MATHEMATICAL MODELING OF THE USER'S DECISION-MAKING PROCESS UNDER THE INFLUENCE OF SOCIAL ENGINEERING METHODS

Marinov A.
PhD in Economic Sciences, associate Professor at the Cybersecurity Competence Center, Irkutsk National ResearchTechnical University, Irkutsk, Russia
Larionova L.
PhD in Pedagogical Sciences, associate Professor at the Cybersecurity Competence Center, Irkutsk National ResearchTechnical University, Irkutsk, Russia

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРИНЯТИЯ РЕШЕНИЙ ПОЛЬЗОВАТЕЛЕМ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Маринов А.А.
кандидат экономических наук, доцент центра компетенций по кибербезопасности, ФГБОУ ВО «Иркутский национальный исследовательский технический университет», г. Иркутск, Россия.
Ларионова Л.А.
кандидат педагогических наук, доцент центра компетенций по кибербезопасности, ФГБОУ ВО «Иркутский национальный исследовательский технический университет», г. Иркутск, Россия.
https://doi.org/10.5281/zenodo.21649102

Abstract

In this article, we present a mathematical modeling approach to examining user decisionmaking processes under attack by social engineering.

The relevance of this study stems from the increasing number of attacks on individuals and the increasing sophistication of these attacks, which rely on psychological and behavioral influence. Fraudsters exploit trust, urgency, authority, curiosity, greed, and cognitive overload to induce users to make erroneous decisions. We propose a probabilistic model that formalizes the relationship between these influence parameters and the likelihood of making a dangerous decision. Key variables include the level of trust in the message source, perceived urgency, cognitive load, user experience, ability to recognize risk signs, and the intensity of the manipulative influence. The results demonstrate that the use of mathematical modeling enables quantitative assessment of user vulnerability, refinement of preventative training, and improvement of the effectiveness of organizational security measures.

Аннотация

В статье мы представляем рассмотрение процесса принятия пользователем решений в ситуациях воздействия на него злоумышленниками с использованием методов социальной инженерии с помощью математического моделирования.

Актуальность исследования обусловлена тем, что постоянно увеличивается не только количество атак на человека со стороны злоумышленников, но и растет их изощренность, основанная на психологическом и поведенческом воздействии, при которых мошенники используют доверие, срочность, авторитет, любопытство, жадность и когнитивную перегрузку для побуждения пользователя к ошибочному принятию решений. Мы предлагаем вероятностную модель, позволяющую формализовать зависимость между параметрами воздействия и вероятностью принятия опасного решения. В качестве ключевых переменных нами рассматривается уровень доверия к источнику сообщения, степень воспринимаемой срочности, когнитивная нагрузка, опыт пользователя, способность распознавать признаки риска и интенсивность манипулятивного воздействия. Полученные результаты показывают, что использование математического аппарата дает возможность количественно оценивать уязвимость пользователя, уточнять направления профилактического обучения и повышать эффективность организационных мер защиты.

Keywords: social engineering; information security; decision-making; mathematical modeling; probabilistic model; behavioral risks; user vulnerability.

Ключевые слова: социальная инженерия; информационная безопасность; принятие решений; математическое моделирование; вероятностная модель; поведенческие риски; уязвимость пользователя.

Введение

Методы социальной инженерии в современном обществе используются часто, так как позволяют эффективно несанкционированно воздействовать на пользователей в цифровом пространстве. Их особенность состоит в том, что атака направлена не на техническую защиту, которая постоянно совершенствуется, а на когнитивную, эмоциональную и поведенческую сферу человека, используя его уязвимости. Делая ставку именно на человеческий фактор, злоумышленник пытается обходить систему обеспечения информационной безопасности, и получает доступ через пользователя к конфиденциальным сведениям, учетным данным и внутренним ресурсам организации.

Актуальность исследования определяется тем, что атаки социальной инженерии строятся на мани-

пулятивных процессах воздействия на пользователя, побуждая его к принятию ошибочных решений. В условиях информационного давления, дефицита времени и перегрузки внимания пользователь может принять решение, не соответствующее требованиям безопасности. Следовательно, исследование механизмов и закономерностей таких процессов требует не только качественного описания, но и формализации в математической форме. Вероятностный подход в данном случае является наиболее оправданным, поскольку отражает неоднозначность человеческого поведения и зависимость результата от совокупности внешних и внутренних факторов [1].

