КРАТКИЕ СООБЩЕНИЯ | SHORT REPORTS

Современная наука и инновации.
2023. № 4 (44). С. 145-151.
Modern Science and Innovations.
2023; 4(44):145-151.

ТЕХНИЧЕСКИЕ НАУКИ / TECHNICAL SCIENCE

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ / INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Научная статья / Original article

УДК 323
https://doi.org/10.37493/2307-910X.2023.4.16

Эдуард Альбертович Шайхулов
[Eduard A. Shaikhulov][1],
Александр Петрович Смирнов
[Aleksandr P. Smirnov][2],
Ольга Борисовна Болдина
[Olga B. Boldina][3*],
Геннадий Юрьевич Азаренко
[Gennadii Yu. Azarenko][4],
Ирина Юрьевна Благова
[Irina Yu. Blagova][5]

Современные методы обучения информационной безопасности

Modern methods of information security training

[1]Казанский инновационный университет им. В.Г. Тимирясова, г. Казань, Россия / Kazan Innovative University named after V.G. Timiryasov, Kazan, Russia
[2]Российский Государственный Аграрный Университет – МСХА им. К.А.Тимирязева, г. Москва, Россия / Russian State Agrarian University - Moscow Agricultural Academy named after K.A. Timiryazev, Moscow, Russia
[3]Санкт-Петербургский государственный морской технический университет, г. Санкт-Петербург, Россия / Saint Petersburg State Marine Technical University, Saint Petersburg, Russia
[4]Сибирский государственный университет науки технологий им. Академика М.Ф. Решетнева, г. Красноярск, Россия / Siberian State University of Science and Technology named after Academician M.F. Reshetnev, Krasnoyarsk, Russia
[5]Санкт-Петербургский Политехнический Университет Петра Великого, Санкт-Петербург, Россия / Peter the Great St. Petersburg Polytechnic University, Saint Petersburg, Russia

****Автор, ответственный за переписку: Ольга Борисовна Болдина, tristan5401@rambler.ru / Corresponding author: Olga B. Boldina, tristan5401@rambler.ru***

Аннотация. *В статье рассматриваются методы и инструменты обучения в области информационной безопасности. Основное внимание уделяется необходимости адаптации к современным вызовам в области ИТ, исследованию эффективности различных методов, а также способам их внедрения в крупных компаниях. Рассматриваются преимущества и ограничения как традиционных, так и новаторских подходов к обучению, включая онлайн-курсы, симуляции и игровые методы.*

Ключевые слова: информационная безопасность, методы обучения, онлайн-курсы, симуляции, ИТ-компании

Для цитирования: *Шайхулов Э. А., Смирнов А. П., Болдина О. Б., Азаренко Г. Ю., Благова И. Ю. Современные методы обучения информационной безопасности // Современная наука и инновации. 2023. № 4 (44). С. 145-151. https://doi.org/10.37493/2307-910X.2023.4.16*

Abstract. *This article explores methods and tools for training in the field of information security. The primary focus is on the need to adapt to modern challenges in the IT sector, examining the effectiveness of*

various methods, and ways of their implementation in large companies. Advantages and limitations of both traditional and innovative approaches to training are discussed, including online courses, simulations, and gamified methods.

Keywords: information security, training methods, online courses, simulations, IT companies

For citation: *Shaikhulov EA, Smirnov AP, Boldina OB, Azarenko GYu, Blagova IYu. Modern methods of information security training. Modern Science and Innovations. 2023;4(44):145-151. (In Russ.).* https://doi.org/10.37493/2307-910X.2023.4.16

Введение. В современном цифровом веке информационные технологии (ИТ) развиваются с потрясающей скоростью, что значительно упрощает повседневные задачи, от планирования расписания до покупок продуктов. В то же время, согласно отчетам [1, 2], количество кибератак увеличивается каждый год на 15%. Это приводит к значительным глобальным экономическим потерям, превышающим 400 миллиардов долларов в год [3] – за счет штрафов за утечку данных, потере доверия клиентов и других причин. В 2022 году в России за год было зафиксировано 403 атаки, что на 25% больше, чем за 2021 год [4]. При таком раскладе информационная безопасность (ИБ) становится критически важной не только для IT-компаний, но и для других сфер, включая оборонную, банковскую, производственную, строительную.

