Экономические и социально-гуманитарные исследования. 2024. № 2 (42). С. 68—83.
Economic and Social Research. 2024. No. 2 (42). P. 68—83.
Научная статья

УДК 332.1 + 330.101:33:004
doi: 10.24151/2409-1073-2024-2-68-83
https://elibrary.ru/altxye

Зависимость уровня цифрового мошенничества, совершённого с помощью методов социальной инженерии, от экономических факторов в субъектах Российской Федерации

***А. Ю. Стрижак*[1], *О. А. Пекарская*[2]**

[1] *Национальный открытый институт г. Санкт-Петербург, Санкт-Петербург, Россия*
[2] *Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия*

[1] *strizhak.a86@mail.ru*
[2] *pekarskaya.olga@mail.ru*

Аннотация. Представлен теоретический анализ феномена социальной инженерии в условиях развития цифрового пространства. Исследованы основные методы социальной инженерии, используемые мошенниками с целью получить доступ к конфиденциальной информации потенциальной жертвы. Проведен корреляционно-регрессионный анализ влияния экономических факторов (средней заработной платы и безработицы в регионах) на коэффициент пострадавших от преступлений, совершённых с применением методов социальной инженерии. Для анализа использованы данные зарегистрированных в МВД РФ заявлений граждан, потерпевших от мошеннических действий, совершённых с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации. Выявлена прямая связь количества преступлений, совершённых с использованием приемов социальной инженерии, с показателями безработицы по регионам РФ, а также обратная — со средней заработной платой жителей регионов. Предложены меры нивелирования проблемы мошенничества в цифровом пространстве.

Ключевые слова: социальная инженерия, оппортунистическое поведение, мошенничество, кибератака, цифровое пространство

Для цитирования: Стрижак А. Ю., Пекарская О. А. Зависимость уровня цифрового мошенничества, совершённого с помощью методов социальной инженерии, от экономических факторов в субъектах Российской Федерации // Экономические и социально-гуманитарные исследования. 2024. № 2 (42). С. 68—83. https://doi.org/10.24151/2409-1073-2024-2-68-83 EDN: ALTXYE.

Original article

Dependence of the level of digital fraud committed using social engineering methods on economic factors in the federal subjects of the Russian Federation

A. Yu. Strizhak[1], O. A. Pekarskaya[2]

[1] National Open Institute Saint-Petersburg, St. Petersburg, Russia
[2] Saint-Petersburg University of State Fire Service of EMERCOM of Russia, St. Petersburg, Russia

[1] strizhak.a86@mail.ru
[2] pekarskaya.olga@mail.ru

Abstract. The authors present theoretical analysis of the phenomenon of social engineering under conditions of digital space development and discuss the principal methods of social engineering used by fraudsters to gain access to the confidential information about a potential victim. Correlation and regression analysis of economic factors impact on the coefficient of victims of crimes committed using social engineering methods is carried out. The factors under consideration include average salary and unemployment in the regions. The analysis was conducted using the data from statements registered with the Ministry of Internal Affairs of the Russian Federation by citizens who suffered from fraudulent actions committed using information and telecommunication technologies or in the field of computer information. A direct relationship between the number of criminal incidents committed using social engineering methods and unemployment rates in the regions of the Russian Federation, as well as an inverse relationship between the dependent variable and the average salary of residents of the regions have been revealed. Measures to deal with the digital fraud problem are proposed.

Keywords: social engineering, opportunistic behavior, fraud, cyberattack, digital space

For citation: Strizhak A. Yu., Pekarskaya O. A. "Dependence of the Level of Digital Fraud Committed Using Social Engineering Methods on Economic Factors in the Federal Subjects of the Russian Federation". *Economic and Social Research* 2 (42) (2024): 68—83. (In Russian). https://doi.org/10.24151/2409-1073-2024-2-68-83 EDN: ALTXYE.

Введение

В современном мире информационные технологии становятся важнейшим инструментом общественных коммуникаций, при этом устойчивость оппортунистической природы человеческого поведения сохраняется, и проблема социальной инженерии приобретает особую остроту. В широком смысле под социальной инженерией понимают комплекс манипулятивных техник, методов и приемов, используемых для воздействия на мотивы и убеждения людей в целях побуждения их к определенным действиям. Проблемы социальной инженерии нашли отражение в трудах иностранных и отечественных ученых из разных областей знаний (социологии, философии, экономики, психологии, компьютерных технологий): об этих проблемах писали за рубежом — Ч. С. Бхусал [13], Р. Хартфилд и Дж. Лукас [16], П. Каул и Д. Шарма [17], К. Менски (K. Manske) [18], Ф. Мутон с соавторами [19], К. Пархи и П. Питикайнен [20], в России — Ю. М. Резник [7], А. М. Бекарев и М. В. Плотников [1], О. Г. Ламинина [3], Н. Н. Равочкин [5], П. В. Ревенков и А. А. Бердюгин [6],

О. А. Уржа [11] и др. Однако авторы этих работ не анализировали влияние макроэкономических факторов на количество преступлений, совершаемых в цифровом пространстве с помощью методов социальной инженерии.

Обзор основных теорий и методов социальной инженерии

Важный аспект социальной инженерии — понимание психологических особенностей людей и анализ их поведения. Социальная инженерия дает возможность прогнозировать реакции людей на определенные ситуации, используя полученную информацию для реализации частных или групповых интересов. Например, маркетологи используют социальную инженерию для создания рекламного контента, наиболее релевантного и убедительного для целевой аудитории. Результаты деятельности социальных инженеров могут быть самыми разнообразными: от совершенствования бизнес-процессов и повышения эффективности командной работы в организациях до моделирования общественного мнения и изменения политического климата в государстве.

Сегодня ученые и практики рассматривают социальную инженерию как инструмент социально-психологической манипуляции, используемый мошенниками в целях реализации действий оппортунистического характера: получения доступа к конфиденциальной информации потенциальной жертвы и завладения ее имуществом. Современные информационно-коммуникационные технологии дают возможность злоумышленнику получить доступ к конфиденциальным данным потенциальной жертвы практически из любой точки мира в любое время. Неправомерный информационный обмен происходит посредством облачных технологий, мобильной связи, социальных сетей, мессенджеров, приложений и других цифровых площадок.

