Научная статья

УДК 378.147

МЕТОДИКА И ТЕХНОЛОГИЯ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННЫХ МАТЕМАТИЧЕСКИХ ПАКЕТОВ

Алексей Дмитриевич Косолапов[1], Алексей Иванович Примакин[2],
[1–2] Академия войск национальной гвардии, Санкт-Петербург, Россия
[1] a.kosolapov@mail.ru
[2] a.primakin@mail.ru

Аннотация. Учитывая особую актуальность борьбы с информационным терроризмом, в статье сделан акцент на методике и технологии построения математических моделей в области информационного противоборства. В качестве математического инструментария построения соответствующих моделей с целью дальнейшего составления научно-обоснованного прогноза ситуации, предлагаются алгоритмы и процедуры многопараметрического статистического анализа, выполненные в среде специализированных математических программ, таких как Statistica и интегрированный математический пакет Mathcad.

Математическое описание ситуаций, противодействующих информационному терроризму, позволяет в дальнейшем рационально подойти к решению вопросов материально-технического обеспечения соответствующих подразделений войск Росгвардии для предотвращения и нейтрализации информационных угроз.

Ключевые слова: информационный терроризм, математические модели информационного противоборства, показатели уровня противодействия терроризму структурного подразделения Росгвардии, методы многофакторного статистического анализа

Для цитирования: Косолапов А.Д., Примакин А.И. Методика и технология построения математических моделей в области информационного противоборства с помощью специализированных математических пакетов // Вестник Военной академии войск национальной гвардии. 2025. № 2 (31). С. 255–266. URL: https://vestnik-spvi.ru/2025/06/027.pdf.

Original article

THE METHODOLOGY AND TECHNOLOGY OF CONSTRUCTING MATHEMATICAL MODELS IN THE FIELD OF INFORMATION WARFARE USING SPECIALIZED MATHEMATICAL PACKAGES

Alexey D. Kosolapov[1], Alexey I. Primakin[2]
[1–2] Academy of the National Guard Troops, Saint-Petersburg, Russia
[1] a.kosolapov@mail.ru
[2] a.primakin@mail.ru

Abstract. Taking into account the special relevance of the fight against information terrorism, the article focuses on the methodology and technology of building mathematical models in the field of information warfare. Algorithms and procedures for multiparametric statistical analysis performed in the environment of specialized mathematical programs such as Statistica and the integrated mathematical package Mathcad are proposed as mathematical tools for constructing appropriate models in order to further compile a scientifically based forecast of the situation.

A mathematical description of the situations countering information terrorism makes it possible to further rationally address the issues of logistical support for the relevant units of the Russian Guard troops to prevent and neutralize information threats.

Keywords: information terrorism, mathematical models of information warfare, indicators of the level of counter-terrorism of the Rosgvardiya structural unit, methods of multifactorial statistical analysis

For citation: Kosolapov A.D., Primakin A.I. The methodology and technology of constructing mathematical models in the field of information warfare using specialized mathematical packages. Vestnik Voennoj akademii vojsk nacional'noj gvardii. 2025;2(31):255–266. (In Russ.). Available from: https://vestnik-spvi.ru/2025/06/027.pdf.

Введение

Вопросы обеспечения национальной безопасности являются приоритетными в политике любого государства. Одно из ее направлений связано с предотвращением, отражением и нейтрализацией информационного терроризма [1].

Повсеместное применение информационных технологий и глобальная цифровая трансформация всех областей деятельности человека обосновывают тематику статьи, направленной на применение математических методов для прогнозирования проявлений террористической деятельности и, прежде всего, в информационной сфере.

Очевидно, что информационная безопасность структурно может рассматриваться, как одно из направлений обеспечения национальной безопасности. Это следует из Доктрины информационной безопасности Российской Федерации, где представлены официальные положения, направления и принципы обеспечения информационной безопасности. В частности, утверждается, что «уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи» представляют собой перечень угроз, устранить которые, в данном случае, – первостепенная задача в области информационного противоборства [2].

Приведенная в Доктрине классификация возможных источников угроз, где основной акцент делается на внешних угрозах (информационный терроризм, разведка иностранных государств и т. п.), позволяет определить направленность информационного противоборства, как «выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз» [2].

Учитывая особую актуальность борьбы с терроризмом во всех видах его проявления [3], для информационной сферы появилось даже понятие «информационный терроризм» [4], целью которого считается расшатывание и ослабление конституционного строя России [5]. В работах [6, 7] освещается круг вопросов, связанных с проявлением информационного терроризма, предложены меры противодействия ему.

В связи с этим перед силовыми министерствами России и спецструктурами по борьбе с информационным терроризмом, поставлены задачи [8, 9, 10]:

обеспечить охрану закрытых территорий, предполагающих интерес для вражеских структур, с точки зрения информационного терроризма;

пресекать проникновение нарушителей на охраняемые территории и т. п.

Таким образом, возникает необходимость поиска и применения математического инструментария, для описания информационных угроз и прогнозирования проявлений террористической деятельности в информационной сфере, что позволит в соответствующих структурах Росгвардии своевременно определить недоработки в системе информационного противоборства и своевременно нейтрализовать потенциальные информационные угрозы.