При этом, обычно причиной успеха кибератаки является не брешь в системе защиты, а неопытность сотрудников компании [3]. Традиционные методы обучения в области информационной безопасности, такие как лекции и семинары не всегда подходят для обучения ввиду быстрого изменения сферы ИТ. Недавние исследования показывают, что 70% профессионалов в области ИБ считают, что их организации нуждаются в более инновационных методах обучения, которые помогли бы сотрудникам лучше понимать, как реагировать на внештатные ситуации или запросы мошенников.

Таким образом, существует необходимость в разработке новых методик и инструментов для обучения сотрудников в области ИБ. Цель настоящего исследования — не только разобрать, какие подходы к обучению наиболее эффективны в настоящий момент, но также понять, как лучше адаптировать их к конкретным отраслям.

Материалы и методы исследований. Традиционные методы обучения в области ИБ, долгое время считались надежными и проверенными. Обычно обучение по ИБ проводится в организациях на регулярной основе и в общем формате: в виде заготовленной лекции от одного или нескольких специалистов из профильного отдела, рассказывающих материалы по готовой презентации. Однако теперь такие методы обучения становятся все менее актуальными. Причин этого несколько:

Темпы увеличения серьезности киберугроз: обучение, основанное на устаревших данных, быстро теряет свою актуальность. Традиционные методы обучения, особенно рассчитанные на широкую аудиторию, часто не могут обеспечить своевременное обновление содержания курсов, предупредить обо всех возможных угрозах, дать такой шаблон взаимодействия пользователя (сотрудника) с киберугрозами, чтобы полностью его обезопасить [5].

Отсутствие практики: традиционные лекции зачастую концентрируются на теории, не давая сотрудникам возможности получить реальную практику. Этот фактор значительно снижает эффективность традиционных методов обучения.

Отсутствие индивидуализации: все люди разные, и тот формат, который хорошо подошел одному человеку и дал ему полное понимание того, как корректно себя вести, может плохо сработать для другого. Причины могут быть разными – плохая способность воспринимать аудиальную информацию, усталость, параллельный звонок или встреча. Традиционные методы обычно игнорируют индивидуальные потребности и предпочитаемый стиль и время обучения слушателей.

Среди более современных методов обучения можно выделить онлайн-обучение, контролируемое ИИ; игровые методы; симуляцию – в виде круглых столов или тестовых

проверок, например, через рассылки писем, предлагающих получателям перейти по неизвестной ссылке. Рассмотрим современные методы более подробно.

Результаты исследований и их обсуждение. В настоящий момент, в соответствии с результатами исследований, около 65% профессионалов предпочитают иным способам обучения онлайн-курсы и вебинары. Это обусловлено тем, что онлайн-обучение предполагает гибкость в рабочем графике и возможность изучать материал в своем темпе [6]. Онлайн-обучение чаще всего запускают одновременно на все группы обучаемых и так или иначе ограничивают во времени для прохождения. Вебинары обычно включают в себя интерактивные элементы, например, опросы, часто дают доступ к чатам. Все это обогащает процесс обучения и позволяет обеспечивать своевременную обратную связь от экспертов.

В то же время, такой инструмент как симуляции позволяет обучающимся взаимодействовать с виртуальной средой, имитирующей реальные кибератаки. Это очень важный инструмент, который обеспечивает практический опыт без риска нарушения реальных систем. При этом 75% специалистов по ИБ считают, что симуляции помогают лучше усвоить материал, чем традиционные методы [7, 8]. Подобные игровые методы более интересны участникам за счет своей новизны, за счет этого усваиваются до 20% лучше, чем при получении знаний только в привычной форме, а также они серьезно развивают навыки решения проблем в условиях стресса [9].

По данным опроса Лаборатория Касперского [10], более половины топ-менеджеров (62%) признают, что недопонимание с ИТ- или ИБ-отделом привело как минимум к одному инциденту в их организациях, а 67% подтвердили, что проблемы с коммуникацией серьёзно задерживали реализацию проектов в области кибербезопасности. Улучшить понимание между отделами призваны современные методы обучения.

Наиболее результативным может быть подход, при котором совмещаются два современных метода обучения, то есть сначала обучающиеся получают теоретические навыки, а после – закрепляют знания в режиме симуляции. Отдельным качественным этапом может быть последующая проверка службой ИБ усвоенных навыков.

Выделим отдельно ряд преимуществ, которые предлагают современные методы обучения: гибкость, практическая направленность, адаптивность.