В качестве объекта манипуляции социальные инженеры используют такие интеллектуально-эмоциональные составляющие человека, как дружелюбие, доверие, конформизм, сочувствие, чувство вины и невежество. Характерными особенностями социальной инженерии, независимо от характера действий, К. Менски (K. Manske) называет: осознанное поведение, активный образ действий, целенаправленное влияние [18]. Убеждение, пишут П. Лоусон с соавторами, является неотъемлемым элементом социальной инженерии и фокусируется именно на связи между злоумышленником и жертвой [15]. Принципами убеждения, по мнению Р. Чалдини, могут быть: авторитет, конформизм, взаимность, приверженность, симпатия и дефицит (*товара или услуги. — А. С., О. П.*) [14].

Отдельные типы атак социальной инженерии легко автоматизировать. Основное преимущество автоматизированных атак отмечают К. Кромбхолц с соавторами: возможность добраться до несравнимо большего количества потенциальных целей в течение короткого отрезка времени [22]. Кроме того, автоматизированные атаки обходятся мошенникам дешевле офлайн-атак с точки зрения трансакционых издержек, поскольку требуют минимум времени и средств для поиска информации о потенциальной жертве, связи с ней, а также минимизируют риски ответственности за противоправное деяние.

Границы социальной инженерии, подчеркивает К. Менски, весьма расплывчаты. Некоторые методы атак (перехват сигнала, отказ в обслуживании, веб-поиск и т. д.) превратились в пограничные случаи социальной инженерии [18] (например, «водопой» — кибератака на веб-ресурс определенной социальной группы с целью заразить компьютерные системы пользователей; межсайтовая подделка запроса — кибератака на посетителей веб-сайтов, основанная на тайной отправке запроса от лица жертвы на вредоносный сервер; межсайтовый скриптинг — кибератака, в рамках которой вредоносные скрипты внедряются в контент веб-сайта).

Результатом мошеннических действий со стороны агентов социальной инженерии становятся колоссальные экономические и репутационные издержки для бизнеса и общества: утрата денежных средств, разглашение инсайдерской информации, судебные процессы, публичные скандалы, потеря доверия партнеров и клиентов и т. д. Социальная инженерия может угрожать и национальной безопасности страны, когда ее используют террористические организации и иностранные агенты с целью нанести вред государству.

Перечислим наиболее распространенные методы социальной инженерии в киберпространстве.

1. Фишинг (fishing, phishing) — попытка мошенника получить конфиденциальную информацию (чаще всего данные финансового характера) путем массовой рассылки вредоносных электронных писем, ссылок на веб-сайты и социальные сети. Например, потенциальная жертва получает от интернет-магазина, в котором иногда совершает покупки, электронное письмо следующего содержания: «Подтвердите свой аккаунт, чтобы получить 30 %-ную скидку на следующую покупку». Переходя по ссылке, жертва вводит свои персональные данные и данные банковской карты. После осуществления «пробного платежа» в несколько рублей и введения кода CVV со счета списываются все денежные средства жертвы. Фишинговые атаки могут носить и целенаправленный характер, т. е. быть нацелены на конкретных лиц или организации.

2. Погружение в мусорные контейнеры (dumpster diving) — практика получения конфиденциальных данных жертвы путем проникновения в его (ее) корзину с выброшенной (удаленной) информацией: банковскими выписками, счетами, договорами, содержащими реквизиты сторон, финансовой информацией о деятельности компании и т. д.

3. Создание фейковых (фальшивых) аккаунтов в социальных сетях. «Снабжая фейковые аккаунты характеристиками (фотографией, персональной информацией о себе), — предостерегают А. Д. Кавеева и К. Е. Гурин, — их создатели имитируют реальных пользователей. Эта имитация построена на изначально большем доверии пользователей таким же “обычным людям”, как они сами...» [2, с. 215]. Поддельные профили могут быть использованы мошенниками для рассылки фишинговых писем друзьям жертвы от ее имени, обманного набора большого количества комментариев и лайков на различных цифровых платформах, получения доступа к конфиденциальной информации пользователей сетей, продажи несуществующих товаров и услуг, шантажа, вымогательства, разглашения сведений, порочащих честь и достоинство, романтических знакомств в сетях с преследованием корыстных целей и т. п.

4. Обратная социальная инженерия — разновидность мошенничества, основанная на создании ситуации, при которой злоумышленник выдает себя за человека, способного помочь решить проблему целевой жертвы, при этом цель социального инженера — не помощь, а получение конфиденциальной информации жертвы. Например, кибермошенник отправляет потенциальным жертвам электронное письмо, в котором указывает контакты «технической поддержки», а через некоторое время создает проблемы на компьютере жертвы. В данном случае жертва сама свяжется с мошенником, после чего злоумышленник получит все ее конфиденциальные данные.

5. Вишинг (vishing, voice phishing) — фишинг с использованием телефона. Социальные инженеры, выходя на телефонную связь с потенциальной жертвой, могут представиться сотрудниками банка, правоохранительных органов, страховой компании, государственной организации, службы безопасности, коллекторского агентства и т. д. с целью получить доступ к конфиденциальной информации. Как правило, мошенники

подменяют номер телефона городским или корпоративным и звонят потенциальной жертве, создавая ощущение срочности, и этим дестабилизируют ее эмоциональное состояние. Во всем мире по меньшей мере 40 % работающих взрослых людей становятся жертвами атак вишинга в течение года[1].

6. Диджитал-мимикрия — создание клонов популярных приложений для смартфонов и планшетов, целью которых является похищение персональных данных или денежных средств потенциальной жертвы. Диджитал-мимикрия банковских приложений — одна из наиболее опасных, поскольку дает возможность злоумышленникам получить кратчайший доступ к реквизитам банковской карты. Как подсчитал Д. Морев, «в 2022 г. “Лаборатория Касперского” обнаружила около 200 тыс. новых банковских вирусов — приложений, которые попадают на устройство под видом легитимных программ. Это в два раза больше, чем в 2021 г., и максимум за последние шесть лет»[2].

7. «Дорожное яблоко» (привлекательный предмет, «забытый» на дороге) — способ кибератаки, предполагающий использование физических носителей (CD, флеш-накопители). Злоумышленник подбрасывает вредоносный носитель с вызывающей любопытство подписью (например, «совершенно секретно», «личная информация», «конфиденциально») в общественное место, рассчитывая, что жертва, нашедшая носитель, откроет мошенникам доступ к конфиденциальной информации.