Структурно статья состоит из двух частей.

В первой части приводится анализ предметной области, позволяющий сформировать систему показателей отражающих уровень подготовки и укомплектованности соответствующего структурного подразделения Росгвардии для эффективного противостояния возможным террористическим угрозам в информационной сфере.

Вторая часть статьи посвящена краткой характеристике и предназначению различных видов многопараметрических статистических анализов применительно к решаемой задаче. Приведены процедуры и алгоритмы, выполняемые как в среде специализированного программного обеспечения (программа Statistica), так и в стандартных (обычных) офисных приложениях (электронных таблицах MS Excel или LO Calc), обеспечивающие построение математической модели с возможностями прогнозирования и противодействия информационному терроризму.

Основные положения

1. Анализ предметной области и формирование системы показателей, отражающих уровень подготовки и укомплектованности соответствующего структурного подразделения Росгвардии для успешного противоборства с информационным терроризмом.

Для оценки уровня укомплектованности и подготовки сотрудников структурного подразделения Росгвардии к борьбе с информационным терроризмом необходимо определить факторы, отражающие это явления, моделирующие информационное противоборство. Очевидно, что иско-

мые факторы во многом аналогичны показателями уровня обеспечения информационной защиты соответствующего подразделения.

В работах [11, 12], на основе анализа использования информационных технологий и применения технических средств защиты информации в структурных подразделениях Росгвардии, представлены некоторые из показателей, отражающих степень защиты информации в рамках информационного противоборства.

Ниже приводится сводная таблица (таблица 1) показателей (или факторов), связанных с решением задач информационного противоборства в подразделениях Росгвардии [13]. Возьмем за основу данный материал для нашей дальнейшей работы.

Таблица 1 – Описание показателей, определяющих степень обеспечения информационной безопасности структурного подразделения Росгвардии

Table 1 – Description of the indicators determining the degree of information security of the Rosgvardiya structural unit

Показатель	Содержание показателя
$X1$	Доля л/с структурного подразделения Росгвардии, освоивших учебные программы переподготовки по вопросам решения задач информационного противоборства и способных их выполнять. Этот показатель может быть отнесен к организационным методам защиты информации.
$X2$	Экономический метод защиты информации, связанный с освоением бюджетных средств, направленных на решение задач информационного противоборства.
$X3$	Показатель укомплектованности подразделения техническими средствами защиты информации в соответствии с табелем положенности. Этот показатель может быть отнесен к программно-техническим методам защиты информации.
$X4$	Доля пользователей (или автоматизированных рабочих мест), подключенных к ведомственному сервису электронного документооборота «СЭД Росгвардии», позволяющих проводить аттестацию объектов информатизации и обрабатывать информацию ограниченного распространения. Этот показатель может быть отнесен к организационно-техническим методам защиты информации.
$X5$	Доля пользователей (или автоматизированных рабочих мест), применяющих для работы отечественные программные продукты (операционные системы и офисные приложения). Этот показатель может быть отнесен к организационно-техническим методам защиты информации.
$X6$	Доля пользователей (или автоматизированных рабочих мест), осуществляющих взаимодействие с органами государственной власти посредством подключения к открытым и закрытым информационным системам. Этот показатель может быть отнесен к организационным методам защиты информации.
Показатели, связанные с программно-аппаратными методами защиты информации в структурных подразделениях Росгвардии	
$X7$	Обеспеченность рабочих мест антивирусной защитой. Этот показатель может быть отнесен к программным методам защиты информации.
$X8$	Обеспеченность рабочих мест системами обнаружения компьютерных атак со стороны противника с возможностью сбора информации об особенностях и характеристиках нападения. Этот показатель может быть отнесен к программным методам защиты информации.
$X9$	В соответствии с рекомендациями ФСТЭК России и ФСБ России обеспеченность ведомственных информационных систем программно-аппаратным комплексом межсетевого экранирования. Этот показатель может быть отнесен к программно-аппаратным методам защиты информации.

Показатель	Содержание показателя
$X10$	Обеспеченность ведомственных объектов информатизации программно-аппаратными комплексами анализа защищенности систем, поиска уязвимостей и контроля соответствия международным и отраслевым стандартам. Этот показатель может быть отнесен к программно-аппаратным методам защиты информации.
$X11$	Возможность осуществления мероприятий по всем объектам информатизации, связанных с аттестацией рабочих мест. Этот показатель, в большей степени, может быть отнесен к организационным методам защиты информации.
$X12$	Обеспеченность объектов информатизации профильными специалистами по программно-технической защите информации, а также наличие соответствующих должностей. Этот показатель может быть отнесен к организационным методам защиты информации.

Очевидно, что представленный перечень показателей ($X1 - X12$), отражающий уровень готовности структурного подразделения к информационному противоборству, не может считаться полным, поскольку разнообразие возможных угроз на объект информатизации постоянно видоизменяется. Тем не менее данные показатели способны в целом охарактеризовать сущность проблемы. В рамках данной статьи важно отметить, что проблема информационного противоборства многоплановая и зависит от многих показателей, которые мы должны учитывать в комплексе.

