УДК 343.2.7

ПРОГНОЗИРОВАНИЕ ТЕНДЕНЦИЙ КИБЕРПРЕСТУПНОСТИ С УЧЕТОМ ДЕМОГРАФИЧЕСКИХ И ЭКОНОМИЧЕСКИХ ДАННЫХ

Соколинский Юрий Валерьевич **—** студент РЭУ им. Г.В. Плеханова

Соколинская Мария Олеговна — студент НИУ ВШЭ

Лозовицкая Галина Петровна — д.ю.н., доцент, профессор кафедры государственно-правовых и уголовно-правовых дисциплин

РЭУ им. Г.В. Плеханова

Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский экономический университет имени Г.В. Плеханова»

Адрес: 115054, Москва, Стремянный переулок, д. 36

Телефон: +7 (495) 800-12-00

Электронная почта: yurysokolinskiy@yandex.ru**,** Naantonova2011@yandex.ru, Lozovitskaya.GP@rea.ru

Аннотация. В современном мире развитие информационных технологий сопровождается ускоренным ростом огромного числа кибератак, что требует эффективных мер по их предотвращению. В данной статье рассматривается взаимосвязь и соотношение между уровнем цифровизации стран и количеством киберпреступлений. Исследование также фокусируется на влиянии искусственного интеллекта на динамику киберпреступности. AI рассматривается как инструмент, который может как усиливать атаки, повышая их сложность и автоматизацию, так и обеспечивать защиту с помощью инновационных решений.

Исследование проведено с учетом основных положений и в рамках выполнения научно-исследовательской работы на тему «Совершенствование правового регулирования в области обеспечения социальной безопасности граждан», финансируемой из средств ФГБОУ ВО «РЭУ им. Г.В. Плеханова» (приказ № 1514 от 26.07.2024 г.).

Ключевые слова: уголовное право, киберпреступность, прогнозирование, экономико-демографические данные, искусственный интеллект (AI), цифровизация, тенденции.

FORECASTING CYBERCRIME TRENDS BASED ON DEMOGRAPHIC AND ECONOMIC DATA

In the modern world, the development of information technology is accompanied by an accelerated increase in the number of cyber attacks, which requires effective measures to prevent them. This article examines the relationship between the level of digitalization of countries and the number of cybercrimes. The study also focuses on the impact of artificial intelligence on the dynamics of cybercrime. AI is seen as a tool that can both enhance attacks, increasing their complexity and automation, and provide protection with innovative solutions.

The study was conducted taking into account the main provisions and within the framework of the research work on the topic "Improving legal regulation in the field of ensuring social security of citizens", financed from the funds of the Federal State Budgetary Educational Institution of Higher Education "PRUE named after G.V. Plekhanov" (order No. 1514 dated July 26, 2024).

Keywords: criminal law, cybercrime, forecasting, economic and demographic data, artificial intelligence (AI), digitalization.

Введение. С развитием цифровых технологий киберпреступность становится одной из самых актуальных угроз современного мира. С каждым годом растет количество кибератак, целью которых становятся как частные лица, так и крупные компании и государственные учреждения. Этот рост требует более глубокого понимания факторов, влияющих на преступную активность и разработку эффективных методов прогнозирования и противодействия угрозам [8].

Одним из ключевых аспектов изучения киберпреступности является анализ демографических и экономических данных. Экономическая ситуация,

уровень цифровизации, доступ к интернету, демографические характеристики населения и уровень образования — все эти факторы могут прямо или косвенно влиять на степень распространенности кибератак. Развивающиеся страны, где экономическая и технологическая инфраструктура еще только формируются, могут быть менее защищены от киберугроз, тогда как в странах с высокоразвитой экономикой и сильной IT-инфраструктурой наблюдается значительное количество целей для атак при высоком уровень защиты.

Кроме того, важную роль в тенденциях киберпреступности играет искусственный интеллект. AI стал мощным инструментом как для защиты от атак, так и для их совершения: преступники используют новые технологии для автоматизации и поиска уязвимостей в системах безопасности.

Кроме этого, AI (artificial intelligence) в ряде случаев в качестве расшифровки данной аббревиатуры подразумевает под собой не только искусственный интеллект/разум, но и способность компьютера имитировать человеческие действия либо навыки.

Авторский анализ исследований

Российские исследования. Правовое регулирование кибератак в России достаточно активно обсуждается в отечественной юридической и технологической литературе [1,2,3,4,5,6,7,8]. Вопросы кибербезопасности и законодательного контроля исследовались многими учеными, среди которых можно выделить:

Для исследования правового регулирования киберпреступлений в России можно обратиться к труду такого автора, как О.М. Сафонов, который в своей диссертации анализировал использование компьютерных технологий при совершении преступлений и предлагал пути совершенствования законодательства. В своих работах он также указывал на необходимость усиления уголовно-правовой оценки кибератак, поскольку текущее законодательство не всегда соответствует темпам развития технологий [1].

А.С. Черепашкин, анализирует уголовно-правовые и криминологические аспекты противодействия киберпреступности в России.

Он подчеркивает необходимость совершенствования законодательства, особенно в части расширения перечня киберпреступлений и более четкого их определения. Это включает кибератаки, фишинг, DDoS-атаки и другие современные виды преступлений, которые пока недостаточно охвачены в действующем законодательстве [2].