8. Атаки через облачную службу. В данном сценарии злоумышленник помещает вредоносный файл в облако другого пользователя. Одна из самых больших проблем в подобных случаях — то, что компании и частные лица теряют контроль над своими данными при использовании облачного сервиса для их хранения и доступа к ним. На традиционных серверах, принадлежащих самим пользователям, компании могут ограничивать доступ и определять индивидуальные его политики. При использовании облачных сервисов ответственность перекладывается на третью сторону. Следовательно, рекомендуют Дж. С. Робертс и В. Аль-Хамдани, при использовании облачных сервисов для обмена конфиденциальной информацией сначала необходимо установить определенный уровень доверия между участниками [21].

9. Мошенничество с использованием нейросети. Данный сценарий социальной инженерии предполагает использование нейросети для создания фальшивых документов, дипфейков[3], аудио- и видеозаписей с целью получить доступ к конфиденциальной информации потенциальной жертвы посредством шантажа, вымогательства денежных средств, просьбы о финансовой помощи якобы от лица родных и друзей, а также совершения других противоправных деяний. Часто мошенники имитируют голоса и изображения известных личностей, представителей правоохранительных органов, чиновников. Использование авторитета, отмечают Я. У. Булле с соавторами, повышает вероятность успеха атаки социальных инженеров [23].

Более подробный теоретический анализ сценариев оппортунистических действий в киберпространстве и информационной защиты проведен нами в работах [4; 8; 9].

[1] По данным исследования: State of the phish [web]: 2019 report / Wombat Security // Proofpoint: security awareness & education platform. URL: https://www.proofpoint.com/sites/default/files/wombat-security/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf (accessed: 30.05.2024).

[2] ***Морев Д.*** Диджитал-мимикрия [Электронный ресурс]: как поддельные приложения воруют ваши деньги // РБК Тренды: [инф. портал РБК]. 29.05.2023. URL: https://trends.rbc.ru/trends/industry/647456e09a794724fb5793bb (дата обращения: 30.05.2024).

[3] Видеоматериал, не отснятый, а созданный средствами нейросети.

Исследование связи макроэкономических факторов и киберпреступности

Нами проведено исследование с целью определить, какие макроэкономические факторы влияют на рост или сокращение числа мошеннических действий, совершённых с использованием информационно-телекоммуникационных технологий (ИКТ) или в сфере компьютерной информации, в регионах России [10]. В исследовании мы опирались и на абсолютные криминологические показатели, которые указывали на число пострадавших жителей, и на относительные (индексы преступности). Достоинства абсолютных показателей — их простота, а также оперативность получения. Но при этом нельзя отрицать их определенную ограниченность, невозможность описания полной картины состояния преступности (в нашем случае — мошенничества с использованием ИКТ), которая представляет собой весьма сложное социальное явление и требует тщательного и разностороннего анализа. Абсолютные показатели не позволяют характеризовать структуру преступности, моделировать и прогнозировать криминогенные явления, тогда как это необходимо при выполнении задач предупреждения и профилактики преступлений, а также планирования деятельности правоохранительных органов в области обеспечения борьбы с преступностью всеми видами имеющихся в их распоряжении ресурсов.

Рассмотрим полученные из ФКУ «ГИАЦ МВД России» абсолютные криминологические показатели: число зарегистрированных в регионах России мошеннических эпизодов по ст. 159 УК РФ (далее обозначаемые как число преступлений), для совершения которых были использованы ИКТ (табл. 1). В качестве объекта исследования выбраны 20 регионов России, различающихся по числу преступлений, зарегистрированных в МВД за отчетный период (январь — декабрь 2023 г.). Из выборки исключены Москва и Московская область, а также Санкт-Петербург и Ленинградская область как аномальные (значения показателей преступности в них слишком выбиваются из общего ряда). Отметим, что число зарегистрированных преступлений было равно числу обращений от пострадавших в результате совершения этих преступлений. Регионы в табл. 1 ранжированы по возрастанию числа преступлений.

Таблица 1

Распределение числа преступлений по регионам России в 2023 г.

Регион	Число преступлений
1. Республика Калмыкия	387
2. Республика Тыва	408
3. Карачаево-Черкесская Республика	697
4. Республика Адыгея	913
5. Кабардино-Балкарская Республика	1157
6. Республика Северная Осетия — Алания	1326
7. Псковская область	1418
8. Курганская область	1538
9. Г. Севастополь	1623

Таблица 1 (Продолжение)

Регион	Число преступлений
10. Ивановская область	1968
11. Астраханская область	2040
12. Новгородская область	2083
13. Мурманская область	2326
14. Республика Крым	3735
15. Тюменская обл. (без а/о)	4489
16. Волгоградская область	6066
17. Ставропольский край	6439
18. Алтайский край	6709
19. Ростовская область	8258
20. Краснодарский край	17 649

Источник: данные получены нами из письма ФКУ «ГИАЦ МВД России» в ответ на официальное обращение.

Важнейшим показателем, характеризующим преступность, является коэффициент пострадавших от преступлений (КПП). Использовалась следующая формула расчета КПП:

$$КПП = (\text{число преступлений}) \times 100\,000 / \text{численность населения}. \quad (1)$$

Подставив в формулу (1) данные Росстата о численности населения в регионах РФ, мы получили значения КПП для выбранных регионов (табл. 2). Здесь и далее (в табл. 3 и 4) регионы ранжированы по возрастанию значения коэффициента.

Таблица 2

КПП в регионах России в 2023 г.

Регион	КПП
1. Мурманская область	226
2. Республика Крым	230
3. Краснодарский край	234
4. Тюменская область (без а/о)	238
5. Новгородская область	241
6. Ростовская область	242
7. Псковская область	244
8. Республика Адыгея	245

Таблица 2 (Продолжение)

Регион	КПП
9. Курганская область	248
10. Ставропольский край	251
11. Г. Севастополь	253
12. Волгоградская область	254
13. Астраханская область	257
14. Республика Тыва	261
15. Карачаево-Черкесская Республика	263
16. Кабардино-Балкарская Республика	268
17. Республика Калмыкия	269
18. Ивановская область	273
19. Алтайский край	273
20. Республика Северная Осетия — Алания	274

На криминогенную обстановку могут влиять многие институциональные и экономические факторы, в частности, эффективность законов и правовой системы, демографическая обстановка, уровень коррупции, качество образования, величина доходов населения и т. д. Все регионы имеют свои особенности в части, касающейся социальной и экономической обстановки. От региона к региону разнятся качество работы всех видов государственных органов, в том числе правоохранительных. В качестве независимых переменных, влияющих на КПП в регионах России, нами использованы два макроэкономических показателя: средняя заработная плата и уровень безработицы.