Перейдем к следующей части статьи, посвященной краткой характеристике и предназначению различных видов многопараметрических статистических анализов применительно к решаемой задаче – прогнозированию ситуаций информационного терроризма в целях его нейтрализации.

Комплексность (многофакторность) решаемых задач в сфере информационного противоборства предполагает анализ показателей, определяющих степень информационного противоборства, их связь друг с другом, значимость влияния каждого на существо решаемых задач. Все сводится к необходимости анализа сложного взаимосвязанного многообразия показателей, описывающих изучаемое явление или процесс.

Проведение подобных исследований требуют от специалиста знания многопараметрических методов анализа и практических навыков их осуществления с помощью специализированных математических пакетов.

Методы многопараметрического анализа формируют такую статистическую модель, которая адекватно отражает особенности изучаемого явления, его специфику и тенденции дальнейшего развития. Как правило, в этом случае применяется выборочный статистический метод, который позволяет при определенном уровне значимости и с помощью процедур и алгоритмов статистических гипотез распространить полученный результат на генеральные совокупности [13].

Так, в работе [14] представлены особенности применения некоторых видов многофакторного статистического анализа. Прежде всего, это множественный корреляционно-регрессионный анализ, кластерный, метод главных компонент и другие.

В рамках настоящей статьи интересно рассмотреть, прежде всего, множественный корреляционно-регрессионный анализ, который позволяет оценить взаимную тесноту связи между показателями $(X_1, X_2, \dots, X_n)$ и построить множественную регрессионную модель их влияния на изучаемый показатель (переменная Y – уровень подготовки подразделения для успешного информационного противоборства). Это позволяет понять и визуализировать достаточно сложный механизм отношений между показателями $(X_1, X_2, \dots, X_n)$ и спрогнозировать дальнейший ход развития изучаемого явления.

В соответствии с тематикой статьи нас будет интересовать множественный линейный корреляционно-регрессионный анализ, позволяющий установить тесноту и взаимосвязи (вид функции) между переменными (или факторами) в их влиянии на итоговый показатель – уровень противодействия информационному терроризму.

Необходимо отметить, что переменные $(X_1, X_2, \dots, X_n)$ измеряются в разных единицах (размерностях), а это требует от исследователя нормировки исходных статистических данных.

Для этого со значениями каждой переменной $(X_1, X_2, \dots, X_n)$ производят процедуру нормализации исходных статистических данных по формуле $z_i = \frac{(x_i - \bar{x}_i)}{\sigma_{x_i}}$, где $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$ – средние выборочные значения соответствующих случайных величин x_i; z_i – нормированная случайная величина; σ_{x_i} – среднеквадратическое отклонение, как характеристика рассеивания случайной величины относительно среднего выборочного значения.

Данная процедура обеспечивает корректность сравнения самых разных переменных, превращая их в безразмерные величины со средним значением $\bar{z}_i = 0$ и среднеквадратическим отклонением $\sigma_{z_i} = 1$.

Помимо нормировки исходных статистических данных, необходимо выполнение еще ряда процедур. Во-первых, требуется убедиться, что выборки по переменным $X_1, X_2, \dots, X_n$ соответствуют нормальному закону плотности распределения вероятностей. Во-вторых, объемы сравниваемых выборок должны быть одинаковыми $(n_1 = n_2 = \dots = n_i)$ [15].

Дальнейший алгоритм корреляционного анализа предполагает построение корреляционной матрицы, элементы которой характеризуют направление и тесноту взаимосвязи как между переменными $X_1, X_2, \dots, X_n$, так их влияние на выходной показатель Y (в нашем случае, Y – уровень противодействия информационному терроризму соответствующего подразделения Росгвардии). Пример корреляционной матрицы, выполненный в среде специализированного математического пакета Statistica, представлен на рисунке 1.

Variable	Correlations (Spreadsheet3) Casewise deletion of MD N=43				
	Var1	Var2	Var3	Var4	Var5
Var1	1,00	0,82	-0,04	-0,05	-0,30
Var2	0,82	1,00	-0,07	-0,01	-0,20
Var3	-0,04	-0,07	1,00	0,85	0,40
Var4	-0,05	-0,01	0,85	1,00	0,39
Var5	-0,30	-0,20	0,40	0,39	1,00

Рисунок 1 – Корреляционная матрица, иллюстрирующая линейную зависимость между переменными $X_1, X_2, \dots, X_5$ в среде специализированного математического пакета Statistica

Figure 1 – Is a correlation matrix illustrating the linear relationship between the variables X_1,X_2,...,X_5 in the environment of the specialized mathematical package Statistica

Элементами корреляционной матрицы являются коэффициенты корреляции, характеризующие тесноту и направление линейной связи между соответствующими переменными. Так, наиболее тесная положительная связь наблюдается между переменными X_3 и X_4 (на рисунке 1 – $Var3$ и $Var4$), поскольку $r_{x_3,x_4} = 0{,}85$.