И.М. Полухтин, также акцентирует внимание на организационно-правовых аспектах кибербезопасности в России. В своих исследованиях он подчеркивает важность международного сотрудничества в борьбе с киберпреступностью, а также необходимость создания единых стандартов для защиты критической информационной инфраструктуры [6].

Международные исследования. На международной арене вопросы киберпреступности и правового регулирования кибератак рассматриваются в работах многих ученых, которые анализируют различные подходы к борьбе с киберпреступностью и сравнивают законодательные системы разных стран.

В качестве международных исследований по правовому регулированию киберпреступлений можно привести работы, представленные в "Palgrave Handbook of International Cybercrime and Cyberdeviance", где исследуются киберпреступления в глобальном контексте. Например, в работе Адама М. Босслера и Томаса Дж. Хольта проводится анализ законодательных механизмов США и других стран, таких как Великобритания и Индия, по борьбе с киберпреступностью [4]. В их исследованиях затрагиваются вопросы, связанные с правоприменением и международным сотрудничеством в области кибербезопасности.

Кроме того, работа "Global Approaches to Cyber Policy, Legislation and Regulation" от Пиа Хюша и Джеймса Салливана (RUSI) описывает подходы к разработке политик в области кибербезопасности в таких странах, как США, Канада, Япония и страны Европейского Союза [3]. Они акцентируют внимание на важности защиты критической национальной инфраструктуры и развитии международного сотрудничества в этой области.

В целом, научная литература подчеркивает, что правовое регулирование киберпреступлений находится на стадии постоянного развития, что требует от стран гибкости и готовности адаптировать свои законы в ответ на новые киберугрозы.

Обобщенный обзор литературы. Таким образом, исследования киберпреступности и правового регулирования в этой области в последние годы привлекают значительное внимание ученых и экспертов. На наш взгляд, в условиях стремительного развития информационных технологий и увеличения числа кибератак важнейшей задачей научных исследований становится создание эффективных юридических механизмов для их предотвращения и наказания. Для этого следует сделать авторский акцент и на результатах исследований.

Результаты исследований. На основе анализа правового регулирования киберпреступлений в России и стран G20, а также текущих тенденций в развитии IT-инфраструктуры, можно выделить несколько ключевых факторов, объясняющих высокие показатели киберпреступности в России и других странах. Эти факторы связаны с уровнем цифровизации, степенью уязвимости IT-систем, юридическими пробелами и трудностями в расследовании трансграничных кибератак. Такими факторами являются:

1. Развитая цифровая инфраструктура как цель для атак

Россия, благодаря своей развитой цифровой инфраструктуре, привлекает киберпреступников как внутри страны, так и за ее пределами. Основные технологические и финансовые центры страны, такие как Москва и Санкт-Петербург, являются ключевыми целями для кибератак. Рост числа пользователей интернета и широкое распространение цифровых технологий увеличивают количество уязвимых точек в сети, что делает системы более подверженными атакам, таким как взломы и распространение вредоносных программ. В развитых странах с высокой концентрацией IT-компаний и бизнес-структур кибератаки становятся более частыми и системными.

2. Недостаточный уровень кибербезопасности. Многие предприятия в России, включая малый и средний бизнес, а также государственные учреждения, уделяют недостаточно внимания защите своих информационных систем. Вследствие этого многие системы остаются уязвимыми для атак, таких как фишинг, внедрение вредоносного ПО и кража данных. Недостаток культуры кибербезопасности усугубляется низкой осведомленностью пользователей и сотрудников компаний, что позволяет преступникам легче проникать в корпоративные сети.

3. Юридические пробелы и несовершенство законодательства. Российское законодательство, несмотря на наличие статей УК РФ, таких как 272, 273, 274 и 274.2, охватывающих ответственность за киберпреступления, не всегда успевает адаптироваться к новым технологиям и методам атак. Быстрое развитие кибер - преступлений и правонарушений, таких как атаки на блокчейн, криптовалюты и искусственный интеллект, создает множественные пробелы в правовом регулировании. Например, такие кибератаки, как шифрование данных с целью вымогательства (рансомваре), недостаточно детализированы в российском законодательстве, что позволяет преступникам использовать новые формы преступлений без серьезного риска наказания.

4. Трудности в расследовании киберпреступлений. Расследование киберпреступлений требует специфических знаний и технических ресурсов, что создает дополнительные сложности для правоохранительных органов. Преступники часто используют прокси-серверы, шифрование и другие методы сокрытия своей активности, что затрудняет их обнаружение. Важно отметить, что международные киберпреступления, которые осуществляются через границы, создают значительные проблемы с юрисдикцией и международным сотрудничеством, что замедляет расследования и привлечение виновных к ответственности.

5. Экономическая и социальная мотивация преступников. Экономическая нестабильность и социальные трудности во всем мире также способствуют росту киберпреступности. Организованные преступные группы

активно вербуют новых участников и обучают их навыкам взлома и атак, используя интернет как платформу для незаконной деятельности. Широкий доступ к инструментам для взлома, вредоносным программам и базам данных в darknet создает благоприятные условия для вовлечения людей в киберпреступную деятельность.