Результаты и обсуждение

Зависимость КПП от уровня заработной платы. Известно, что низкий уровень доходов и отсутствие равных возможностей в аспекте социальной мобильности приводят к тому, что среди населения четко выделяются группы финансово безграмотных людей с низким уровнем практической культуры делового общения. Граждане с низкой заработной платой, как правило, менее адаптированы к изменениям в экономике и часто становятся жертвами мошенников, совершающих экономические преступления.

По данным Росстата нами составлена таблица, показывающая зависимость КПП от средней заработной платы в регионе (см. табл. 3).

По расположению точек на корреляционном поле можно судить о том, что зависимость между средней заработной платой в регионе и зависимой переменной (число преступлений на 100 тыс. человек) близка к линейной (см. рис. 1).

Статистические гипотезы H_0 и H_1 формулируются так:

– нулевая гипотеза H_0: средняя заработная плата по региону не оказывает статистически значимого влияния на КПП;

Таблица 3

Первичные статистические данные о средней заработной плате и КПП в регионах России в 2023 г.

Регион	Средняя заработная плата, тыс. руб.	КПП
1. Мурманская область	94,845	226
2. Республика Крым	43,229	230
3. Краснодарский край	54,168	234
4. Тюменская область (без а/о)	58,168	238
5. Новгородская область	52,558	241
6. Ростовская область	50,784	242
7. Псковская область	43,384	244
8. Республика Адыгея	44,577	245
9. Курганская область	48,443	248
10. Ставропольский край	45,303	251
11. Г. Севастополь	48,924	253
12. Волгоградская область	47,789	254
13. Астраханская область	51,104	257
14. Республика Тыва	39,321	261
15. Карачаево-Черкесская Республика	38,769	263
16. Кабардино-Балкарская Республика	38,510	268
17. Республика Калмыкия	36,746	269
18. Ивановская область	37,227	273
19. Алтайский край	34,876	273
20. Республика Северная Осетия — Алания	39,544	274

Источник: официальные данные Росстата (Доклад «Социально-экономическое положение России» [Электронный ресурс]. 2023 г. // Федеральная служба государственной статистики: [сайт]. URL: https://rosstat.gov.ru/compendium/document/50801 (дата обращения: 30.05.2024).)

– альтернативная гипотеза H_1: средняя заработная плата по региону оказывает статистическое влияние на КПП.

В качестве независимой переменной X_1 нами принята средняя заработная плата в регионе (тыс. руб.), а в качестве зависимой переменной Y — КПП.

Зависимость между переменными X_1 и Y проанализирована нами с применением корреляционно-регрессионного анализа и построением уравнения парной линейной регрессии (см. [12]). С помощью специальных инструментов программы Excel рассчитаны коэффициенты уравнения парной линейной регрессии, коэффициент парной линейной корреляции, а также определены параметры, характеризующие значимость всего уравнения и его коэффициентов.

Получено значение коэффициента парной линейной корреляции r_{xy}, равное –0,71,

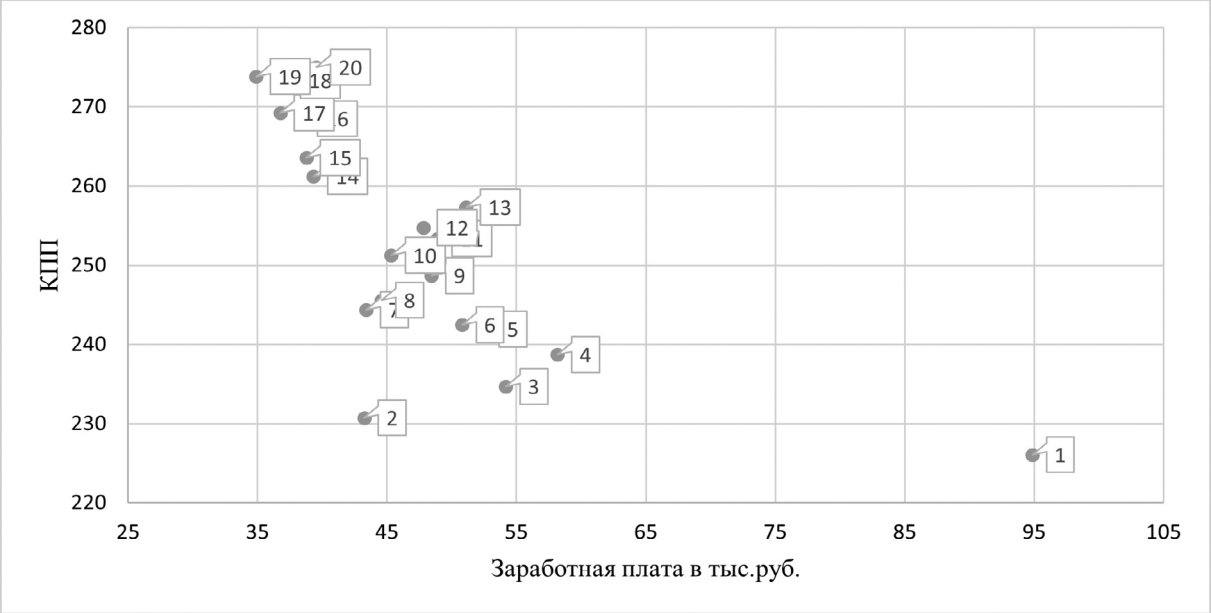

Рис. 1. Первичные статистические данные о заработной плате и КПП в регионах России (в поле диаграммы цифрами указаны номера регионов из табл. 2—4)

что, согласно таблице Чеддока[4], позволило охарактеризовать связь между переменными как значительную обратную.

Зависимость между заработной платой и КПП в регионе можно представить в виде уравнения регрессии:

$$Y = a + bX_1. \qquad (2)$$

Для нахождения коэффициентов a и *b* уравнения регрессии нами был использован метод наименьших квадратов (МНК). Найденные коэффициенты a и *b* уравнения парной линейной регрессии соответственно равны 292 и –0,82, отсюда $Y = 292 - 0{,}82X_1$.