Целью настоящей статьи является разработка математической модели процесса принятия решений пользователем в условиях воздействия методов социальной инженерии. Для достижения указанной цели были выдвинуты задачи:

1. Проанализировать основные механизмы социальной инженерии;
2. Определить значимые параметры поведения пользователя;
3. Формализовать зависимость между воздействующими факторами и вероятностью ошибочного решения; рассматриваются
4. Описать возможности практического применения модели в задачах информационной безопасности.

Объектом исследования является процесс принятия решений пользователем в условиях информационно-психологического воздействия.

Предметом исследования выступают математические зависимости, описывающие влияние методов социальной инженерии на вероятность совершения небезопасного действия.

Методологическую основу составляют методы математического моделирования, логистической регрессии, вероятностного анализа и системного подхода к исследованию поведенческих рисков.

Теоретические основы

Социальная инженерия – совокупность методов воздействия на человека через его психологические особенности. Схемы злоумышленников основываются на таких факторах, как использование авторитета, создание условий цейтнота, эксплуатация чувства страха, построение резонансных отношений, создание дефицита информации и оказание директивного социального давления. Такие приёмы манипулятивного воздействия ориентированы на снижение критичности мышления, затруднение конструктивной оценки и тем самым, искусственное ускорение процесса принятия решения. Это создаёт условия, при которых пользователь может совершить действие, идентифицируемое как небезопасное при более взвешенном подходе [2].

В рамках поведенческой модели принятие решения в ситуациях социальной инженерии формализуется как стохастический процесс, зависящий от множества факторов. В их число включаются: уровень доверия к источнику, фактор срочности, объём потребляемых когнитивных ресурсов, текущая осведомлённость пользователя, ретроспективный опыт взаимодействия с угрозами и способность к идентификации риск-индикаторов. Первые три параметра при увеличении своих значений повышают вероятность небезопасного выбора; два последних, наоборот, обеспечивают её снижение [5].

Для адекватной формализации процесса целесообразно использовать модель ограниченной рациональности, постулирующую, что субъект решения действует в условиях неполноты информации и неопределённости. Это означает, что исход взаимодействия с атакующим не может быть описан детерминистически. Единственным корректным способом количественного выражения такого исхода является вероятность Q совершения ошибочного действия.

Постановка задачи

Опишем поведение пользователя в момент получения потенциально вредоносного сообщения вектором признаков [6].

$$x = (T, U, C, E, R, P). \quad (1)$$

Здесь:

$$T \in [0, 1] \quad (2)$$

уровень доверия к источнику сообщения;

$$U \in [0, 1] \quad (3)$$

степень воспринимаемой срочности;

$$C \in [0, 1] \quad (4)$$

когнитивная нагрузка;

$$E \in [0, 1] \quad (5)$$

уровень опыта и осведомленности пользователя;

$$R \in [0, 1] \quad (6)$$

способность распознавать признаки риска;

$$P \in [0, 1] \quad (7)$$

интенсивность психологического воздействия.

Тогда вероятность принятия небезопасного решения обозначим через

$$Q = \mathbb{P}(Y = 1 \mid x), \quad (8)$$

где $Y = 1$ означает совершение ошибочного действия, а $Y = 0$ – отказ от него.

Задача моделирования состоит в том, чтобы определить функциональную зависимость

$$Q = f(x), \quad (9)$$

которая позволяет количественно оценить вероятность ошибки в зависимости от параметров воздействия.