6. Ограниченный охват новых видов преступлений. Законодательство РФ, как было нами показано, не полностью охватывает современные виды атак, к примеру такие, как атаки на IoT-устройства, криптовалюты и другие новые технологии. Социальная инженерия и фишинговые атаки также остаются на периферии уголовного регулирования, что позволяет преступникам использовать эти методы без страха перед наказанием. Это создает правовой вакуум, в котором злоумышленники могут действовать безнаказанно и пользуются этим.

Визуализация данных с помощью тепловой карты. Одним из результатов исследования является создание тепловой карты, отражающей динамику киберпреступлений, технологическую инфраструктуру и деятельность мониторинговых центров киберугроз в разных странах. Она показывает взаимосвязь между уровнем IT-развития, числом кибератак и ключевыми технологическими центрами. Таким образом, на тепловой карте представлены такие показатели, как:

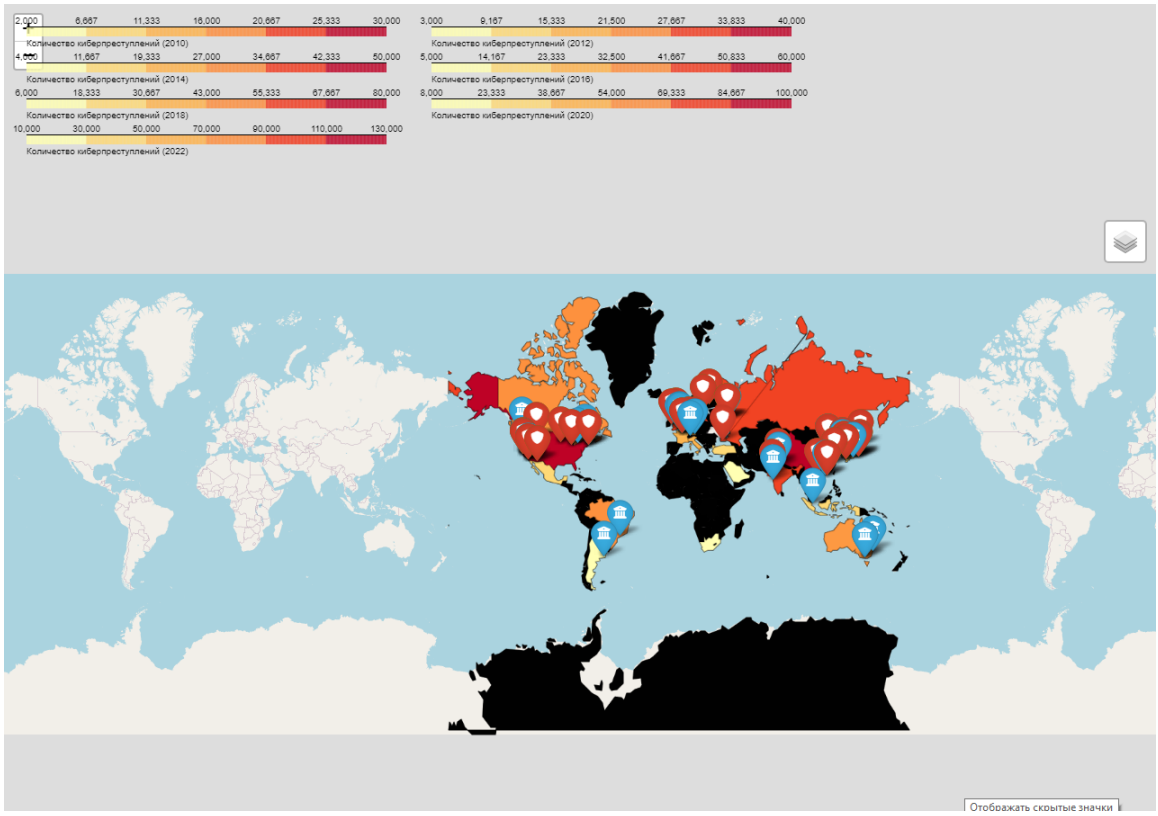
1. Состояние киберпреступности с 2010 по 2022 годы. Тепловая карта визуализирует рост числа кибератак в таких странах, как США, Китай и Россия. В США отмечен значительный рост киберпреступлений, что связано с развитием цифровых технологий и увеличением числа пользователей интернета. Китай и Россия также демонстрируют рост количества атак, что связано с развитием IT-инфраструктуры.

2. Ключевые технологические университеты. На карте, созданной в рамках данного исследования (см. Карту 1 на иллюстрации и по ссылке), представлены ведущие университеты, такие как MIT (США), Tsinghua (Китай)

и МФТИ (Россия), которые активно готовят специалистов в сфере кибербезопасности. Страны с развитой образовательной системой и сильными IT-компаниями более подвержены кибератакам, что связано с высокой концентрацией IT-специалистов.

3. Мониторинговые центры киберугроз. Центры мониторинга (см. Карту 1 на иллюстрации и по ссылке), такие как Google (США), Yandex (Россия) и Baidu (Китай), играют важную роль в защите критической инфраструктуры и противодействии кибератакам, предоставляя данные о киберугрозах в своих странах и за рубежом.

Карта 1.