Проведенный по отношению выборочных дисперсий тест Фишера (значимости уравнения регрессии при уровне значимости 0,05) показал, что уравнение статистически значимо, так как расчетное значение параметра *F* на данной выборке $F_{\text{набл.}} = 18{,}54$, что значительно меньше критического ($F_{\text{крит.}} = 4{,}38$).

Далее с целью оценить значимость показателей уравнения регрессии, позволившего с вероятностью 95 % охарактеризовать зависимость между показателями, применен *t*-критерий Стьюдента с расчетом доверительных интервалов для обоих показателей. О статистической значимости коэффициентов регрессии говорит низкий уровень *p*-значений каждого из них. Поясним: если *p*-значение меньше 0,05, с вероятностью 0,95 можно считать, что соответствующий коэффициент модели значим (т. е. его нельзя считать равным нулю и эндогенная переменная *Y* значимо зависит от соответствующего фактора *X*).

В нашем случае можно констатировать, что оба коэффициента *a* и *b* уравнения регрессии (2) статистически значимо влияют на эндогенную переменную *Y* и между переменными X_1 и *Y* существует значимая линейная связь.

Таким образом, подтвердилась гипотеза H_1: средняя заработная плата по региону оказывает статистическое влияние на КПП.

Интерпретируем каждый из коэффициентов уравнения (2). По значению коэффициента *b* можно судить об изменении значения зависимой переменной *Y* в случае, когда значение переменной X_1 изменится на одну единицу.

[4] См., напр.: Структурная трансформация региональной экономики: монография / Т. В. Ускова, Е. В. Лукин, Е. Г. Леонидова и др. Вологда: Вологодский научный центр РАН, 2020. С. 121.

Так, если средняя заработная плата в регионе увеличится на 10 000 руб., прогнозное снижение КПП, согласно уравнению регрессии, составит около 8,2, и это значение сильно скажется на абсолютном числе пострадавших: вызовет его уменьшение.

Влияние уровня безработицы в регионе на КПП. Мы предполагаем, что безработный как не имеющий постоянного источника доходов более подвержен психологическому воздействию со стороны мошенников. Это объясняется следующим: во-первых, жажда легких и быстрых денег нередко свойственна людям, находящимся в затруднительном материальном положении (безработным, малоимущим, студентам, пенсионерам, людям с ограниченными физическими возможностями), а мошенники часто пользуются их социальной уязвимостью, обещая потенциальным жертвам высокие доходы в кратчайшие сроки. Во-вторых, по данным Министерства труда и социальной защиты РФ, до 51 % безработных не имеют профессионального образования[5], что может свидетельствовать об их более низкой цифровой грамотности по сравнению с людьми, получившими профессиональное образование и коммуницирующими в профессиональных кругах с коллегами (такие неформальные коммуникации повышают уровень осведомленности о сценариях мошенничества и дают возможность обмениваться опытом борьбы с подобными проблемами). В-третьих, отсутствие работы высвобождает много времени, которое безработный не всегда правильно использует (например, постоянно пребывает в социальных сетях, на сайтах знакомств, платформах бесплатных объявлений и т. д.), что создает благоприятную почву для осуществления мошенниками действий оппортунистического характера.

Статистические гипотезы H_0 и H_1 формулируются следующим образом:

– нулевая гипотеза H_0: уровень безработицы не оказывает статистически значимого влияния на КПП;

– альтернативная гипотеза H_1: уровень безработицы оказывает статистическое влияние на КПП.

В качестве независимой переменной X_2 нами принято число безработных на 1000 человек населения, а в качестве зависимой переменной Y — КПП (табл. 4).

Таблица 4

Первичные статистические данные о числе безработных и КПП в регионах России в 2023 г.

Регион	Число безработных, на 1000 чел.	КПП
1. Мурманская область	45	226
2. Республика Крым	41	230
3. Краснодарский край	32	234
4. Тюменская область (без а/о)	16	238
5. Новгородская область	27	241
6. Ростовская область	34	242
7. Псковская область	38	244
8. Республика Адыгея	41	245

[5] Минтруд и ВНИИ труда составили «портрет безработного» [Электронный ресурс] // Минтруд России: [официальный сайт]. 31.08.2020. URL: https://mintrud.gov.ru/employment/67 (дата обращения: 30.05.2024).

Таблица 4 (Продолжение)

Регион	Число безработных, на 1000 чел.	КПП
9. Курганская область	58	248
10. Ставропольский край	45	251
11. Г. Севастополь	40	253
12. Волгоградская область	32	254
13. Астраханская область	67	257
14. Республика Тыва	80	261
15. Карачаево-Черкесская Республика	102	263
16. Кабардино-Балкарская Республика	98	268
17. Республика Калмыкия	110	269
18. Ивановская область	116	273
19. Алтайский край	284	273
20. Республика Северная Осетия — Алания	119	274

Источник: официальные данные Росстата (Доклад «Социально-экономическое положение России» [Электронный ресурс]. 2023 г. // Федеральная служба государственной статистики: [сайт]. URL: https://rosstat.gov.ru/compendium/document/50801 (дата обращения: 30.05.2024).)

Зависимость между переменными X_2 и Y снова проанализирована выбранным методом корреляционно-регрессионного анализа и построением уравнения парной линейной регрессии.

Получено значение коэффициента парной линейной корреляции r_{xy}, равное 0,73, что, согласно таблице Чеддока, позволило охарактеризовать связь между переменными как значительную прямую.

