DOI: 10.37930/1990-9780-2024-2-80-113-121

П. И. Бурак [1], *В. И. Глотов* [2], *В. П. Бауэр*[3]

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЕЙ ЦИФРОВЫХ МЕТАВИРТУАЛЬНЫХ СЕРВИСОВ

Отмечается рост внимания к финансовой безопасности пользователей цифровых метавиртуальных сервисов (далее – М-сервисы) после выявления их негативного влияния на сознание, психологию и мышление пользователей, приводящего к финансовым издержкам. Актуализируются вопросы выявления рисков финансовой безопасности пользователей М-сервисов и разработки подходов к их купированию. Полученные результаты могут быть полезными для пользователей М-сервисов, ИТ-специалистов при создании новых видов М-сервисов; профессионалов финансовой разведки при разработке средств ПОД/ФТ для М-сервисов, а также учёных и специалистов при исследованиях последствий внедрения средств формирования метавиртуальной реальности.

Ключевые слова: цифровая экономика, цифровые онлайн-игры, цифровые социальные сервисы, пользователи сервисов, информационно-психологическое воздействие, личная финансовая безопасность.

УДК 330.352

Под концептом *метавиртуальная реальность* понимается совокупность технологий виртуальной (VR), дополненной (AR), расширенной (XR) и смешанной (MR) реальности, машинного обучения (ML), искусственного интеллекта (AI), блокчейна, смарт-контрактов, криптовалюты, невзаимозаменяемых токенов (NFT) и других современных цифровых технологий [17, с. 333–339]. Метавиртуальная реальность является следствием масштабного поступательного развития и внедрения объектов цифровой экономики в киберфизическую среду современного сетевого социума [21, с. 16, 92–98, 773–779]. Она используется при создании цифровых метавиртуальных сервисов (далее – М-сервисы). В число таких объектов входят цифровые двойники, платформы, экосистемы, метавселенные и цифровые двойники (аватары) пользователей данных объектов. М-сервисы широко применяются в военных, космических, политических и

[1] *Петр Иосифович Бурак,* директор АО «Институт региональных экономических стратегий» (119002, РФ, Москва, пер. Сивцев Вражек, 29/16), д-р экон. наук, профессор, президент РАЕН, e-mail: irei@irei.ru.

[2] *Владимир Иванович Глотов,* руководитель Центра межолимпиадной подготовки школьников и студентов Физического института имени П. Н. Лебедева РАН (119991, РФ, Москва, Ленинский пр., 53, корп. 4, каб. 305), канд. экон. наук, профессор, действительный член РАЕН, e-mail: center@lebedev.ru.

[3] *Владимир Петрович Бауэр,* главный научный сотрудник АО «Институт региональных экономических стратегий» (119002, РФ, Москва, пер. Сивцев Вражек, 29/16), д-р экон. наук, доцент, действительный член РАЕН, e-mail: bvp09@mail.ru.

экономических исследованиях и разработках; в сфере образования (школьного, среднего и высшего); при реализации социальных и культурных проектов (конференций, выставок, экскурсий); в промышленности, медицине, маркетинге, рекламе, архитектуре, скульптуре, цифровой живописи и креативном дизайне, киноиндустрии, театральной деятельности, журналистике, робототехнике, кибербезопасности, онлайн-торговле товарами, продуктами и услугами, кредитовании, страховании, управлении цепочками поставок продукции; в ролевых онлайн-играх, киберспорте, сферах туризма, путешествий и гостиничного дела.

У каждого пользователя М-сервиса как субъекта информационного действия [18, с. 182–190] своё понимание и восприятие его ценностных свойств, которое, как показывают исследования [5], в процессе эксплуатации М-сервиса путём манипуляций [7, с. 99–108] может оказать негативное влияние на когнитивное [12, с. 50–56], психофизическое [9, с. 231–244] и эмоциональное состояние [4]. В связи с этим и в силу онтологического дуализма экономической реальности [11, с. 584–601] цифровая среда М-сервиса формирует благоприятные условия для разработки и практического использования средств цифрового финансового мошенничества [6] и виртуальных преступлений [1, с. 9–35], которые создают угрозу личной финансовой безопасности участников М-сервисов.

Финансовая безопасность в широком понимании – это перечень мер, способов, инструментов по охране экономических интересов государства. Сюда же относится финансовый аспект работы корпоративных структур и многочисленных субъектов хозяйствования [19]. Отдельного внимания заслуживает понятие *личной финансовой безопасности*. По сути, это *социально-экономическая деятельность личности, направленная на финансовую независимость и удовлетворение собственных материально-духовных потребностей. Этот процесс направлен на саму личность и на общество в целом, его главной задачей становится сохранение и развитие обозначенной независимости* [4].