Важность визуализации данных. Тепловая карта демонстрирует взаимосвязь между развитием цифровой инфраструктуры и количеством кибератак. Она помогает анализировать региональные различия в распространенности киберпреступлений и прогнозировать будущие угрозы. Ссылка на тепловую карту: https://sciencebysokol.ru/cyberheatmap.html

Выводы. Таким образом, правовое регулирование киберпреступлений в России требует модернизации и адаптации к текущим вызовам, связанным с развитием технологий и глобализацией. Учитывая растущее число кибератак и их сложность, необходимо усилить правоприменительную практику, активизировать международное сотрудничество и повысить уровень кибербезопасности среди бизнеса и граждан.

Одним из важных направлений решения обозначенных нами выводов может послужить прогностическая модель.

Прогностическая модель. Одним из инструментов для анализа и прогнозирования количества преступлений является регрессионное моделирование, которое позволяет выявить закономерности между множеством факторов и количеством киберпреступлений. В данном исследовании была построена полиномиальная регрессионная модель для прогнозирования количества преступлений в Российской Федерации на основе 19 предикторов, которые охватывают различные аспекты социально-экономической и демографической ситуации в стране:

1. Уровень цифровой грамотности
2. Доля молодежи (15-24 лет)
3. Доля пожилого населения (>65 лет)
4. Доля населения с высшим образованием
5. Доля населения с ИТ-специализацией
6. Доля городского населения
7. Доля сельского населения
8. Плотность населения (чел/км²)
9. Процентное соотношение мужчин к женщинам
10. Уровень безработицы
11. Доля населения, занятого в ИТ-сфере
12. Процент населения с доступом к интернету
13. ВВП на душу населения (в $)
14. Уровень инфляции

15. Доход на душу населения (в $)
16. Коэффициент Джини (неравенство доходов)
17. Процент населения за чертой бедности
18. Инвестиции в ИТ (в млрд $)
19. Расходы на кибербезопасность (в млрд $)

Данные за 2010–2022 года были собраны из разных источников, поэтому разработанная модель дает лишь приблизительное представление о динамике изменения преступлений, совершенных в информационном пространстве.

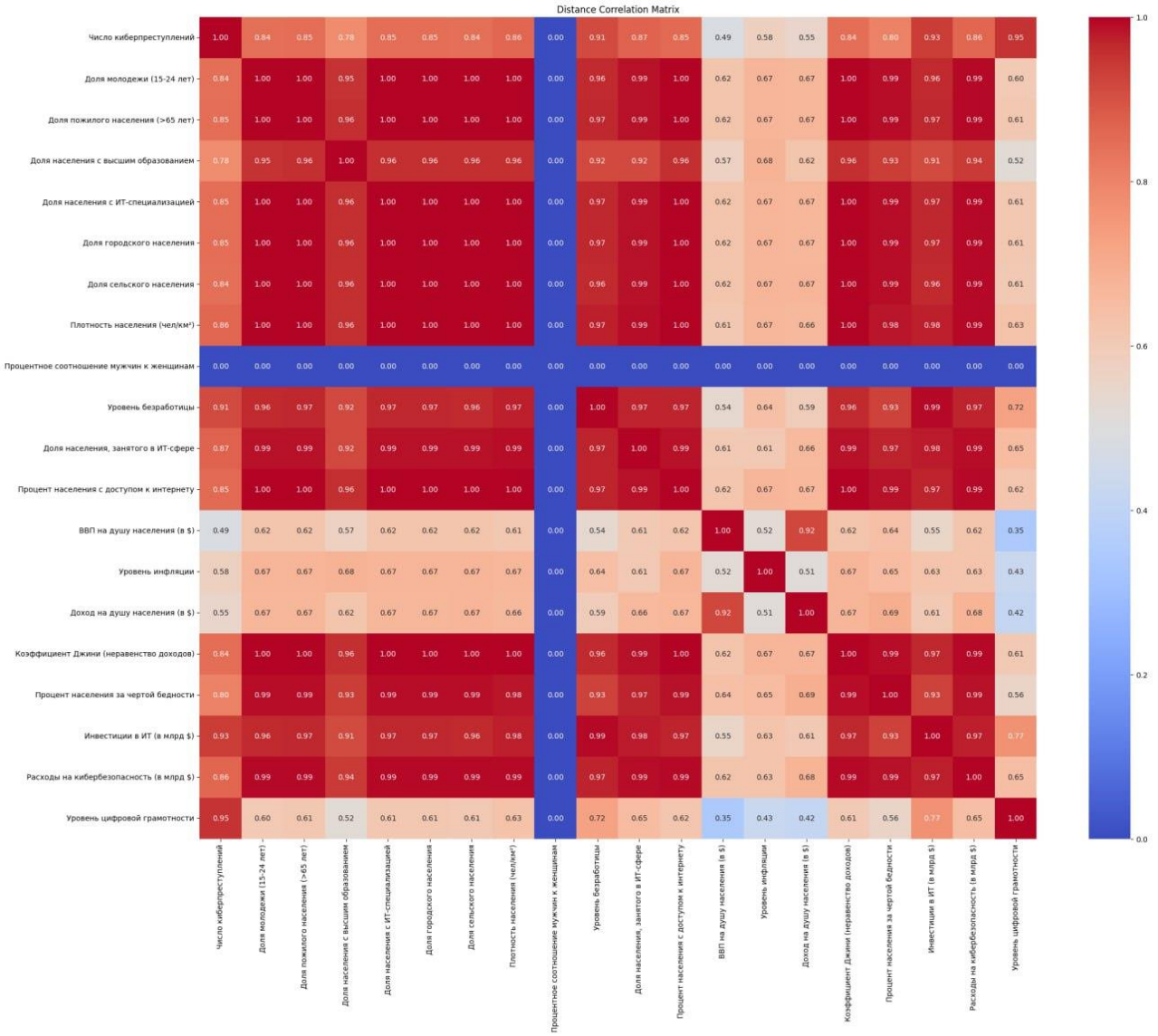
Перед построением модели машинного обучения был выполнен анализ распределения данных: применялся тест Шапиро -Уилка для проверки нормальности распределения данных. Результаты теста представлены в таблице 1.