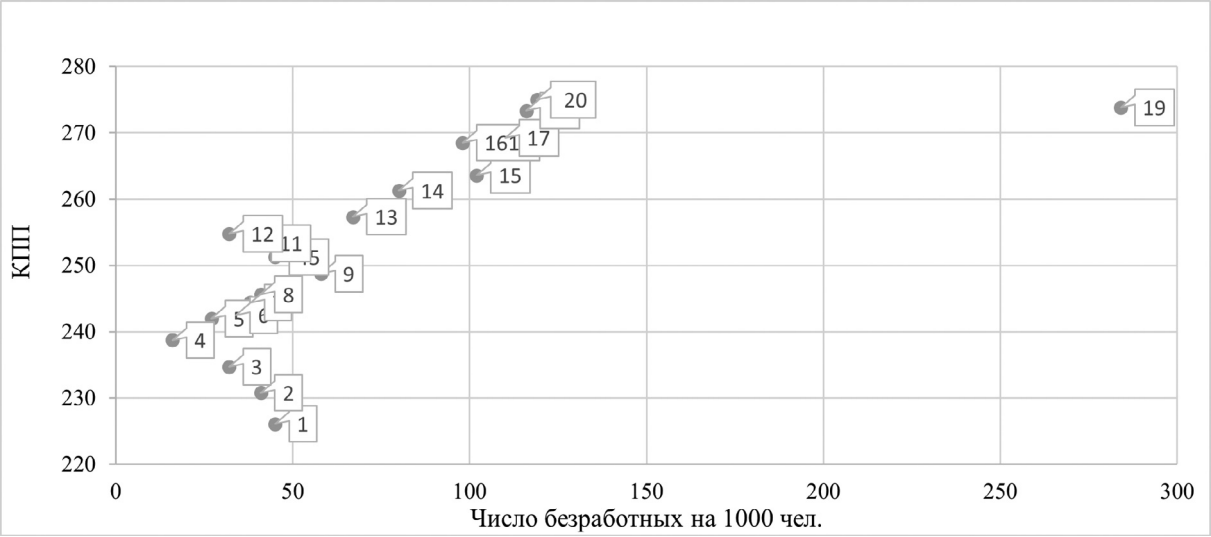

Рис. 2. Зависимость между КПП и числом безработных (на 1000 чел. населения) по регионам России (в поле диаграммы цифрами указаны номера регионов из табл. 2—4)

Зависимость между уровнем безработицы и КПП в регионе можно представить в виде уравнения регрессии:

$$Y = a + bX_2. \quad (3)$$

Найденные с помощью МНК коэффициенты a и *b* уравнения парной линейной регрессии соответственно равны 240 и 0,18. Подставив их в уравнение (3), получим: $Y = 240 + 0{,}18X_2$.

Проведенный по отношению выборочных дисперсий тест Фишера показал, что это уравнение, так же как и уравнение (2), статистически значимо, потому что расчетное значение параметра *F* на данной выборке $F_{\text{набл.}} = 19{,}39$, что значительно больше табличного параметра ($F_{\text{крит.}} = 4{,}38$).

При оценке значимости показателей уравнения регрессии (3) мы применили *t*-критерий Стьюдента с расчетом доверительных интервалов для обоих показателей уравнения и, получив снова низкие *p*-значения, убедились в статистической значимости обоих показателей.

На этом основании можно утверждать, что между переменными X_2 и *Y* существует значимая линейная связь, а оба коэффициента a и *b* уравнения регрессии статистически значимо влияют на эндогенную переменную *Y*.

Поясним смысл каждого из коэффициентов уравнения (3).

Если, например, число безработных (на 1000 человек населения) в регионе увеличится на 10 человек, это приведет, согласно уравнению регрессии, к увеличению КПП на 1,8 единицы, и соответственно существенно увеличится общее число преступлений.

Таким образом, нашла подтверждение гипотеза H_1: уровень безработицы оказывает статистическое влияние на КПП.

Выводы

Резюмируя изложенное, обращаем внимание общественности и академических кругов на остроту и сложность проблемы прогрессирующего роста случаев мошенничества с использованием методов и техник социальной инженерии в цифровом пространстве. Самую большую угрозу действия мошенников представляют для социально уязвимых слоев населения: малоимущих, безработных и т. п., что подтверждается результатами нашего исследования. Мошенничество как разновидность атаки социальной инженерии на рядовых россиян ежедневно совершенствуется с использованием всего арсенала передовых информационных технологий. В целях нивелирования данной проблемы необходимо объединить усилия государства, бизнеса и гражданского общества в борьбе с кибермошенничеством. *Пользователям цифровых технологий* рекомендуется следующее: никогда не переходить по ссылкам, полученным из электронных писем и сообщений от неизвестных отправителей и не открывать вложения; не вводить персональные данные при переходе на подозрительный сайт; не отвечать на спам-сообщения и послания от лиц с фейковыми страницами в социальных сетях; использовать антивирусное программное обеспечение и инструменты многофакторной аутентификации для всех учетных записей; производить регулярный контроль онлайн-аккаунтов, банковских счетов и кредитных профилей; осуществлять резервное копирование важной информации, содержащейся на компьютере или в смартфоне; не вступать в вербальный контакт по телефону с лицами, представляющимися сотрудниками различных государственных структур, банков, операторов сотовой связи и пр.; не вносить предоплату за товары и услуги без предварительной проверки аутентичности сайта продавца и изучения отзывов и комментариев о его деятельности. *Организациям* следует проводить с сотрудниками беседы, повышающие финансовую грамотность, с привлечением психологов и специалистов по информационным технологиям.

Важнейшая роль в борьбе с кибермошенничеством принадлежит *государству* как

единственному легитимному источнику инфорсмента[6]. Эффективным государственным институтом, на наш взгляд, должна стать киберполиция, создание которой представляется нам первоочередной задачей в борьбе с мошенничеством в цифровом пространстве.