К числу наиболее значимых различий в психологических особенностях пользователей М-сервисов можно отнести: *«приспособление, внутренний и внешний мониторинг, желание доминирования, нацеленность на себя, нацеленность на коммуникацию, нацеленность на деятельность, склонность к риску»* [13, с. 77–84]. Исходя из этого, в данной работе под финансовым риском (в широком смысле) будем понимать риск, сопряжённый с возможностью утраты финансовых инструментов (денежных средств); минимизации доходов, уменьшения капитала и др. В такой ситуации наблюдается неопределённость факторов финансовой деятельности [5].

Учитывая, что доминирующей особенностью пользователей М-сервисов является *склонность к риску* [2, с. 72–81], рассмотрим информационную среду с позиций характеристик обобщённого риска, оценки которого даются на уровне как личности (пользователя, субъекта), так и информационной среды М-сервиса (см. таблицу).

Из таблицы следует, что информационная среда преобразуется в фактор риска для участвующего в ней субъекта. Примечательно, что субъект причастен к данной среде в рамках поступающих информационных сообщений и может минимизировать

[4] Риски и угрозы, сопутствующие развитию индустрии киберспорта и гейминга // https://rdc.grfc.ru/2021/05/cybersport-and-gaming/ (дата обращения: 13.01.2024).

[5] Финансовый риск. URL: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D0%B9_%D1%80%D0%B8%D1%81%D0%BA (дата обращения: 03.09.2023).

риски существования в ней. В результате появляется возможность физического влияния на неё (применять/не применять информационный ресурс).

Разделение цифровой информационной среды в рамках идентификации обобщённого риска [14, с. 124–137]

Риск	В аспекте субъекта	В аспекте среды
Как факт	Без учёта диспозиционных свойств участника, присутствия риска в среде, отсутствия взаимодействия субъекта и среды	Присутствует вероятность риска в среде (приведём примеры среды или общения)
Как фактор	Участник может подвергаться воздействию среды	Среда аккумулирует функцию квазисубъекта физиологического и психологического влияния на участников
Как условие	Субъект обладает диспозиционными свойствами, нуждами, которые формируют условия риска, что делает среду рискогенной	Среда содействует удовлетворению в рамках определённого вида деятельности участника, что сопряжено с риском
Как средство	Субъект обладает потребностями в информационно-коммуникационной деятельности, что предусматривает эффективное взаимодействие с другими субъектами	Среда формирует интерес для субъекта в рамках достижения эффективности и успешности действий

Информационная среда как фактор риска («риск как фактор») активно воздействует на субъекта, что может привести к изменению его поведения или социальной роли.

В третьем случае («риск как условие») субъект под влиянием информационной среды может совершить какие-либо информационно-коммуникативные действия (возможен риск для личной финансовой безопасности) или отказаться от них (указанный риск отсутствует).

С точки зрения анализа рисков личной финансовой безопасности для пользователей сервисов четвёртый вариант («риск как средство») является определяющим, поэтому пользователей сервисов следует рассматривать как *квазисубъектов*, которые преобразуют информационный сегмент М-сервисов субъективными личностными свойствами. В рамках такого взаимодействия происходит взаимодействие субъекта как с *живым* участником коммуникации [8, с. 58–62].

Представленный взгляд на проблему взаимодействия пользователей М-сервисов позволяет на основе публикаций по данной тематике определить состав основных финансовых рисков, угрожающих личной финансовой безопасности пользователей, и предложить методы их купирования, что является необходимым условием создания доверительных отношений между пользователями, которые попадают в зависимость от компьютерных игр и друг от друга [20, с. 86–98].

Аватар-опосредованная деятельность в М-сервисах производительна, что даёт возможность пользователям удовлетворять не только информационно-психологические, но и материальные потребности посредством обмена виртуальных продуктов труда на обычные деньги и/или цифровые финансовые активы (криптовалюта, токены, жетоны и др.).

При использовании М-сервисов выплаты, как правило, осуществляются в цифровых финансовых активах (с возможным их обменом на фиатные деньги), поэтому все М-сервисы имеют браузерный криптокошелёк, функционирующий на основе тех-

нологии распределённого реестра (блокчейна)[6]. В контексте проблемы обеспечения личной финансовой безопасности будем исходить из того, что мошенничество одного из пользователей М-сервиса может являться преступлением с целью отобрать цифровой финансовый актив у партнёра (прямой способ мошенничества) или аккумулировать личные данные о нём для модернизации отложенного механизма мошенничества.