Таблица 1. Результаты теста Шапиро-Уилка

	Statistic	**P-value**
Уровень цифровой грамотности	0,9656249911	0,8371814846
Число киберпреступлений	0,901960156	0,142274063
Доля молодежи (15-24 лет)	0,964939827	0,82748605
Доля пожилого населения (>65 лет)	0,965624991	0,837181485
Доля населения с высшим образованием	0,874539214	0,060178066
Доля населения с ИТ-специализацией	0,965624991	0,837181485
Доля городского населения	0,965624991	0,837181485
Доля сельского населения	0,965624991	0,837181485
Плотность населения (чел/км²)	0,965624991	0,837181485
Процентное соотношение мужчин к женщинам	1	1
Уровень безработицы	0,891587964	0,102548448
Доля населения, занятого в ИТ-сфере	0,971995001	0,916886074
Процент населения с доступом к интернету	0,965624991	0,837181485
ВВП на душу населения (в $)	0,88716608	0,089235264
Уровень инфляции	0,964751765	0,824795837
Доход на душу населения (в $)	0,967144977	0,858035547
Коэффициент Джини (неравенство доходов)	0,965624991	0,837181485

Процент населения за чертой бедности	0,965624991	0,837181485
Инвестиции в ИТ (в млрд $)	0,959557352	0,746814091
Расходы на кибербезопасность (в млрд $)	0,972085434	0,917851303

Результаты показали, что данные подчиняются нормальному распределению, что улучшает числовую устойчивость регрессионной модели. Далее был проведен авторский корреляционный анализ и построены диаграммы рассеяния для выявления вида зависимости между предикторами и зависимой переменной. В качестве корреляционной матрицы была выбрана матрица расстояний (Distance correlation), способная выявлять любые



зависимости между переменными, включая нелинейные. Итоговая корреляционная матрица представлена на рисунке 1.

Рисунок 1. Корреляционная матрица расстояний

На основе данной корреляционной матрицы были выбраны предикторы, которые наибольшим образом коррелируют с зависимой переменной (кол-во преступлений) и имеют наименьшую мультиколлинеарность между собой. Также была выявлена полиномиальная взаимосвязь второй степен между уровнем цифровой грамотности и кол-вом киберпреступлений, инвестициями в IT и кол-вом киберпреступлений, процентом населения за чертой бедности и кол-вом киберпреступлений, расходами на кибербезопасность и кол-вом киберпреступлений. Данные зависимости представлены на рисунках 2,3,4,5.

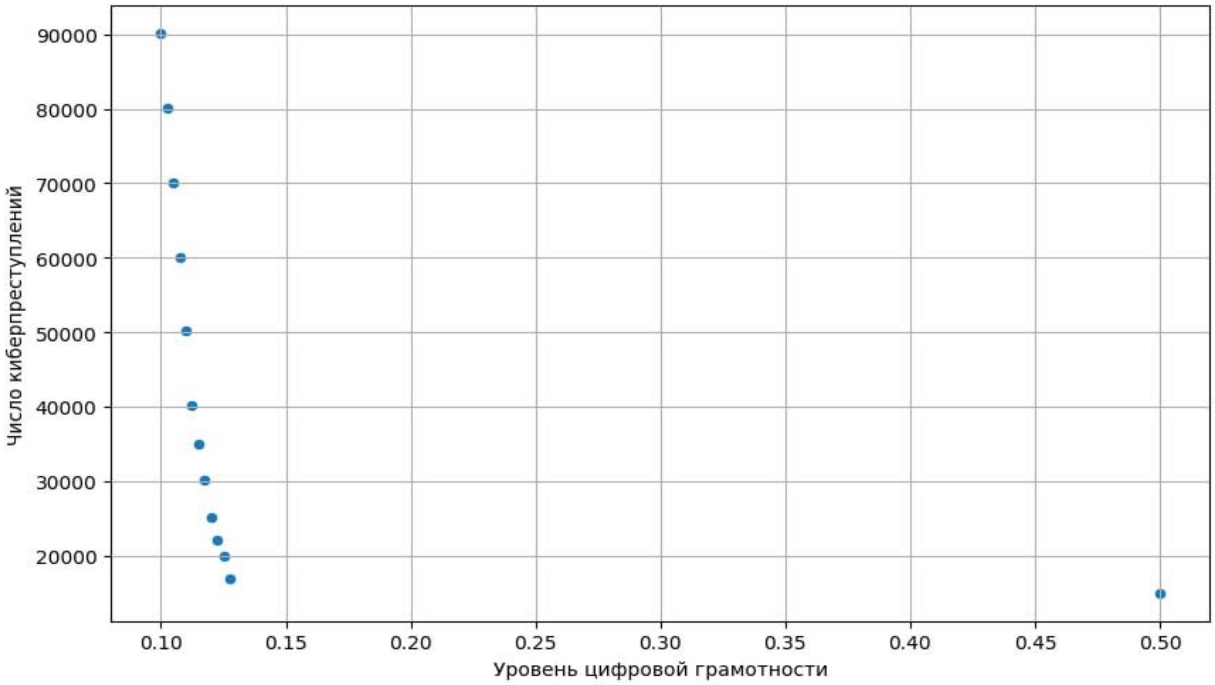


Рисунок 2. Диаграмма рассеяния: зависимость числа киберпреступлений от уровня цифровой грамотности

Диаграмма рассеяния показывает обратную квадратичную зависимость между уровнем цифровой грамотности и числом киберпреступлений.