Список литературы и источников

1. ***Бекарев А. М., Плотников М. В.*** Проблемы социальной инженерии // Личность. Культура. Общество. 2012. Т. 14. № 1. С. 219—227. EDN: OUPPBT.
2. ***Кавеева А. Д., Гурин К. Е.*** Искусственные профили «ВКонтакте» и их влияние на социальную сеть пользователей // Журнал социологии и социальной антропологии. 2018. Т. 21. № 2. С. 214—231. https://doi.org/10.31119/ jssa.2018.21.2.8 EDN: XZOGHB.
3. ***Ламинина О. Г.*** Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. 2017. № 2. С. 21—23. EDN: YFNAWP.
4. ***Парфёнова И. А., Пекарская О. А.*** Основные концепции информационной защиты // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сб. науч. ст. XII Междунар. науч.-техн. и науч.-метод. конф. (С.-Петербург, 28 февр. — 01 мар. 2023): в 4 т. / под ред. С. И. Макаренко; сост. В. С. Елагин, Е. А. Аникевич. Т. 2. СПб.: СПбГУТ им. М. А. Бонч-Бруевича, 2023. С. 833—837. EDN: OBWAEF.
5. ***Равочкин Н. Н.*** Идея как инструмент социальной инженерии: философский анализ // Социодинамика. 2019. № 12. С. 237—255. https://doi.org/10.25136/2409-7144.2019.12.31237 EDN: IXWAYP.
6. ***Ревенков П. В., Бердюгин А. А.*** Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. № 9 (354). С. 1747—1760. https://doi.org/10.24891/ni.13.9.1747 EDN: WTCYWU.
7. ***Резник Ю. М.*** Социальная инженерия: предметная область и границы применения // Социологические исследования. 1994. № 2. С. 87—95.
8. ***Стрижак А. Ю.*** Контагиозность оппортунизма в киберпространстве: тенденции и пути нивелирования // Новое в экономической кибернетике. 2020. № 3-4. С. 346—353. EDN: QAQHUB.
9. ***Стрижак А. Ю.*** Оппортунистическое поведение в киберпространстве: новый вызов пандемии // Вестник ДонНУ. Сер. В. Экономика и право. 2020. № 3. С. 184—189. EDN: RMRQQB.
10. ***Стрижак А. Ю., Пекарская О. А.*** Проблемы социальной инженерии в киберпространстве: региональный аспект // Инновационная парадигма экономических механизмов хозяйствования: сб. науч. тр. IX Междунар. науч.-практ. конф. (Симферополь, 15 мая 2024). Симферополь: Тип. «Ариал», 2024. С. 621—623. EDN: JHJJKB.
11. ***Уржа О. А.*** Социальная инженерия как методология управленческой деятельности // Социологические исследования. 2017. № 10 (402). С. 87—96. https://doi.org/10.7868/ S0132162517100099 EDN: ZNGYKL.
12. Экономико-математические подходы к исследованию банковской системы России / В. Д. Никифорова, М. Ю. Волокобинский, А. А. Никифоров, О. А. Пекарская // Технологическая перспектива в рамках Евразийского пространства: Новые рынки и точки экономического роста: материалы 4-й Междунар. науч. конф. (С.-Петербург, 13—15 дек. 2018) / под ред. О. Н. Кораблевой и др. СПб.: ЦНИТ «Астерион», 2018. С. 248—253. EDN: QWJPNF.
13. ***Bhusal Ch. S.*** Systematic review on social engineering: Hacking by manipulating humans // Journal of Information Security. 2021. Vol. 12. No. 1. P. 104—114. https://doi.org/10.4236/jis.2021.121005
14. ***Cialdini R.*** Influence: The Psychology of Persuasion. New York: Harper Collins, 2006. 336 p.
15. Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy / P. Lawson, C. J. Pearson, A. Crowson, C. B. Mayhorn // Applied Ergonomics. 2020. Vol. 86. Art. ID: 103084. https://doi.org/10.1016/j.apergo.2020.103084
16. ***Heartfield R., Loukas G.*** A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks // ACM Computing Surveys. 2015. Vol. 48. Iss. 3. P. 1—39. https://doi.org/10.1145/2835375

[6] См., напр.: ***Радыгин А., Энтов Р., Межераупс И.*** Проблемы правоприменения (инфорсмента) в сфере защиты прав акционеров. М.: Ин-т экономики переходного периода, 2002. С. 5.

17. ***Kaul P., Sharma D.*** Study of automated social engineering, its vulnerabilities, threats and suggested countermeasures // International Journal of Computer Applications. 2013. Vol. 67. No. 7. P. 13—16. https://doi.org/10.5120/11406-6726
18. ***Manske K.*** An introduction to social engineering // Information Systems Security. 2000. Vol. 9. Iss. 5. P. 53—59. https://doi.org/10.1201/1086/43312.9.5.20001112/31378.10
19. ***Mouton F., Leenen L., Venter H. S.*** Social engineering attack examples, templates and scenarios // Computers & Security. 2016. Vol. 59. P. 186—209. https://doi.org/10.1016/j.cose.2016.03.004
20. ***Parhi K., Pietikainen P.*** Socialising the anti-social: Psychopathy, psychiatry and social engineering in Finland, 1945—1968 // Social History of Medicine. 2017. Vol. 30. Iss. 3. P. 637—660. https://doi.org/10.1093/shm/hkw093
21. ***Roberts J. C. II, Al-Hamdani W.*** Who can you trust in the cloud? A review of security issues within cloud computing // Proceedings of the 2011 Information Security Curriculum Development Conference. New York: ACM, 2011. P. 15—19. https://doi.org/10.1145/2047456.2047458
22. Social engineering attacks on the knowledge worker / K. Krombholz, H. Hobel, M. Huber, E. Weippl // Proceedings of the 6th International Conference on Security of Information and Networks. New York: ACM, 2013. P. 28—35. https://doi.org/10.1145/2523514.2523596
23. The persuasion and security awareness experiment: Reducing the success of social engineering attacks / J.-W. Bullée, L. Montoya, W. Pieters et al. // Journal of Experimental Criminology. 2015. Vol. 11. P. 97—115. https://doi.org/10.1007/s11292-014-9222-7