Для оценки уровня достоверности коэффициентов корреляции необходимо пользоваться формулой (1) и таблицей критических значений для критерия t-Стьюдента (или встроенными функциями программ Mathcad – $qt(p, df)$ и Excel – СТЬЮДЕНТ$(1 - \frac{\alpha}{2}, df)$) с числом степеней свободы $df = n - 2$ [16]:

$$T_{\text{ф}} = |r_{\text{эмп.}}| \cdot \sqrt{\frac{n-1}{1-r_{\text{эмп.}}^2}}, \quad (1)$$

где $r_{\text{эмп.}}$ – эмпирический коэффициент корреляции между парными переменными; n – число коррелируемых признаков (количество парных объектов – объем выборки); $T_{\text{ф}}$ – эмпирическое значение критерия, по которому проверяется уровень значимости коэффициента корреляции (сравниваем $T_{\text{ф}}$ с табличным значением t-критерия Стьюдента).

Часто требуется определить коэффициент множественной корреляции, смысл которого сводится к оценке тесноты линейной связи конкретной переменной, допустим Y, с совокупностью остальных переменных (X_1 и X_2).

Особенности «чистого» влияния друг на друга пары переменных при условии, что все прочие переменные не меняются и не

оказывают какого-либо воздействия на характер изучаемой связи, определяет частный коэффициент корреляции.

Алгоритм и процедуры расчета множественного и частного коэффициентов корреляции подробно представлены в работе [17].

Множественный регрессионный анализ позволяет найти приближенную математическую зависимость одной переменной от нескольких других.

При этом функциональная многопараметрическая зависимость определяется линейной зависимостью (2):

$$Y = b_0 + b_1 \cdot X_1 + b_2 \cdot X_2 + \ \dots \ b_n \cdot X_n. \quad (2)$$

Задача регрессионного анализа состоит в том, чтобы по конкретной выборке найти оценки неизвестных коэффициентов $(b_0, b_1, \dots, b_n)$ так, чтобы построенная линия регрессии являлась бы наилучшей в определенном смысле среди всех других прямых.

Существует несколько методик по расчету коэффициентов $b_0, b_1, \dots, b_n$.

Более полное понимание процедур расчета искомых коэффициентов обеспечивает матричный метод [18]. Данный метод в матричной форме представлен ниже (3):

$$B = (X^T \cdot X)^{-1} \cdot X^T \cdot Y, \quad (3)$$

где B – матрица искомых коэффициентов $b_0, b_1, \dots, b_n$; X – матрица исходных переменных; X^T – транспонированная матрица исходных переменных; $(X^T \cdot X)^{-1}$ – обратная матрица результата перемножения матриц X^T и X; Y – матрица значений изучаемого признака при соответствующих значениях X.

Существенно упрощает поиск коэффициентов уравнения регрессии встроенная в среду электронных таблиц функция ЛИНЕЙН. В ходе ее применения от исследователя требуется указать только адреса ячеек, в которых находятся исходные данные (Y и X), результат расчета с некоторой дополнительной информацией выдается в форме, показанной на рисунке 2.

b3	b2	b1	b0
0,45265	-0,4763	1,137868	-1,18896E-15
0,20952	0,153132	0,132771	0,067016541
0,960804	0,232152	#Н/Д	#Н/Д
65,36736	8	#Н/Д	#Н/Д
10,56884	0,431157	#Н/Д	#Н/Д

Рисунок 2 – Пример вывода результатов расчета коэффициентов линейного уравнения регрессии (три переменных) в случае применения функции ЛИНЕЙН

Figure 2 – Is an example of the output of the calculation results of the coefficients of a linear regression equation (three variables) in the case of using the LINEAR

В результате (рисунок 2) получили математическую модель в виде линейного уравнения регрессии, связывающего изучаемое явление (Y) с тремя исходными переменными (X_1, X_2, X_3): $Y = 1{,}138 \cdot X_1 - 0{,}476 \cdot X_2 + 0{,}453 \cdot X_3$.

Здесь же указывается дополнительная информация о том, что полученная модель на 96 % описывает закономерности процесса (предметная область многофакторного дисперсионного анализа – коэффициент детерминации $R^2 = 0{,}9608$).

В специализированных математических пакетах (например, Mathcad) также имеются в наличии встроенные функции по поиску коэффициентов регрессии. Ниже приводятся примеры применения различных процедур в среде интегрированного пакета Mathcad для нахождения коэффициентов линейной регрессии общего вида (рисунок 3) и построения математической модели полиноминальной регрессии (рисунок 4) [19].

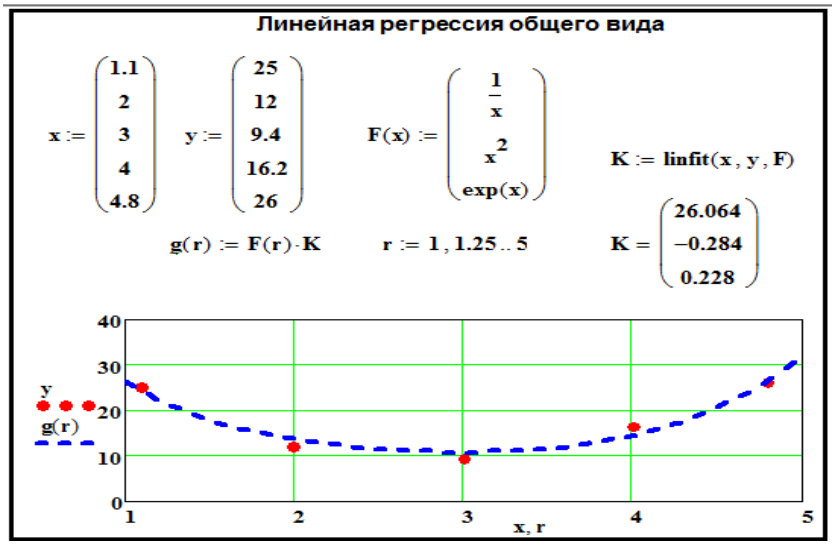

Рисунок 3 – Нахождения коэффициентов линейной регрессии общего вида в среде интегрированного математического пакета Mathcad