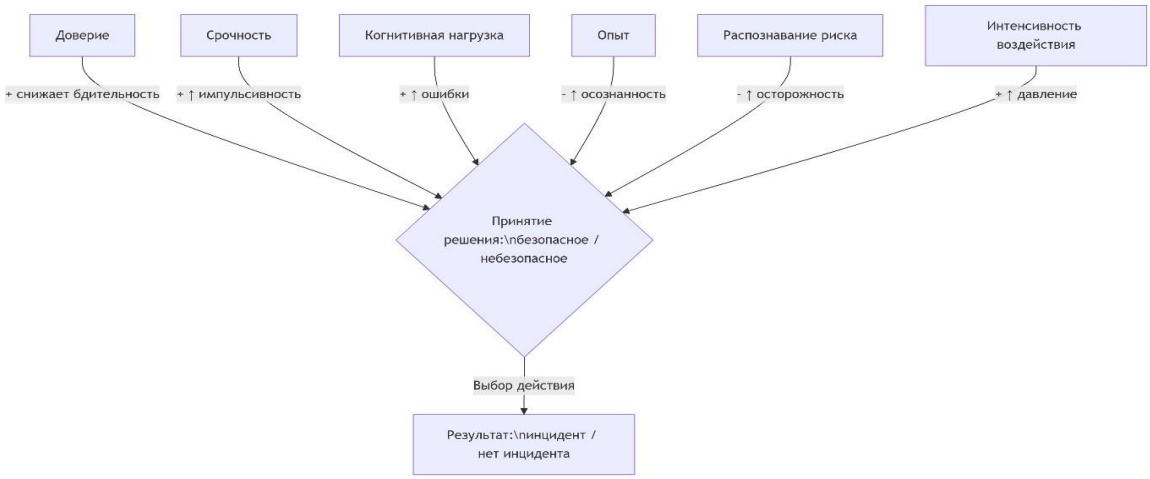

Рис.1. Концептуальная модель факторов, влияющих на принятие решения

Математическая модель

В качестве основной модели предлагается логистическая функция:

$$Q = \frac{1}{1 + e^{-Z}}, \quad (10)$$

где

$$Z = \beta_0 + \beta_1 T + \beta_2 U + \beta_3 C + \beta_4 P - \beta_5 E - \beta_6 R. \quad (11)$$

Здесь β_0 – свободный член, а β_i – параметры модели, характеризующие вклад соответствующих факторов в итоговую вероятность ошибочного решения.

Значения коэффициентов β_1, β_2, β_3 и β_4 имеют положительную направленность, что свидетельствует о прямой корреляции между увеличением соответствующих факторов и ростом вероятности небезопасного выбора. Можем предположить, чем выше степень доверия к источнику, острее ощущение срочности, значительнее когнитивная загрузка и интенсивнее внешнее манипулятивное давление, тем более вероятным становится ошибочное действие со стороны пользователя. В противоположность этому, коэффициенты β_5 и β_6 характеризуются отрицательными значениями, что отражает их защитную функцию: развитый опыт противодействия угрозам и сформированная способность к идентификации риск-индикаторов выступают в роли сдерживающих механизмов, снижающих вероятность компрометации.

Применение логистической функции в рамках разрабатываемой модели не является произвольным решением, а обусловлено её фундаментальными свойствами.

Во-первых, данная функция обеспечивает естественное ограничение результирующей вероятности в интервале [0; 1], что соответствует вероятностной природе описываемого процесса.

Во-вторых, она позволяет адекватно отразить плавный характер перехода между состояниями низкого и высокого риска. Данное свойство имеет принципиальное значение, поскольку реальное поведение человека в условиях информационного воздействия не демонстрирует скачкообразных изменений, за исключением крайне редких случаев.

Для учёта нелинейного характера некоторых видов манипулятивного воздействия в модель вводится дополнительный параметр θ, задающий критический уровень риска. Введение данного порога позволяет трансформировать вероятностную оценку в бинарную классификацию:

$$Y = \begin{cases} 1, & Q \geq \theta, \\ 0, & Q < \theta. \end{cases} \quad (12)$$

Подобное расширение модели придаёт ей дополнительную функциональность: помимо количественной оценки вероятности ошибочного действия, появляется возможность категоризировать ситуацию как безопасную или потенциально опасную, что существенно расширяет спектр практических приложений.

Интерпретация переменных

Переменная T (доверие к источнику). Данный параметр количественно отражает степень уверенности пользователя в добросовестности отправителя сообщения. В способах воздействия на человека злоумышленники используют доверие в качестве одного из наиболее эффективных инструментов подавления критического мышления. При маскировке под руководителя организации, представителя банка, сотрудника службы поддержки или знакомого лица значение T закономерно возрастает, что сопровождается снижением вероятности осуществления проверочных действий со стороны пользователя.