Примеры успешного применения современных методов обучения в ИБ

В реальной практике использование современных методов обучения уже доказало свою эффективность. Рассмотрим конкретные примеры и подробности применения данных методов:

Онлайн-курсы от Нетологии, Skillfactory или Skillbox по обучению ИБ являются одними из лидирующих онлайн-курсов в области ИБ, комбинируют лекции, видео, интерактивные тесты и вебинары. В 2022 году было отмечено, что студенты, завершившие такие курсы, показали улучшение своих навыков на 30% в сравнении с их предыдущим уровнем [11].

Варианты разработки **игр-симуляций** от Sber Gamification Lab [12]. На своем сайте Сбер предлагает так называемые potions — зелья геймификации, то есть набор практических инструкций, которые объединяют в себе различные элементы и механики геймификации. При их использовании для создания игры для сотрудников в своей компании, разработчики изначально получают понятный и готовый к применению рецепт, который решает конкретную проблему. Для получения четких инструкций, как создать интересную игру по обучению кибербезопасности, нужно выбрать категорию бизнеса, для которой разрабатывают игру. А далее – следовать инструкции и получать результаты.

Командная игра от Kaspersky Interactive Protection Simulation (KIPS) для топ-менеджеров и линейных руководителей доказала свою эффективность [13]. В игре демонстрируется влияние кибербезопасности на эффективность и доходы коммерческой организации. Бизнес-симуляция KIPS помогает научиться мыслить стратегически, предвидеть последствия атак и правильно реагировать в условиях ограниченного времени

и средств. Компании могут персонализировать игру с учётом специфики своего бизнеса, выбирая различные типы атак из библиотеки. Один сценарий может быть пройден несколько раз, не теряя своей актуальности и интереса для игроков, благодаря возможности выбирать количество и типы атак. Также игра может быть адаптирована под конкретную отрасль бизнеса. Онлайн-версия позволяет одновременно играть большому количеству людей из разных локаций либо добавлять удалённые команды к очному мероприятию, а также создавать отдельные голосовые чаты для команд. Кроме того, руководители могут получить статистику по тому, какой выбор делали игроки и как действовали в определённых ситуациях, чтобы сравнивать с их действиями в предыдущей игре. Каждый сценарий и разыгрываемая атака основаны на реальных инцидентах и показывают, почему кибербезопасность важна для непрерывности и доходности бизнеса.

Эти примеры иллюстрируют преимущества современных методов обучения: погружение в реальные ситуации, активное взаимодействие участников и возможность тестировать и улучшать свои навыки в безопасной среде. Все эти методы направлены на то, чтобы обеспечить сотрудников актуальными и практическими навыками, которые они смогут эффективно применять в реальной работе.

Адаптация современных методов обучения для крупных ИТ-компаний

Для крупных ИТ-компаний применение современных методов обучения может представлять определенные сложности из-за объема персонала. Вот несколько способов адаптации данных методов:

Масштабируемые онлайн-платформы: крупные компании могут внедрять масштабируемые обучающие платформы, которые поддерживают одновременное обучение тысяч сотрудников. Эти платформы могут предлагать персонализированные треки обучения в зависимости от роли и уровня знаний сотрудника.

Централизованные симуляции: вместо отдельных симуляций для каждого отдела, компании могут создать централизованные лаборатории, где команды могут проводить обмениваться опытом.

Перекрестное обучение: учитывая множество специализаций в больших ИТ-компаниях, перекрестное обучение может помочь сотрудникам лучше понимать задачи своих коллег. Например, инженеры безопасности могут провести сессии для разработчиков, объясняя лучшие практики безопасного кодирования.

Геймификация и внутренние соревнования: крупные компании могут организовывать внутренние хакатоны и соревнования, стимулируя сотрудников применять свои навыки в конкурентной среде и одновременно находить и исправлять уязвимости системы. Именно так крупнейшая компания – Яндекс – оперативно совершенствует свои системы. Помимо прочего Яндекс предлагает людям, нашедшим уязвимости, денежное вознаграждение за труды [14].

Обучение на рабочем месте: основываясь на методе "учимся на практике", можно использовать реальные случаи из своей практики для обучения персонала. Это позволит сотрудникам лучше понимать, как теоретические знания применяются на практике.

Менторство и наставничество: программы менторства могут помочь передать опыт от старшего к младшему поколению, обеспечить индивидуальный подход.

Компании должны учитывать культурные различия в своих подразделениях [15], особенно в такой крупной стране, как Россия.