References

1. Bekarev A. M., Plotnikov M. V. "Problems of Social Engineering". *Lichnost'. Kul'tura. Obshchestvo = Personality. Culture. Society* 14.1 (2012): 219—227. (In Russian). EDN: OUPPBT.
2. Kaveyeva A., Gurin K. " 'VKontakte' Fake Accounts and Their Influence on the Users' Social Network". *Zhurnal sotsiologii i sotsialnoy antropologii = The Journal of Sociology and Social Anthropology* 21.2 (2018): 214—231. (In Russian). https://doi.org/10.31119/jssa.2018.21.2.8 EDN: XZOGHB.
3. Laminina O. G. "Possibilities of Social Engineering in Information Technologies". *Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki = Humanities, Socio-Economic and Social Sciences* 2 (2017): 21—23. (In Russian). EDN: YFNAWP.
4. Parfenova I., Pekarskaya O. "Basic Concepts of Information Security". *Aktual'nyye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2023): sb. nauch. st. XII Mezhdunar. nauch.-tekhn. i nauch.-metod. konf.* (S.-Peterburg, 28 fevr. — 01 mar. 2023). Ed. by S. I. Makarenko, comp. V. S. Elagin, E. A. Anikevich. Vol. 2. St. Petersburg: SPbSUT n. a. M. A. Bonch-Bruyevich, 2023. 833—837. (In Russian). EDN: OBWAEF. 4 vols.
5. Ravochkin N. N. "Idea as an Instrument of Social Engineering: Philosophical Analysis". *Sotsiodinamika = Sociodynamics* 12 (2019): 237—255. (In Russian). https://doi.org/10.25136/2409-7144.2019.12.31237 EDN: IXWAYP.
6. Revenkov P. V., Berdyugin A. A. "Social Engineering as a Source of Risks in Online Banking Services". *Natsional'nyye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security* 13.9 (354) (2017): 1747—1760. (In Russian). https://doi.org/10.24891/ni.13.9.1747 EDN: WTCYWU.
7. Reznik Yu. M. "Social Engineering: Subject Area and Boundaries of Application". *Sotsiologicheskiye issledovaniya = Sociological Studies* 2 (1994): 87—95. (In Russian).
8. Strizhak A. "The Contagiousness of Opportunism in Cyberspace: Trends and Ways of Leveling". *Novoye v ekonomicheskoy kibernetike = New in Economic Cybernetics* 3-4 (2020): 346—353. (In Russian). EDN: QAQHUB.
9. Strizhak A. "Opportunist Behavior in Cyberspace: A New Pandemic Challenge". *Vestnik DonNU. Ser. V. Ekonomika i pravo = Bulletin of Donetsk National University. Series V. Economics and Law* 3 (2020): 184—189. (In Russian). EDN: RMRQQB.
10. Strizhak A. Yu., Pekarskaya O. A. "Problems of Social Engineering in Cyberspace: Regional Aspect". *Innovatsionnaya paradigma ekonomicheskikh mekhanizmov khozyaystvovaniya: sb. nauch. tr. IX Mezhdunar. nauch.-prakt. konf.* (Simferopol', 15 maya 2024). Simferopol: Tip. "Arial", 2024. 621—623. (In Russian). EDN: JHJJKB.
11. Urzha O. A. "Social Engineering as Methodology of Management Activity". *Sotsiologicheskiye issledovaniya = Sociological Studies* 10 (402) (2017): 87—96. (In Russian). https://doi.org/ 10.7868/ S0132162517100099 EDN: ZNGYKL.

12. Nikiforova V. D., Volokobinskiy M. Yu., Nikiforov A. A., Pekarskaya O. A. "Economic and Mathematical Approaches to the Investigation on the Russian Banking System". *Tekhnologicheskaya perspektiva v ramkakh Evraziyskogo prostranstva: Novyye rynki i tochki ekonomicheskogo rosta: materialy 4-y Mezhdunar. nauch. konf.* (S.-Peterburg, 13—15 dek. 2018). Ed. by O. N. Korableva et al. St. Petersburg: TsNIT "Asterion", 2018. 248—253. (In Russian). EDN: QWJPNF.
13. Bhusal Chandra S. "Systematic Review on Social Engineering: Hacking by Manipulating Humans". *Journal of Information Security* 12.1 (2021): 104—114. https://doi.org/10.4236/jis.2021.121005
14. Cialdini Robert. *Influence: The Psychology of Persuasion*. New York: Harper Collins, 2006. 336 p.
15. Lawson Patrick, Pearson Carl J., Crowson Aaron, Mayhorn Christopher B. "Email Phishing and Signal Detection: How Persuasion Principles and Personality Influence Response Patterns and Accuracy". *Applied Ergonomics* 86 (2020): 103084. https://doi.org/10.1016/j.apergo.2020.103084
16. Heartfield Ryan, Loukas George. "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks". *ACM Computing Surveys* 48.3 (2015): 1—39. https://doi.org/10.1145/2835375
17. Kaul Priya, Sharma Deepak. "Study of Automated Social Engineering, Its Vulnerabilities, Threats and Suggested Countermeasures". *International Journal of Computer Applications* 67.7 (2013): 13—16. https://doi.org/10.5120/11406-6726
18. Manske Kurt. "An Introduction to Social Engineering". *Information Systems Security* 9.5 (2000): 53—59. https://doi.org/10.1201/1086/43312.9.5.20001112/31378.10
19. Mouton François, Leenen Louise, Venter H. S. "Social Engineering Attack Examples, Templates and Scenarios". *Computers & Security* 59 (2016): 186—209. https://doi.org/10.1016/j.cose.2016.03.004
20. Parhi Katariina, Pietikainen Petteri. "Socialising the Anti-Social: Psychopathy, Psychiatry and Social Engineering in Finland, 1945—1968". *Social History of Medicine* 30.3 (2017): 637—660. https://doi.org/10.1093/ shm/hkw093
21. Roberts John C. II, Al-Hamdani Wasim. "Who Can You Trust in The Cloud? A Review of Security Issues Within Cloud Computing". *Proceedings of the 2011 Information Security Curriculum Development Conference*. New York: ACM, 2011. 15—19. https://doi.org/10.1145/2047456.2047458
22. Krombholz K., Hobel H., Huber M., Weippl E. "Social Engineering Attacks on the Knowledge Worker". *Proceedings of the 6th International Conference on Security of Information and Networks*. New York: ACM, 2013. 28—35. https://doi.org/10.1145/2523514.2523596
23. Bullée Jan-Willem H., Montoya Lorena, Pieters Wolter, Junger Marianne, Hartel Pieter H. "The Persuasion and Security Awareness Experiment: Reducing the Success of Social Engineering Attacks". *Journal of Experimental Criminology* 11 (2015): 97—115. https://doi.org/10.1007/s11292-014-9222-7

Информация об авторах

Стрижак Анна Юрьевна — доктор экономических наук, заведующая кафедрой менеджмента, Национальный открытый институт г. Санкт-Петербург (Россия, 197183, Санкт-Петербург, ул. Сестрорецкая, 6).

Пекарская Ольга Анатольевна — кандидат экономических наук, доцент кафедры высшей математики и системного моделирования сложных процессов, Санкт-Петербургский университет ГПС МЧС России (Россия, 196105, Санкт-Петербург, Московский пр-т, 149).

Information about the authors

Anna Yu. Strizhak — Dr. Sci. (Econ.), Head of the Department of Management, National Open Institute Saint-Petersburg (Russia, 197183, St. Petersburg, Sestroretskaya st., 6).

Olga A. Pekarskaya — Cand. Sci. (Econ.), Associate Professor at the Department of Higher Mathematics and System Modeling of Complex Processes, Saint-Petersburg University of State Fire Service of EMERCOM of Russia (Russia, 196105, St. Petersburg, Moskovsky ave., 149).

Статья поступила в редакцию 17.03.2024.

The article was submitted 17.03.204.