Параметр U (срочность). Указанная переменная фиксирует интенсивность временного давления, оказываемого на пользователя. Типичная тактика злоумышленника предполагает искусственное ограничение времени, отводимого на обдумывание, что создаёт ситуацию дефицита временных ресурсов. Повышение уровня срочности провоцирует переход к автоматизированным, рефлекторным действиям, минуя этап критической оценки поступающей информации.

Параметр C (когнитивная нагрузка). Данная переменная отражает объём информационной пере-

работки, одновременно осуществляемой пользователем. В условиях многозадачности, утомления или высокой интенсивности профессиональной деятельности способность к выявлению скрытых признаков угрозы существенно снижается, что увеличивает уязвимость перед атаками социальной инженерии.

Переменная E (опыт и осведомлённость). Данный параметр выступает в роли ключевого защитного механизма. Пользователи, обладающие релевантным опытом и прошедшие соответствующую подготовку, с большей вероятностью обращают внимание на нетипичные проявления атаки. При этом необходимо отметить, что даже высокие значения E не гарантируют абсолютной защищённости, особенно в условиях бесспорного воздействия.

Параметр R (способность распознавания рисков). Данная переменная характеризует развитость навыков идентификации индикаторов социальной инженерии. К числу таких индикаторов относятся: аномалии в адресе отправителя, стилистические несоответствия сообщения, нехарактерные для коммуниканта просьбы, использование нетипичных каналов взаимодействия и другие маркеры потенциальной угрозы.

Переменная P (интенсивность воздействия). Данный показатель аккумулирует совокупность манипулятивных приёмов, задействованных злоумышленником. Усиление воздействия достигается через применение эмоционально заряженной лексики, апелляцию к авторитетным фигурам, угрозы применения санкций или обещание необоснованных выгод. Возрастание P непосредственно коррелирует с увеличением степени влияния на принимаемое решение [13].

Практическое применение

Разработанная модель находит применение в задачах оценки уязвимости персонала в корпоративной сфере. На основе эмпирических данных представляется возможным определить числовые значения параметров β_i, что создаёт основу для прогнозирования вероятности ошибочных действий в различных сценариях. Особую ценность данный подход представляет при проектировании программ повышения осведомлённости персонала и проведении тестовых симуляций атак методом социальной инженерии [4].

Кроме того, модель открывает возможности для интеграции в системы поддержки принятия решений. В подобной конфигурации программное средство способно в автоматическом режиме оценивать уровень риска и инициировать предупредительные сигналы при превышении порогового значения Q. Реализация такого подхода способствует повышению эффективности превентивных мероприятий и сокращению вероятности успешных атак [10].

Весомый потенциал заложен также в применении модели для анализа инцидентов информационной безопасности. Выявление факторов, оказавших решающее влияние на момент совершения пользователем ошибки, предоставляет организации фактологическую основу для корректировки регламентной документации, инструктивных материалов и содержания обучающих курсов. Таким образом, модель выполняет не только диагностическую, но и регулятивно-управленческую функцию [7].

Апробация и эмпирическая верификация

Для подтверждения практической состоятельности предложенной модели необходима её проверка на эмпирическом материале. Источником таких данных могут выступать результаты анкетирования, лабораторные эксперименты, анализ итогов симуляционных атак социальной инженерии. Указанный подход согласуется с современной исследовательской методологией, рассматривающей поведение пользователя как объект экспериментального изучения в контексте когнитивных и поведенческих факторов.

В качестве эмпирической базы для верификации модели использованы данные о реакциях пользователей на сообщения, содержащие признаки срочности, авторитетного давления и скрытого манипулятивного воздействия. При этом оценка параметров модели проводится путем сопоставления наблюдаемой частоты небезопасных действий с расчетной вероятностью Q. Если значения модели статистически согласуются с результатами эксперимента, это позволяет сделать вывод о ее адекватности и практической применимости

[8].

Полученные в исследованиях социальной инженерии данные свидетельствуют о том, что уязвимость пользователя определяется не одним, а совокупностью факторов, связанных с контекстом, когнитивной нагрузкой и особенностями восприятия сообщения. Это соответствует структуре предложенной модели, в которой вероятность ошибочного решения является функцией нескольких переменных.