Эффективное внедрение современных методов обучения в крупных ИТ-компаниях требует стратегического подхода, но при правильной адаптации может значительно повысить уровень экспертизы и готовность персонала к реальным угрозам.

Интеграция методов обучения в корпоративную культуру

Для эффективного обучения сотрудников важно не только выбрать правильные методы и инструменты, но и интегрировать их в корпоративную культуру компании. Какие подходы при этом рекомендуется соблюдать:

Обеспечивать поддержку со стороны руководства, своевременное

информирование руководителей о статусе обучения. Обучение информационной безопасности должно стать приоритетом на высшем уровне управления. Руководители должны демонстрировать свою приверженность этой инициативе, выделяя вопросу достаточно времени и ресурсов.

Принцип обучения как части корпоративной культуры. Обучение должно быть не эпизодичным, а постоянным. Создание среды, в которой обучение и повышение квалификации являются ежедневной нормой, способствует устойчивому росту компетенций сотрудников.

Предоставлять доступ сотрудникам к обратной связи без последствий. Сотрудники должны иметь возможность давать обратную связь по поводу обучающих программ, делясь своим опытом, идеями и предложениями, не переживая, что могут быть наказаны или уволены за свое мнение.

Регулярное обновлять материалы. Угрозы в области ИБ постоянно меняются. Компании должны регулярно пересматривать и обновлять свои обучающие программы, чтобы оставаться в курсе последних тенденций.

Использовать внутреннюю экспертизу. Использование собственных экспертов в качестве тренеров может значительно усилить эффективность обучения, так как они лучше понимают специфику компании и ее потребности.

Интеграция этих методов обучения в корпоративную культуру может привести к созданию среды, в которой сотрудники не только обучаются новым навыкам, но и активно применяют их на практике, улучшая общую безопасность и эффективность организации.

Заключение. В современном мире, где информационные технологии играют ключевую роль во многих аспектах нашей жизни и бизнеса, значимость обучения в области информационной безопасности не может быть недооценена. Исследование традиционных и современных методов обучения показало, что изменение моделей обучения в этой области направлено на увеличение гибкости, глубины погружения и практической пользы для обучаемых.

Традиционные методы обучения, хотя и заслуживают уважения за их проверенное временем значение, становятся менее эффективными в быстро меняющемся цифровом ландшафте. В то же время современные методы, такие как онлайн-курсы, симуляции и игровые методы, предлагают персонализированный и практичный опыт, который может быть адаптирован для различных потребностей и организаций.

Для гарантии безопасности и успешного внедрения новых методов в корпоративную культуру необходимо учитывать индивидуальные потребности, ресурсы и особенности каждой организации. В этом контексте, непрерывное обновление знаний и методов обучения становится жизненно важным для поддержания конкурентоспособности и защиты важной корпоративной информации.

ЛИТЕРАТУРА

1. Турутина Е. Э., Шевко Н. Р. Прогнозирование развития кибератак и концепция защиты от них // Вестник Российского университета кооперации. 2023. № 1 (51). С. 147–151.
2. Шогенов З. А. Киберпреступность как одна из основных проблем современного общества // Право и управление. 2023. № 2. С. 222–226.
3. Жалсанов М. К. Международный опыт обеспечения экономической безопасности в условиях цифровой трансформации // Академическая мысль. 2023. № 2 (23). С. 61–64.
4. Кузьминых Е. С., Маслова М. А. Анализ роста кибератак и рынка информационной безопасности РФ // Научный результат. Информационные технологии. 2023. № 2. С. 11–17.
5. Проваткина В. Е., Квасникова Т. В. Современные тенденции в противодействии кибертерроризму // Международный журнал гуманитарных и естественных наук. 2023. № 7-2 (82). С. 226–230.
6. Файзиева Д. Х., Яхяева Ш. Т. Влияние цифрового образования на успехи учащихся // Universum: технические науки. 2022. № 5-2 (98). С. 48–50.
7. Бородиенко А. В. Бизнес-симуляция vs традиционные педагогические технологии: эффекты использования // Образовательные технологии (г. Москва). 2014. № 4. С. 71–77.
8. Ксенофонтова А. Н., Заир-Бек Е. С. Влияние современных интерактивных технологий на развитие профессиональных компетенций студентов // Интеллект. Инновации. Инвестиции. 2014. № 4. С. 87–92.

