5,1 %, а преступлений, совершаемых в сфере компьютерной информации — на 37,5 % [13].

Вместе с тем, полагаем, что практически любой опрос репрезентативной группы граждан покажет разительно отличающиеся представления населения о фактических состоянии и динамике киберпреступлений и преступности, совершаемой в киберпространстве, в целом. Отметим также, что привести математически подтвержденную корреляционную связь рассматриваемых переменных весьма затруднительно, поскольку сведения о количестве фактически совершенных киберпреступлений могут иметь лишь приблизительный характер. Поэтому выделение данной корреляционной связи базируется на анализе и сопоставлении официальных статистических данных и результатов собственных социологических исследований.

Таким образом, выделим основные выводы относительно содержания, возможностей и направлений использования метода корреляционного анализа преступности в киберпространстве.

1. Использование метода корреляционного анализа при исследовании преступности в киберпространстве направлено на выявление связей между изменениями определенных факторов и трансформациями, наблюдаемыми в структуре и динамике такого криминалитета в целом, и входящих в него отдельных групп и видов киберпреступлений.

2. Корреляционный анализ преступности в киберпространстве затруднен вследствие ее особенностей и тенденций, в том числе высокого уровня латентности, включения в ее потенциальный объем практически всех видов уголовно наказуемых деяний, при совершении которых используются информационно-коммуникационные технологии или затрагивается компьютерная информация, а также влияния на состояние, структуру и динамику киберпреступности множества различных факторов, в том числе нейтрализующих или существенно ослабляющих детерминирующее воздействие определенных обстоятельств.

Список источников

1. Баврина А. П., Борисов И. Б. Современные правила применения корреляционного анализа // Медицинский альманах. 2021. № 3.
2. Козырев М. С., Масликов В. А. Применение корреляционного анализа при исследовании некоторых видов преступлений, совершаемых в Москве // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 1.
3. Честнов И. Л. Проблемы и перспективы юридического прогнозирования // Российская юстиция. 2024. № 12. С. 36–37.
4. Федотов А. А. Систематизация и корреляционный анализ факторов, воздействующих на уровень преступности // Народонаселение. 2024. Т. 27. № 1.
5. Иванов И. И., Кондрат И. Н. Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий // Мировой судья. 2024. № 12. С. 2–9.
6. Капинус О. А. Цифровизация преступности и уголовное право // Baikal Research Journal. 2022. Т. 13. № 1.
7. Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.
8. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.
9. Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий (утв. Распоряжением Правительства РФ от 30 декабря 2024 г. № 4154-р) // Собрание законодательства Российской Федерации. 2025. № 2. Ст. 76.
10. Федеральный закон от 9 ноября 2024 г. № 383-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации» // Собрание законодательства Российской Федерации. 2024. № 46. Ст. 6911.
11. Указ Президента Российской Федерации от 15 октября 2025 г. № 738 «О Концепции государственной миграционной политики Российской Федерации на 2026–2030 годы» // Собрание законодательства Российской Федерации. 2025. № 42. Ст. 6143.
12. Кадровый вопрос актуален : как работает полиция в условиях некомплекта личного состава // URL: https://fedpress.ru/article/3407981

13. Краткая характеристика состояния преступности в Российской Федерации за январь-сентябрь 2025 г. // URL: https://мвд.рф/reports/item/72174303/

References

1. Bavrina A. P., Borisov I. B. Modern rules of application of correlation analysis // Medical almanac. 2021. № 3.
2. Kozyrev M. S., Maslikov V. A. The use of correlation analysis in the study of certain types of crimes committed in Moscow // Criminological Journal of the Baikal State University of Economics and Law. 2016. Vol. 10. № 1.
3. Chestnov I. L. Problems and prospects of legal forecasting // Russian justice. 2024. № 12. P. 36–37.
4. Fedotov A. A. Systematization and correlation analysis of factors influencing the crime rate // Population. 2024. Vol. 27. № 1.
5. Ivanov I. I., Kondrat I. N. Features of the prevention of crimes committed using modern information and telecommunication technologies // Justice of the Peace. 2024. № 12. P. 2–9.
6. Kapinus O. A. Digitalization of crime and criminal law // Baikal Research Journal. 2022. Vol. 13. № 1.
7. Reshnyak M. G. Modern problems of the criminal legislation of Russia and certain foreign countries related to the digitalization of criminal activity // Business security. 2020. № 6. P. 54–61.
8. Decree of the President of the Russian Federation dated December 5, 2016 № 646 «On Approval of the Information Security Doctrine of the Russian Federation» // Collection of Legislation of the Russian Federation. 2016. № 50. Art. 7074.
9. The concept of the state system for countering illegal acts committed using information and communication technologies (approved by Decree of the Government of the Russian Federation dated December 30, 2024 № 4154-r) // Collection of Legislation of the Russian Federation. 2025. № 2. Art. 76.
10. Federal Law № 383-FZ of November 9, 2024 «On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation» // Collection of Legislation of the Russian Federation. 2024. № 46. Art. 6911.
11. Decree of the President of the Russian Federation № 738 dated October 15, 2025 «On the Concept of the State Migration Policy of the Russian Federation for 2026–2030» // Collection of Legislation of the Russian Federation. 2025. № 42. Art. 6143.
12. The personnel issue is relevant : how the police work in conditions of shortage of personnel // URL: https://fedpress.ru/article/3407981
13. Brief description of the state of crime in the Russian Federation in January–September 2025 // URL: https://мвд.рф/reports/item/72174303/

Информация об авторе

А. Ж. Саркисян — декан факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

Information about the author

A. Zh. Sarkisian — Dean of the Faculty of Advanced Training of the Moscow Academy of the Investigative Committee named after A.Ya. Sukharev, Candidate of Legal Sciences, Associate Professor.

Статья поступила в редакцию 20.11.2025; одобрена после рецензирования 01.12.2025; принята к публикации 12.12.2025.

The article was submitted 20.11.2025; approved after reviewing 01.12.2025; accepted for publication 12.12.2025.