Для получения личной информации или пароля мошенники применяют социальные инженерные практики или различные психологические уловки и трюки, чтобы отвлечь внимание партнёров, усыпить их бдительность, ввести их в состояние шокового эффекта для выработки и принятия быстрого, но финансово рискованного для них решения. Это может произойти вследствие информационного и психологического давления. С этой целью мошенники используют многочисленные инструменты: представляются знакомыми или родственниками, сотрудниками службы безопасности кредитно-финансовых учреждений, работниками правоохранительных органов и др. – воздействуя на эмоциональную составляющую. Это приводит к нерациональным и непоправимым финансовым расходам цифровых финансовых ресурсов. Эффективность работы мошенников зависит от знаний психологии жертвы и умелого применения психологических механизмов. Популярный приём – убеждение человека в необходимости приобретения продуктов, товаров и услуг. При этом мошенники могут обманом заставить партнёра-жертву сделать авансовый платёж, который не окупится.

К непоправимым финансовым потерям пользователей М-сервисов может привести анонимность партнёров. Для этого мошенники применяют временные аккаунты по реализации поддельной продукции или фальшивых сервисов; могут использовать виртуальные или подложные кредитные карты и/или криптосчета, перевод на которые средств пользователя-жертвы позволяет осуществить противоправные действия в кратчайшие сроки.

Современные мошенники обычно кооперируются с киберпреступниками. Это повышает количество сомнительных финансовых случаев в виртуальном пространстве и изощрённых схем. За счёт чатов, анонимных программ, фишинга и прочих цифровых финансовых активов, модернизации инструментов финансовых атак эксперты по взлому информации организуют варианты взаимодействия, координируют преступную деятельность, реализуют мошеннические действия против участников М-сервисов.

Особо отметим, что мошенники непрерывно изобретают новые и совершенствуют известные схемы финансового обмана пользователей М-сервисов. Финансово не просвещённый и не подготовленный к этому пользователь может не знать о местах и случаях вероятной опасности. Лучшим вариантом преодоления сложностей является финансовая грамотность, она помогает минимизировать финансовые риски и соответственно – получить максимальный доход от применения М-сервисов. В результате она становится базовым компонентом системы ликвидации финансовых рисков для гарантии личной финансовой безопасности субъектов [7].

---

[6] Blockchain Universal Glossary. 2020 Association of International Certified Professional Accountants. URL: https://us.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/blockchain-universal-glossary.pdf (дата обращения: 21.01 2024).

[7] Методические рекомендации по подготовке и проведению Всероссийского тематического урока «Финансовая безопасность». https://www.rudn.ru/storage/u/www/files/news/Met_rekom_Finansovaya-bezopasnost.pdf (дата обращения: 21.01 2024).

В условиях сетевой организации современной экономики взаимодействие российских пользователей М-сервисов с партнёрами может осуществляться на удалённом расстоянии, в том числе с партнёрами из СНГ, ШОС, Африки, Латинской Америки, Ближнего Востока, Юго-Восточной Азии и др. Поэтому в контексте настоящей статьи (с учётом международного аспекта использования удалённых М-сервисов) считаем целесообразным предложить следующее. Как известно, страны СНГ, ЕАЭС И ШОС сформировали эффективные договорные правовые платформы кооперации, чтобы избежать противоправной деятельности в сегменте гарантии сетевой финансовой безопасности [3, с. 6–10]. Предлагаем воспользоваться их многолетним опытом совместной деятельности:

– обмен данными в сфере финансового мошенничества и аналогичной противоправной деятельности путём оказания помощи в рамках проверочных мероприятий относительно подозрительных субъектов;

– кооперация при осуществлении оперативно-розыскных действий, специальных согласованных операций, нацеленных на устранение, идентификацию, пресечение финансовой противоправной деятельности;

– взаимодействие при выполнении научно-исследовательской работы по темам, формирующимся в результате кооперации, в том числе при создании рабочих групп;

– проведение подготовительных мероприятий, переподготовки и повышения профессионального уровня кадров финансовой разведки;

– осуществление научно-практических мероприятий по противодействию противоправной деятельности в сфере финансов;

– предоставление правовой помощи по уголовным делам финансовой направленности.

Для оказания правовой поддержки по уголовным делам необходимо упростить специфику кооперации и осуществление прямых контактов между субъектами уголовной юстиции стран – членов СНГ, ЕАЭС, ШОС и БРИКС+. В целях развития координации, методического руководства, мониторинга периодов и правильности применения запросов в контексте ПОД/ФТ целесообразно централизовать взаимодействие государств-участников и государств-членов (СНГ, ЕАЭС, ШОС и БРИКС+) путём создания единого банка данных по направленным, поступившим и отработанным запросам о девиантном финансовом поведении пользователей М-сервисов.

Таким образом, практика показывает, что в М-сервисах происходят формирование и конвергенция специфических виртуальных и физических цифровых миров, что в контексте оценок этики, морали и психологии может негативно повлиять на личную финансовую безопасность пользователей. С учётом этих особенностей нами уточнены риски личной финансовой безопасности пользователей М-сервисов и предложены подходы к их купированию. Показано, что ключевыми факторами обеспечения личной финансовой безопасности пользователей М-сервисов являются их финансовая грамотность и взаимное доверие, которые определяют систему социальных, кросс-культурных, финансовых и информационно-психологических отношений пользователей [10, с. 9].