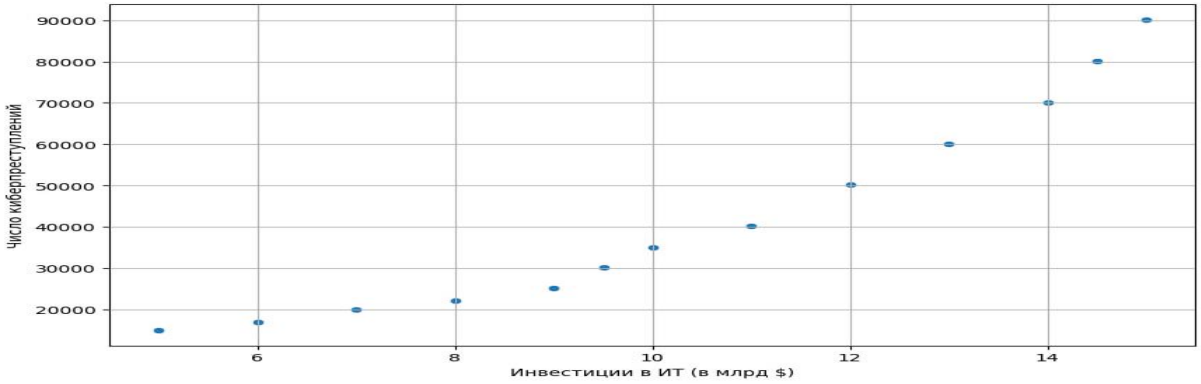


Рисунок 3. Диаграмма рассеяния: зависимость числа киберпреступлений от инвестиций в IT

На данной диаграмме рассеяния (рисунок 3) наблюдается положительная зависимость между инвестициями в IT (в млрд $) и числом киберпреступлений. В верхней части графика можно заметить небольшие отклонения от линейности, что может указывать на возможное наличие квадратичной зависимости.

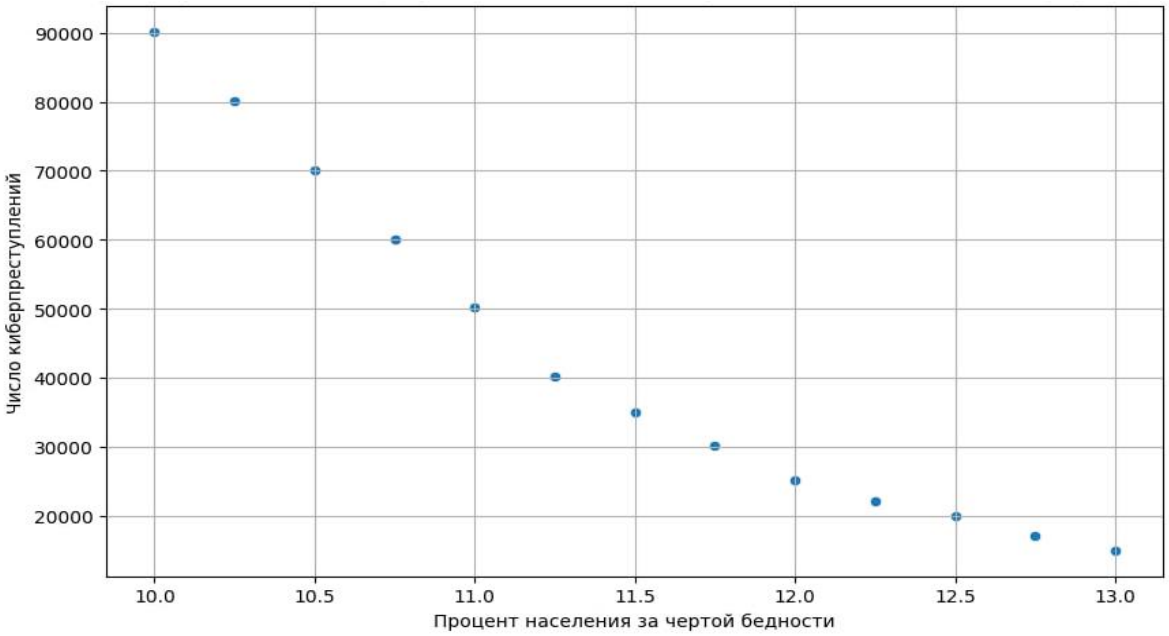


Рисунок 4. Диаграмма рассеяния: зависимость числа киберпреступлений от процента населения за чертой бедности

Диаграмма (рисунок 4) визуализирует обратную зависимость между процентом населения за чертой бедности и числом киберпреступлений. Зависимость выглядит нелинейной, с более резким снижением числа киберпреступлений при увеличении процента бедного населения в диапазоне от 10% до 12%.