Figure 3 – Finding the coefficients of general linear regression in the environment of the integrated Mathcad mathematical package

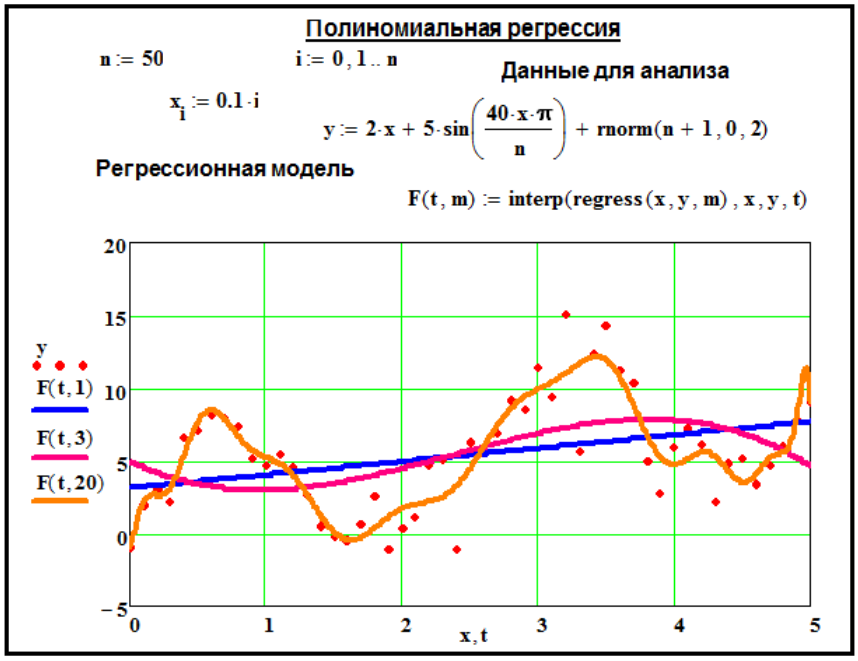

Рисунок 4 – Построение математической модели полиноминальной регрессии вида в среде интегрированного математического пакета Mathcad

Figure 4 – Construction of a mathematical model of a polynomial regression in the environment of the integrated Mathcad mathematical package

Относительно вопросов прогнозирования состояния информационного терроризма, то в работе [20] представлены результаты комплексного исследования криминогенной ситуации в Санкт-Петербурге.

Применяемые в этом случае методы прогнозирования можно классифицировать следующим образом:

методы, основанные на алгоритмах и процедурах множественного корреляционно-регрессионного анализа;

методы, основанные на анализе временных рядов каждой из изучаемых переменных;

методы, основанные на особенностях определяющих (значимых) взаимосвязей

между переменными, по сути, на базе многопараметрического факторного анализа.

Первая группа методов прогнозирования преступлений экстремистской и террористической направленности, собственно, и соответствует названию настоящей статьи. Определив коэффициенты уравнения регрессии, т. е. построив математическую модель процесса, можем говорить о тренде (тенденции) рассматриваемого явления в зависимости от значимых переменных.

Для оценки адекватности регрессионной модели применяются статистические критерии, в данном случае, критерий Фишера (*F*-тест), отражающий особенности многофакторного дисперсионного анализа [16].

Критерий Стьюдента (*t*-тест) оценивает значимость каждого из коэффициентов $b_0, b_1, \ldots, b_n$ регрессионной модели (2) в отдельности [13].

Если инструментом для обработки исходных данных выбирается электронная таблица, то вся эта дополнительная информация по результатам многофакторного статистического анализа явления в табличной форме автоматически предоставляется исследователю (рисунок 2).

Для упрощения, не погружаясь в тонкости математических алгоритмов, и автоматизации осуществления прогноза в рамках предметной области, целесообразно использовать возможности офисных программ (электронных таблиц) и специализированные функции, встроенные в математические пакеты.

Так, представленные в работе [20] результаты прогнозирования состояния преступности в Санкт-Петербурге были составлены на основе встроенной в электронную таблицу Excel статистической функции «ТЕНДЕНЦИЯ».

Фрагмент данного криминологического прогноза относительно ситуаций террористической направленности показан в таблице 2 (нумерация показателей сохраняется по первоисточнику).