9. Страхова Г. А., Страхов А. А. Активные формы и методы преподавания в современном образовании // Проблемы педагогики. 2017. № 9 (32). С. 39–42.

10. Татаринов К. А., Белых Е. Р. Рост конкурентоспособности компании через обучение сотрудников // Азимут научных исследований: педагогика и психология. 2021. № 3 (36). С. 271–273.

11. Жукова Л. В., Кирюшина А.А., Ковальчук И.М., Рузаева А.В. Повышение результативности системы дистанционного образования с помощью машинного обучения и технологии блокчейн // Прикаспийский журнал: управление и высокие технологии. 2018. № 2 (42). С. 56–68.

12. Ветушинский А. С. Больше, чем просто средство: новый подход к пониманию геймификации // Социология власти. 2020. № 3. С. 14–31.

13. Колесникова Д. С., Рудниченко А. К. Требования к разработке автоматизированной обучающей системы в области информационной безопасности // Инженерный вестник Дона. 2019. № 1 (52). С. 62.

14. Ревенков П. В., Чебарь А. Г., Бердюгин А. А. Источники киберрисков в условиях функционирования экосистем // В центре экономики. 2022. № 1. С. 1–11.

15. Bobovnikova A., Zrazhevskiy A. Modern lean management trends in the Us market // Proceedings of the XXX International Multidisciplinary Conference «Innovations and Tendencies of State-of-Art Science». Mijnbestseller Nederland, Rotterdam, Nederland. 2023.

REFERENCES

1. Turutina EE, Shevko NR. Prognozirovanie razvitiya kiberatak i kontseptsiya zashchity ot nikh. Vestnik Rossiiskogo universiteta kooperatsii. 2023;1(51):147-151. (In Russ.).

2. Shogenov ZA. Kiberprestupnost' kak odna iz osnovnykh problem sovremennogo obshchestva. Pravo i upravlenie. 2023;2:222-226. (In Russ.).

3. Zhalsanov M. K. Mezhdunarodnyi opyt obespecheniya ehkonomicheskoi bezopasnosti v usloviyakh tsifrovoi transformatsii. Akademicheskaya mysl'. 2023;2(23):61-64. (In Russ.).

4. Kuz'minykh ES, Maslova MA. Analiz rosta kiberatak i rynka informatsionnoi bezopasnosti RF. Nauchnyi rezul'tat. Informatsionnye tekhnologii. 2023;2:11-17. (In Russ.).

5. Provatkina VE, Kvasnikova TV. Sovremennye tendentsii v protivodeistvii kiberterrorizmu. Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk. 2023;7-2(82):226-230. (In Russ.).

6. Faizieva DKh, Yakhyaeva ShT. Vliyanie tsifrovogo obrazovaniya na uspekhi uchashchikhsya. Universum: tekhnicheskie nauki. 2022;5-2(98):48-50. (In Russ.).

7. Borodienko AV. Biznes-simulyatsiya vs traditsionnye pedagogicheskie tekhnologii: ehffekty ispol'zovaniya. Obrazovatel'nye tekhnologii (g. Moskva). 2014;4:71-77. (In Russ.).

8. Ksenofontova AN, Zair-Bek ES. Vliyanie sovremennykh interaktivnykh tekhnologii na razvitie professional'nykh kompetentsii studentov. Intellekt. Innovatsii. Investitsii. 2014;4:87-92. (In Russ.).

9. Strakhova GA, Strakhov AA. Aktivnye formy i metody prepodavaniya v sovremennom obrazovanii. Problemy pedagogiki. 2017;9(32):39-42. (In Russ.).

10. Tatarinov KA, Belykh ER. Rost konkurentosposobnosti kompanii cherez obuchenie sotrudnikov. Azimut nauchnykh issledovanii: pedagogika i psikhologiya. 2021;3(36):271-273. (In Russ.).

11. Zhukova LV, Kiryushina AA, Koval'chuk IM, Ruzaeva AV. Povyshenie rezul'tativnosti sistemy distantsionnogo obrazovaniya s pomoshch'yu mashinnogo obucheniya i tekhnologii blokchein. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii. 2018;2(42):56-68. (In Russ.).

12. Vetushinskii AS. Bol'she, chem prosto sredstvo: novyi podkhod k ponimaniyu geimifikatsii. Sotsiologiya vlasti. 2020;3:14-31. (In Russ.).