Таким образом, апробация модели позволяет не только подтверждает ее математическую состоятельность, но и показывает, что она согласуется с эмпирически установленными закономерностями поведения пользователей в условиях информационного воздействия.

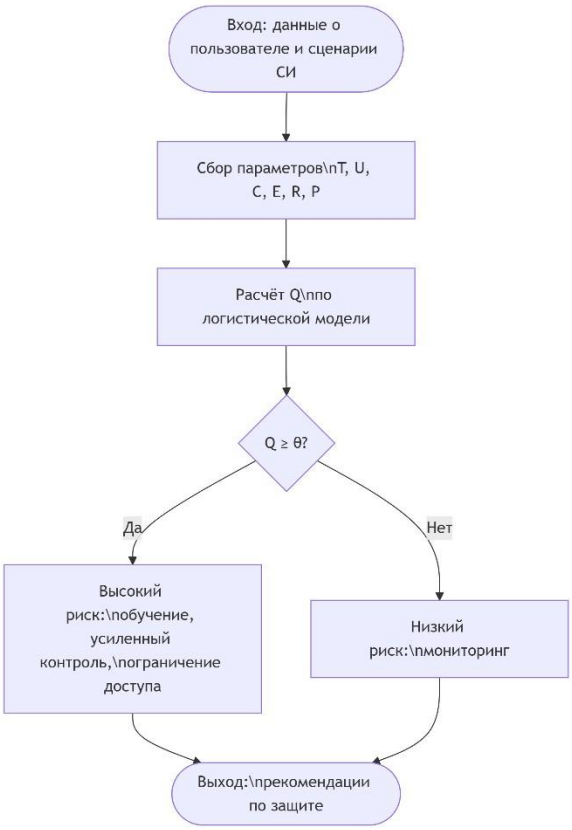

Рис.2. Алгоритм применения модели в системе оценки уязвимости

Обсуждение результатов

Проведенный анализ показывает, что процесс принятия решений пользователем в условиях социальной инженерии обладает выраженным вероятностным характером и зависит от совокупности взаимосвязанных факторов. Наиболее существенное влияние оказывают доверие к источнику, ощущение срочности и когнитивная нагрузка. В то же время опыт, осведомленность и способность распознавать риск выполняют защитную функцию, снижая вероятность ошибки [12].

Разработанная модель обеспечивает переход от сугубо качественного анализа угроз к формализованной количественной оценке, что приобретает особую значимость при решении следующих прикладных задач:

1.Сравнительный анализ различных сценариев манипулятивного воздействия;

2.Идентификация групп пользователей с повышенным уровнем уязвимости;

3.Оценка результативности реализуемых профилактических и обучающих мероприятий.

Применение вероятностного аппарата позволяет корректно учесть стохастическую природу человеческого поведения, что делает модель более адекватной по сравнению с упрощёнными детерминистическими конструкциями.

Вместе с тем необходимо признать, что представленная модель не претендует на исчерпывающую полноту. Поведенческий выбор пользователя детерминируется также комплексом дополнительных факторов, среди которых можно выделить: индивидуальнопсихологические характеристики личности; организационно-управленческий контекст; специфику используемого канала коммуникации; степень институционального доверия к конкретной информационной системе [9].

В связи с этим вектор дальнейших исследований должен быть направлен на расширение параметрического пространства модели и её эмпирическую валидацию на репрезентативных данных.

Заключение

Проведённое исследование позволяет сделать вывод о принципиальной возможности формализации процесса принятия решений пользователем в условиях социально-инженерных атак с использованием математического моделирования. В числе ключевых факторов, оказывающих наиболее существенное влияние на итоговый выбор, выделяются: уровень доверия к источнику информации, воспринимаемая срочность запроса, актуальная когнитивная загрузка, ретроспективный опыт пользователя, развитость навыков идентификации рисков и интенсивность применяемого манипулятивного воздействия.

Логистическая спецификация модели предоставляет возможность количественного измерения вероятности ошибочного действия и соразмерного учёта неоднозначности поведенческих реакций человека [11]. Указанный подход согласуется с современной методологией моделирования сложных социально-поведенческих феноменов.

С практической точки зрения, разработанный инструментарий может быть использован для:

1.Оценки индивидуальной и групповой уязвимости персонала в информационной безопасности;

2.Проектирования целевых программ повышения осведомлённости персонала; 3.Совершенствования организационно-управленческих мер защиты информации.