Таблица 2 – Фрагмент прогнозирования некоторых видов преступлений, связанных с терроризмом в Санкт-Петербурге

Table 2 – A fragment of forecasting some types of terrorism-related crimes in St. Petersburg

№ п/п	Название показателя	Отчет		Оценка	Прогноз		
		2022	2023	2024	2024	2025	2026
16.	Преступления экстремистской направленности, ед.	32	37	44	44	49	555
18.	Преступления террористического характера, ед.	23	48	56	51	52	55
19.	Преступления, связанные с незаконным оборотом оружия, ед.	155	165	535	259	257	274

В среде математического пакета Mathcad для составления прогноза ситуации применяется функция экстраполяции: *predict(data,k,N)*, где *data* – вектор данных; *k* – степень полинома регрессии; *N* – число точек. Эта функция по исходной статистической информации позволяет спрогнозировать некоторое число *N* последующих точек. Она позволяет визуализировать динамику развития изучаемого процесса.

На рисунке 5 представлен пример построения прогноза с помощью функции *predict* в среде интегрированного математического пакета Mathcad.

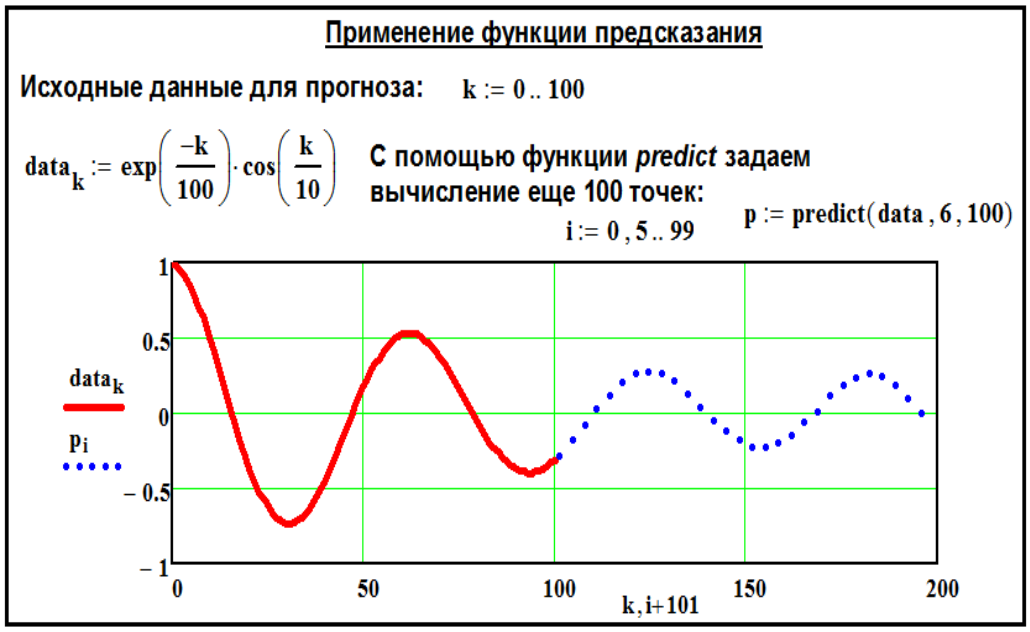

Рисунок 5 – Процедуры построения прогноза с помощью функции *predict* в среде интегрированного математического пакета Mathcad

Figure 5 – Forecasting procedures using the predict function in the environment of the integrated Mathcad mathematical package

Заключение

Опираясь на вышеизложенный материал, можно утверждать, что, обладая объективной информацией по основополагающим показателям (факторам), которые отражают суть изучаемого явления, можно на основе специализированных математических пакетов оперативно сформировать математическую модель изучаемого процесса для дальнейшего прогноза ситуации.

Для этого, в зависимости от цели решаемой задачи, необходимо воспользоваться теми или иными методами многофакторного статистического анализа. В нашем случае для построения модели и прогнозирования ситуаций информационной террористической направленности, целесообразно применять алгоритмы и процедуры многофакторного корреляционно-регрессионного анализа. Упростить и автоматизировать процессы расчета существенно помогают специализированные математические программы и офисные приложения в виде электронных таблиц.

Математически обоснованный прогноз ситуации позволит рационально подойти к решению вопросов материально-технического обеспечения соответствующих подразделений Росгвардии для предотвращения и нейтрализации угроз, связанных с информационным терроризмом.

Список источников

1. Указ Президента Российской Федерации от 02 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 24.04.2025).

2. Доктрина информационной безопасности Российской Федерации. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 24.04.2025).

3. Терроризм в России. URL: https://www.tadviser.ru/index.php/ Статья: Терроризм в России (дата обращения: 24.04.2025).

4. Алоева А. А. Информационный терроризм – угроза национальной безопасности в условиях цифровизации / А. А. Алоева, И. А. Алоев, А. З. Жуков // Пробелы в российском законодательстве. 2020. Т. 13. № 6. С. 197–201.

5. Аношкина А. А. Информационный терроризм как угроза национальной безопасности // Молодой ученый. 2020. № 20 (310). С. 245–247.

6. Манукян А. Р. Проблемы противодействия терроризму и экстремизму в сети интернет в условиях повсеместной цифровизации // Пробелы в российском законодательстве. 2021. Т. 14. № 3. С. 37–41.