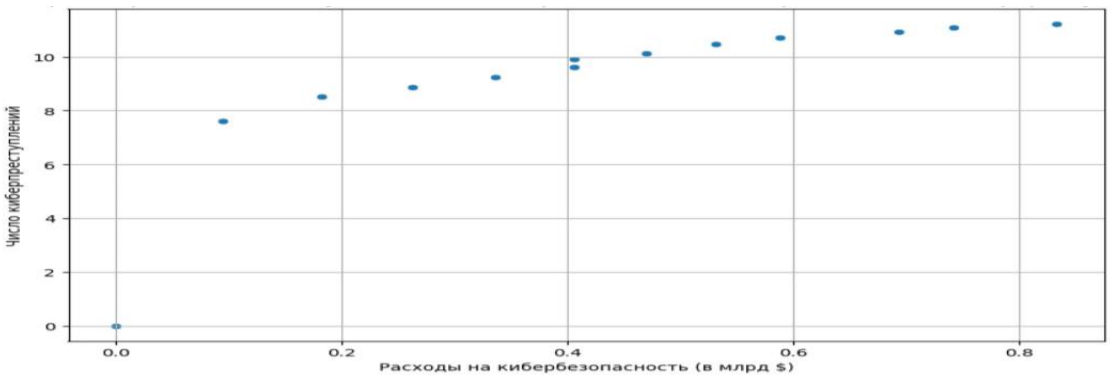


Рисунок 5. Диаграмма рассеяния: зависимость числа киберпреступлений от расходов на кибербезопасность

На представленной диаграмме (рисунок 5) наблюдается нелинейная зависимость между расходами на кибербезопасность и числом киберпреступлений. В начальной фазе, при низких значениях расходов, наблюдается положительная корреляция: увеличение инвестиций в кибербезопасность приводит к снижению числа киберпреступлений. Однако после достижения определённого порога (около 0.2 млрд $) наблюдается эффект насыщения, при котором дальнейший рост расходов на кибербезопасность не сопровождается значительным изменением в уровне киберпреступности.

Результатом построения прогностической модели стала полиномиальная регрессия второй степени, построенная методом наименьших модулей, где зависимой переменной является число киберпреступлений, а независимыми переменными — экономические, демографические и технологические факторы. В модели учтены как линейные, так и нелинейные зависимости (квадраты переменных). Результаты полиномиальной регрессии представлены на рисунке 6.

OLS Regression Results

Dep. Variable:	Число киберпреступлений	R-squared:	0.694
Model:	OLS	Adj. R-squared:	0.581
Method:	Least Squares	F-statistic:	411.8
Date:	Fri, 06 Sep 2024	Prob (F-statistic):	0.00242
Time:	22:33:18	Log-Likelihood:	-78.085
No. Observations:	10	AIC:	172.2
Df Residuals:	2	BIC:	174.6
Df Model:	7		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
const	-8585.5406	2.1704	-0.396	0.431	-1.0205	8.484
Процент населения за чертой бедности	-7.467e+04	1.7205	-0.435	0.506	-8.1405	6.655
Инвестиции в ИТ (в млрд $)	1.1715	2.2205	0.526	0.351	-8.405	1.076
Расходы на кибербезопасность (в млрд $)	-7272.1538	2.9704	-0.245	0.229	-1.3505	1.25
Уровень цифровой грамотности	-746.7406	1718.235	-0.435	0.506	-8139.711	6646.230
Процент населения за чертой бедности^2	5384.9293	1.204	0.449	0.498	-4.63e+04	5.774
Процент населения за чертой бедности Инвестиции в ИТ (в млрд $)	-7009.3367	1.1904	-0.588	0.616	-5.83e+04	4.42e+04
Процент населения за чертой бедности Расходы на кибербезопасность (в млрд $)	385.1176	9716.276	0.040	0.972	-4.1404	4.22e+04
Процент населения за чертой бедности Уровень цифровой грамотности	53.8493	120.056	0.449	0.598	-462.711	570.409
Инвестиции в ИТ (в млрд $)^2	-4436.8013	1.1404	-0.391	0.134	-5.3304	4.4404
Инвестиции в ИТ (в млрд $) Расходы на кибербезопасность (в млрд $)	5.004	1.3305	0.378	0.401	-5.2305	6.2405
Инвестиции в ИТ (в млрд $) Уровень цифровой грамотности	-70.0934	119.06	-0.588	0.616	-582.563	442.376
Расходы на кибербезопасность (в млрд $)^2	-2.333	6.005	-0.386	0.517	-2.83e+06	2.3706
Расходы на кибербезопасность (в млрд $) Уровень цифровой грамотности	3.8512	97.163	0.040	0.272	-414.206	421.909
Уровень цифровой грамотности^2	0.5385	1.201	0.449	0.198	-4.627	5.704

Omnibus:	4.018	Durbin-Watson:	1.674
Prob(Omnibus):	0.134	Jarque-Bera (JB):	1.346
Skew:	-0.869	Prob(JB):	0.510
Kurtosis:	3.457	Cond. No.	2.6418

Рисунок 6. Результаты полиномиальной регрессии

Оценка точности модели, **R-squared** = 0.694, означает, что модель объясняет около 69.4% изменчивости в зависимой переменной. Это достаточно хороший показатель для реальных данных.