В качестве перспективных направлений дальнейших исследований рассматриваются эмпирическая верификация модели, уточнение её параметров на основе экспериментальных данных, а также включение дополнительных переменных, отражающих личностные особенности пользователей и контекстуальные характеристики коммуникационного взаимодействия.

Список литературы:

1. Калачева, Д. А. Социальная инженерия: методы защиты от фишинга и социальной инженерии / Д. А. Калачева, В. Р. Иванова // Цифровые системы и модели: теория и практика проектирования, разработки и использования : материалы международной научно-практической конференции (Казань, 10–11 апреля 2025 года). – Казань: Казанский государственный энергетический университет, 2025. – С. 2153–2157. – EDN LXXQXB.

2. Кузнецов, М. Социальная инженерия и социальные хакеры / М. Кузнецов, И. Симдянов. – Санкт-Петербург: БХВ-Петербург, 2007. – 368 с. – ISBN 5-94157-929-2. – EDN SDSLAJ.

3. Мадилян, Д. Е. Методы защиты информации от социальной инженерии / Д. Е. Мадилян // Государственное и административное управление в России: история и современность, цифровизация, инновации, интеллект. Молодёжный взгляд: материалы Всероссийской научно-практической конференции студентов, магистрантов и аспирантов (Тула, 23 июня 2020 года). – Тула: ООО «Тульский полиграфист 1», 2020. – С. 318–321. – EDN SVVAHT.

4. Маркелов, В. К. Требования к моделям противодействия атакам социальной инженерии в социальных сетях с использованием претекстинга / В. К. Маркелов, А. Н. Привалов //

5. Современное программное обеспечение систем информационной безопасности и интеллектуальной поддержки управленческих решений : сборник научных статей аспирантов. –Москва: Московский финансово-юридический университет МФЮА, 2024. – С. 10–15. – EDN IGJAGT.

6. Назаренко, С. В. Максимизация институционального участия граждан – приоритетное направление социальной инженерии (теории) и проспективного социального контроля (практики) / С. В. Назаренко // Социальная инженерия: как социология меняет мир : материалы IX международной социологической Грушинской конференции (Москва, 20– 21 марта 2019 года) / отв. ред. А. В. Кулешова. – Москва: Всероссийский центр изучения общественного мнения, 2019. – С. 182–187. – EDN DJKHVQ.

7. Разработка математических моделей для информационной системы принятия решений в процессе управления активами // Вестник Сатбаевского университета. – 2021. – URL: https://vestnik.satbayev.university/index.php/journal/article/view/300 (дата обращения: 18.07.2026).

8. Селезнева, И. Е. Экономико-математическая модель организации системных исследований / И. Е. Селезнева // Автоматизация и дистанционное управление. – 2020. – Т. 81. – С. 1136–1148. – DOI: 10.1134/S0005117920060132.

9. Albladi, S. M. User characteristics that influence judgment of social engineering attacks in social networks / S. M. Albladi, G. R. S. Weir // Cybersecurity. – 2018. – Vol. 1, No. 1. – Article 8. – DOI: 10.1186/s13673-018-0128-7.

10. A two-layer model for coevolving opinion dynamics and collective decision-making in complex social systems // Chaos. – 2020. – Vol. 30, No. 8. – Article 083103. – DOI: 10.1063/5.0004787.

11. Breaching the human firewall: social engineering in phishing and spear-phishing emails // AIS eLibrary. – URL: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1097&context=acis2015 (дата обращения: 18.07.2026).

12. Lallodi, L. Cognition in social engineering empirical research: a systematic literature review / L. Lallodi [et al.] // ACM Computing Surveys. – 2024. – Vol. 56, No. 6. – Article 135. – DOI: 10.1145/3635149.

13. Phase transitions, KMS condition and decision making: an introductory model // Philosophical Transactions of the Royal Society A. – 2023. – DOI: 10.1098/rsta.2022.0377.

14. Rodrigues, A. J. Human cognition through the lens of social engineering cyberattacks / A. J. Rodrigues, M. V. de Almeida [et al.] // Frontiers in Psychology. – 2020. – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7554349/ (дата обращения: 18.07.2026).