7. Темботов Р. А. Проблемы установления уголовной ответственности за информационный терроризм // Право, общество, государство: проблемы истории, теории и практики: сборник материалов Всероссийской научно-теоретической конференции / под общ. ред. С. Г. Куликовой, М. В. Конопляниковой. М., 2022. С. 42–44.

8. Вопросы Федеральной службы войск национальной гвардии Российской Федерации: Указ Президента Российской Федерации от 05 апреля 2016 г. № 157 (ред. от 17.06.2019). URL: https://www.consultant.ru/document/cons_doc_LAW_196284/ (дата обращения: 24.04.2025).

9. Федеральный закон от 03 июля 2016 г. № 226-ФЗ «О войсках национальной гвардии Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_200506/ (дата обращения: 24.04.2025).

10. Фофанова А. Ю. Роль Росгвардии в обеспечении безопасности от терроризма в России / А. Ю. Фофанова, А. С. Зиновьева / International Journal of Humanities and Natural Sciences. 2024. Vol. 6-1 (93). С. 40–44.

11. Росгвардия подвела итоги своей работы за 2024 год. Обзор состояния применения информационных технологий и технической защиты информации в Росгвардии. URL: https://stavropolye.tv/news/204974 (дата обращения: 24.03.2025).

12. Потапова Л. С. Факторы оценки уровня подготовки структурных подразделений Росгвардии в сфере информационного противоборства / Л. С. Потапова, А. И. Примакин / Актуальные проблемы противодействия экстремизму и терроризму на современном этапе: сб. науч. ст. II Всероссийской научно-практической конференции с международным участием. Новосибирск: НВИ войск национальной гвардии Российской Федерации, 2023. С. 143–149.

13. Ванягина М. Р. Применение алгоритмов проверки статистических гипотез в среде математического пакета Mathcad при проведении педагогического эксперимента / М. Р. Ванягина, А. И. Примакин / Математика и ее приложение в науке и образовании: материалы Межвузовского научно-методического семинара с международным участием / сост.
Е. Н. Трофимец, Г. Е. Косенко. СПб. : Санкт-Петербургский университет ГПС МЧС России, 2024. С. 208–213.

14. Большакова Л. В. Методы многомерного анализа в вопросах обеспечения информационной и экономической безопасности: учебное пособие / Л. В. Большакова, А. И. Примакин, Н. А. Яковлева. СПб. : Изд-во СПб ун-та МВД России, 2013. 92 с.

15. Гмурман В. Е. Теория вероятностей и математическая статистика: учебник для прикладного бакалавриата. 12-е изд. М. : Юрайт, 2015. 480 с.

16. Большакова Л. В. Теория проверки статистических гипотез при математико-статистическом исследовании педагогических проблем / Л. В. Большакова, Н. А. Яковлева // Вестник Санкт-Петербургского университета МВД России. 2016. № 4 (72). С. 149–157.

17. Ермолаев-Томин О. Ю. Математические методы в психологии: учебник / О. Ю. Ермолаев-Томин. 5-е изд., испр. и доп. М. : Изд-во Юрайт, 2014. 511 с.

18. Ефимова А. Б. Применение математических методов в криминологических исследованиях (на примере коррупционных преступлений) / А. Б. Ефимова, А. И. Примакин / Межведомственное сотрудничество при обеспечении национальных приоритетов в противодействии коррупции: материалы межведомственной научно-практической конференции. СПб., 2022. С. 181–187.

19. Васильев А. Н. Matcad 13 на примерах. СПб. : БХВ-Петербург, 2006. 528 с.

20. Состояние преступности в Санкт-Петербурге. Криминологический мониторинг и прогноз: научно-практическое пособие. СПб. : Изд-во СПб ГУП «СПб ИАЦ», 2024. 332 с.

References

1. Ukaz Prezidenta Rossijskoj Federacii ot 02 iyulya 2021 g. № 400 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii». URL: http://www.kremlin.ru/acts/bank/47046 (data obrashcheniya: 24.04.2025). (In Russ.).

2. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (data obrashcheniya: 24.04.2025). (In Russ.).

3. Terrorizm v Rossii. URL: https://www.tadviser.ru/index.php/ Stat'ya: Terrorizm v Rossii (data obrashcheniya: 24.04.2025). (In Russ.).

4. Aloeva A. A. Informacionnyj terrorizm – ugroza nacional'noj bezopasnosti v usloviyah cifrovizacii / A. A. Aloeva, I. A. Aloev, A. Z. ZHukov // Probely v rossijskom zakonodatel'stve. 2020. T. 13;6: 197–201.

5. Anoshkina A. A. Information terrorism as a threat to national security // Molodoj uchenyj. 2020;20 (310): 245–247. (In Russ.).

6. Manukyan A. R. Problemy protivodejstviya terrorizmu i ekstremizmu v seti internet v usloviyah povsemestnoj cifrovizacii // Probely v rossijskom zakonodatel'stve. 2021. T. 14;3. S. 37–41. (In Russ.).