13. Kolesnikova DS, Rudnichenko AK. Trebovaniya k razrabotke avtomatizirovannoi obuchayushchei sistemy v oblasti informatsionnoi bezopasnosti. Inzhenernyi vestnik Dona. 2019;1(52):62. (In Russ.).

14. Revenkov PV, Chebar' AG, Berdyugin AA. Istochniki kiberriskov v usloviyakh funktsionirovaniya ehkosistem. V tsentre ehkonomiki. 2022;1:1-11. (In Russ.).

15. Bobovnikova A, Zrazhevskiy A. Modern lean management trends in the Us market. Proceedings of the XXX International Multidisciplinary Conference “Innovations and Tendencies of State-of-Art Science”. Mijnbestseller Nederland, Rotterdam, Nederland. 2023.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Эдуард Альбертович Шайхулов – бакалавр, Казанский инновационный университет им. В.Г. Тимирясова, ул. Московская, д. 42, г. Казань, 420111, Россия, +79503232237, https://orcid.org/0009-0002-0027-3634, shaihulove@gmail.com

Александр Петрович Смирнов – кандидат технических наук, Российский государственный аграрный университет – МСХА имени К.А.Тимирязева, ул. Тимирязевская, д. 49, г. Москва, 127434, Россия, +79057217077, https://orcid.org/0000-0002-1507-3312, SPIN-код: 7399-1884, AuthorID: 82657, ap.smirnov@rgau-msha.ru

Ольга Борисовна Болдина – кандидат технических наук, Санкт-Петербургский государственный морской технический университет, ул. Лоцманская, д. 3, г. Санкт-Петербург,

190121, Россия, +79217484749, https://orcid.org/0000-0001-9637-5285, SPIN-код: 2440-5894, tristan5401@rambler.ru

Геннадий Юрьевич Азаренко – аспирант, Сибирский государственный университет науки и технологий имени Академика М.Ф. Решетнева, проспект им. газеты Красноярский рабочий, д. 31, 660037, г. Красноярск, Россия, +79233080277, https://orcid.org/0000-0001-6146-8369, SPIN-код: 8455-8782, Gennadii.azarenko@mail.ru

Ирина Юрьевна Благова – кандидат экономических наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, ул. Политехническая, д. 29, г. Санкт-Петербург, 195251, Россия, +79818808450, https://orcid.org/0000-0002-2418-1702, SPIN-код: 3254-2258, blagova_iyu@spbstu.ru

INFORMATION ABOUT THE AUTHORS

Eduard A. Shaikhulov – Bachelor, Kazan Innovative University named after V.G. Timiryasov, 42, Moskovskaya St., Kazan, 420111, Russia, +79503232237, https://orcid.org/0009-0002-0027-3634, shaihulove@gmail.com

Alexander P. Smirnov – PhD in Technical Sciences, Russian State Agrarian University – Moscow Agricultural Academy named after K.A.Timiryazev, 49, Timiryazevskaya St., Moscow, 127434, Russia, +79057217077, https://orcid.org/0000-0002-1507-3312, SPIN code: 7399-1884, AuthorID: 82657, ap.smirnov@rgau-msha.ru

Olga B. Boldina – PhD in Technical Sciences, Saint Petersburg State Marine Technical University, 3, Lotsmanskaya St., Saint Petersburg, 190121, Russia, +79217484749, https://orcid.org/0000-0001-9637-5285, SPIN code: 2440-5894, tristan5401@rambler.ru

Gennady Yu. Azarenko – Graduate Student, Siberian State University of Science and Technology named after Academician M.F. Reshetnev, 31, gazeta Krasnoyarsk worker Avenue, Krasnoyarsk, 660037, Russia, +79233080277, https://orcid.org/0000-0001-6146-8369, SPIN code: 8455-8782, Gennadii.azarenko@mail.ru

Irina Yu. Blagova – PhD in Economics, Associate Professor, Peter the Great St. Petersburg Polytechnic University, 29, Politechnicheskaya St., St. Petersburg, 195251, Russia, +79818808450, https://orcid.org/0000-0002-2418-1702, SPIN code: 3254-2258, blagova_iyu@spbstu.ru

Вклад авторов: все авторы внесли равный вклад в подготовку публикации.
Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

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

Статья поступила в редакцию: 14.10.2023;
одобрена после рецензирования: 19.11.2023;
принята к публикации: 04.12.2023.

The article was submitted: 14.10.2023;
approved after reviewing: 19.11.2023;
accepted for publication: 04.12.2023.