Adjusted R-squared = 0.581 — это значение указывает на снижение объясняющей способности модели при добавлении новых переменных. Оно показывает, что некоторые переменные могут быть лишними или незначимыми для предсказания числа киберпреступлений. F-statistic = 411.8 и значимость модели (p-value = 0.0024) указывают на статистически значимую регрессию.

Модель содержит переменные, взаимодействующие друг с другом (например, "Процент населения за чертой бедности * Инвестиции в IT"), что позволяет учесть сложные взаимосвязи между факторами.

P-значения. Многие переменные имеют высокие P-значения (например, переменная "Процент населения за чертой бедности", P = 0.506), что говорит о том, что эти переменные не являются статистически значимыми для модели.

Переменные второго порядка (квадраты переменных и взаимодействие между ними): Эти взаимодействия и нелинейные эффекты (например, "Процент населения за чертой бедности^2" и "Инвестиции в ИТ (в млрд $)^2") также не показали статистической значимости.

Тест на нормальность. Значение Prob (Omnibus) = 0.131 и Skew = -0.869 показывают, что остатки модели приближены к нормальному распределению, что является положительным сигналом для адекватности модели.

Интерпретация ключевых коэффициентов. Процент населения за чертой бедности имеет отрицательное влияние на количество киберпреступлений, что может указывать на то, что бедные регионы могут быть менее цифровизированы и, следовательно, менее подвержены кибератакам. переменной с инвестициями в IT и кибербезопасность не является значимым (P-value > 0.05).

Инвестиции в IT показывают положительный коэффициент, но также не являются значимыми (P-value > 0.05), что может указывать на то, что просто увеличение инвестиций в технологии без эффективной политики безопасности не снижает количество кибератак.

Расходы на кибербезопасность имеют отрицательный коэффициент (-7274.135), что указывает на то, что увеличение этих расходов может сокращать количество киберпреступлений. Однако данный результат также не является статистически значимым (P-value > 0.05).

Уровень цифровой грамотности имеет положительный, но незначительный коэффициент, что может указывать на недостаточную подготовку или осведомленность населения в вопросах киберугроз, несмотря на рост цифровой грамотности.

Недостатки модели. Выборка данных за 12 лет (2010-2022) - довольно ограниченный временной промежуток для анализа долгосрочных тенденций в области киберпреступности, особенно учитывая быстрые изменения в технологиях и законодательстве.

Высокие P-значения для многих переменных указывают на отсутствие статистической значимости этих факторов, что говорит о том, что модель нуждается в улучшении и дополнительных.

Заключение. Ключевой вклад статьи заключается в создании тепловой карты, которая визуализирует взаимосвязь между уровнем цифровой инфраструктуры и количеством кибератак, а также в построении прогностической модели на основе полиномиальной регрессии. Тепловая карта выявляет региональные различия в распространенности киберпреступлений, а регрессионная модель демонстрирует влияние социально-экономических факторов на их количество. Статья подчеркивает важность совершенствования правовых механизмов для борьбы с киберпреступностью, особенно в странах с развитой IT-инфраструктурой.

Список литературы:

1. Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: автореф. дис. ... канд. юрид. наук: 12.00.08 / Сафонов Олег Михайлович; Российская правовая академия. [Электронный ресурс]. — Режим доступа: https://search.rsl.ru/ru/record/01005560281
2. Министерства юстиции Российской Федерации. – Москва, 2015. – 22 с.
3. Черепашкин А.С., Тансыкова А.Ш. Противодействие киберпреступности в России: уголовно-правовые и криминологические аспекты. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/protivodeystvie-kiberprestupnosti-v-rossii-ugolovno-pravovye-i-kriminologicheskie-aspekty
4. Hüsch P., Sullivan J. Global Approaches to Cyber Policy, Legislation and Regulation. [Электронный ресурс]. — Режим доступа: https://www.rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
5. Holt T.J., Bossler A.M. (eds). The Palgrave Handbook of International Cybercrime and Cyberdeviance. [Электронный ресурс]. — Режим доступа: https://link.springer.com/referencework/10.1007/978-3-319-78440-3
6. Полухтин И.М., Серебренникова А.В. Правовые основы кибербезопасности в Российской Федерации. [Электронный ресурс]. — Режим доступа: https://www.urvak.ru/articles/probe-5521-vypusk-4-pravovye-osnovy-kiberbezopasno/
7. Ковалев О.Г., Семенова Н.В. Кибербезопасность современной России: теоретические и организационно-правовые аспекты. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-sovremennoy-rossii-teoreticheskie-i-organizatsionno-pravovye-aspekty
8. Лозовицкая, Г. П. Использование искусственного интеллекта в расследовании киберпреступлений: возможности и риски / Г. П. Лозовицкая, М. М. Малькута, К. М. Родионова // Актуальные вопросы расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий в условиях цифровизации экономики и государственного управления : Материалы Межвузовского круглого стола, Москва, 23 ноября 2023 года. – Москва: Общество с ограниченной ответственностью "Русайнс", 2024. – С. 51-59. – EDN BTCRNQ. [Электронный ресурс]. — Режим доступа: https://elibrary.ru/item.asp?id=67906247