7. Tembotov R. A. Problemy ustanovleniya ugolovnoj otvetstvennosti za informacionnyj terrorizm // Pravo, obshchestvo, gosudarstvo: problemy istorii, teorii i praktiki: sbornik materialov Vserossijskoj nauchno-teoreticheskoj konferencii / pod obshch. red. S. G. Kulikovoj, M. V. Konoplyanikovoj. M., 2022. S. 42–44. (In Russ.).

8. Voprosy Federal'noj sluzhby vojsk nacional'noj gvardii Rossijskoj Federacii: Ukaz Prezidenta Rossijskoj Federacii ot 05 aprelya 2016 g. № 157 (red. ot 17.06.2019). Available from: https://www.consultant.ru/document/cons_doc_LAW_196284/ (data obrashcheniya: 24.04.2025). (In Russ.).

9. Federal'nyj zakon ot 03 iyulya 2016 g. № 226-FZ «O vojskah nacional'noj gvardii Rossijskoj Federacii». Available from: https://www.consultant.ru/document/cons_doc_LAW_200506/ (data obrashcheniya: 24.04.2025). (In Russ.).

10. Fofanova A. YU. The role of the Russian Guard in ensuring security against terrorism in Russia / A. YU. Fofanova, A. S. Zinov'eva / International Journal of Humanities and Natural Sciences. 2024. Vol. 6-1 (93): 40–44. (In Russ.).

11. Rosgvardiya podvela itogi svoej raboty za 2024 god. Obzor sostoyaniya primeneniya informacionnyh tekhnologij i tekhnicheskoj zashchity informacii v Rosgvardii. Available from: https://stavropolye.tv/news/204974 (data obrashcheniya: 24.03.2025). (In Russ.).

12. Potapova L. S. Faktory ocenki urovnya podgotovki strukturnyh podrazdelenij Rosgvardii v sfere informacionnogo protivoborstva / L. S. Potapova, A. I. Primakin / Aktual'nye problemy protivodejstviya ekstremizmu i terrorizmu na sovremennom etape: sb. nauch. st. II Vserossijskoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem. Novosibirsk: NVI vojsk nacional'noj gvardii Rossijskoj Federacii, 2023. S. 143–149. (In Russ.).

13. Vanyagina M. R. Primenenie algoritmov proverki statisticheskih gipotez v srede matematicheskogo paketa Mathcad pri provedenii pedagogicheskogo eksperimenta / M. R. Vanyagina, A. I. Primakin / Matematika i ee prilozhenie v nauke i obrazovanii: materialy Mezhvuzovskogo nauchno-metodicheskogo seminara s mezhdunarodnym uchastiem / sost. E. N. Trofimec, G. E. Kosenko. SPb. : Sankt-Peterburgskij universitet GPS MCHS Rossii, 2024. S. 208–213. (In Russ.).

14. Bol'shakova L. V. Metody mnogomernogo analiza v voprosah obespecheniya informacionnoj i ekonomicheskoj bezopasnosti: uchebnoe posobie / L. V. Bol'shakova, A. I. Primakin, N. A. YAkovleva. SPb. : Izd-vo SPb un-ta MVD Rossii, 2013. 92 s. (In Russ.).

15. Gmurman V. E. Teoriya veroyatnostej i matematicheskaya statistika: uchebnik dlya prikladnogo bakalavriata. 12-e izd. M. : YUrajt, 2015. 480 s. (In Russ.).

16. Bol'shakova L. V. The theory of testing statistical hypotheses in the mathematical and statistical study of pedagogical problems / L. V. Bol'shakova, N. A. YAkovleva // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2016;4 (72): 149–157. (In Russ.).

17. Ermolaev-Tomin O. YU. Matematicheskie metody v psihologii: uchebnik / O. YU. Ermolaev-Tomin. 5-e izd., ispr. i dop. M. : Izd-vo YUrajt, 2014. 511 s. (In Russ.).

18. Efimova A. B. Primenenie matematicheskih metodov v kriminologicheskih issledovaniyah (na primere korrupcionnyh prestuplenij) / A. B. Efimova, A. I. Primakin / Mezhvedomstvennoe sotrudnichestvo pri obespechenii nacional'nyh prioritetov v protivodejstvii korrupcii: materialy mezhvedomstvennoj nauchno-prakticheskoj konferencii. SPb., 2022. S. 181–187. (In Russ.).

19. Vasil'ev A. N. Matcad 13 na primerah. SPb. : BHV-Peterburg, 2006. 528 s. (In Russ.).
20. Sostoyanie prestupnosti v Sankt-Peterburge. Kriminologicheskij monitoring i prognoz: nauchno-prakticheskoe posobie. SPb. : Izd-vo SPb GUP «SPb IAC», 2024. 332 s. (In Russ.).

Информация об авторах

А. Д. Косолапов *– кандидат педагогических наук, доцент*
А. И. Примакин *– доктор технических наук, профессор*

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 19.05.2025;
одобрена после рецензирования 11.06.2025;
принята к публикации 19.06.2025.

Information about the authors

A. D. Kosolapov – Candidate of Sciences (Pedagogy), Docent
A. I. Primakin *– Doctor of Sciences (Technical), Professor*

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

The article was submitted 19.05.2025;
approved after reviewing 11.06.2025;
accepted for publication 19.06.2025.