Доверие может формироваться не только в процессе общения пользователей М-сервисов, но и за счёт корректного технико-технологического обслуживания данных сервисов в целях исключения компьютерных и прочих угроз их инфраструктуре. Поэтому ИТ-компании, разрабатывающие и обслуживающие М-сервисы, должны активно внедрять меры кибербезопасности – от аутентификации личности пользовате-

лей до непрерывного совершенствования политики обеспечения их конфиденциальности при общении с партнёрами по этим сервисам.

Научению финансово безопасного использования М-сервисов в условиях проявления вышеуказанных финансовых рисков может способствовать целенаправленное внедрение в образовательные программы финансовой грамотности населения, этических норм и правил общения, которые рекомендуются положениями теории поведенческого дизайна – универсальной для любой сетевой киберфизической среды [15].

Список литературы

1. *Батурин, Ю. М.* Что делает виртуальные преступления реальными / Ю. М. Батурин, С. В. Полубинская // Труды Института государства и права Российской академии наук. – 2018. – Т. 13, № 2. – С. 9–35.

2. *Беляев, Г. Ю.* Оценка потенциалов и рисков интернет-ресурсов формирования социально-цифровой среды сетевого взаимодействия субъектов социализации и воспитания молодёжи / Г. Ю. Беляев // Образование личности. – 2020. – №1-2. – С. 72–81.

3. *Бурак, П. И.* Квазиметавселенные – новые сферы деятельности финансовой разведки / П. И. Бурак, В. П. Бауэр, Ю. П. Липунцов // Вестник РАЕН. – 2023. – Т. 23, № 2. – С. 6–10. DOI: 10.52531/1682-1696-2023-23-2-6-10.

4. *Гордячкова, О. В.* Личные финансы и финансовая безопасность: учеб. пособие / О. В. Гордячкова, Т. Ю. Калаврий. – М.: Мир науки, 2021. – 119 с.

5. *Григорян, Г. Р.* Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации / Г. Р. Григорян. URL: https://www.dissercat.com/content/moshennichestvo-v-sfere-kompyuternoi-informatsii-problemy-kriminalizatsii-zakonodatelnoi-reg?ysdid=laeakwojul871470396 (дата обращения: 13.01.2024).

6. *Есаян, А. К.* Финансовое мошенничество: обнаружение и предупреждение / А. К. Есаян. – М.: Московский гуманитарный университет, 2023. – 384 с.

7. *Зубков, Н. А.* Между нормальной коммуникацией и манипуляцией: границы и способ их определения / Н. А. Зубков, А. М. Осипова, О. В. Титкова // Контекст и рефлексия: философия о мире и человеке. – 2023. – Т. 12, № 9А. – С. 99–108. DOI: 10.34670/AR.2023.84.35.015.

8. *Казанцев, Ю. Ю.* Поведенческие стереотипы российских инвесторов финансовых пирамид: коллаборативный подход в исследовании / Ю. Ю. Казанцев, Н. Г. Филатова // Научный ежегодник Центра анализа и прогнозирования. – 2020. – №1(4). – С. 58–62.

9. *Леньков, С. Л.* Действие в киберпространстве / С. Л. Леньков, Н. Е. Рубцова // Мир психологии. – 2020. – № 2 (102). – С. 231–244.

10. *Медведева, Е. И.* Социально-экономические аспекты феномена «доверие» / Е. И. Медведева // Социальное пространство. – 2022. – Т. 8, № 4. – С. 9. DOI: 10.15838/sa.2022.4.36.9.

11. *Мудрик, Д. Г.* Онтологический дуализм экономической реальности / Д. Г. Мудрик, В. Н. Ковнир // AlterEconomics. – 2022. – Т. 19, № 4. – С. 584–601. DOI: 10.31063/AlterEconomics/2022.19-4.2.

12. *Николаева, Е. М.* Когнитивная деятельность в цифровой среде и интеллектуальные добродетели / Е. М. Николаева, Э. А. Дюкина, П. С. Котляр // Контекст и рефлексия: философия о мире и человеке. – 2022. – Т. 11, № 1А. – С. 50–56. DOI: 10.34670/AR.2022.24.30.006.

13. *Патраков, Э. В.* Социально-психологические предикторы отклонения трудового поведения / Э. В. Патраков, Т. Н. Лобанова // Вестник Костромского государственного уни-

верситета. Серия: Педагогика. Психология. Социокинетика. – 2020. – Т. 26, № 1. – С. 77–84. DOI: 10.34216/2073-1426-2020-26-1-77-84.

14. *Патраков, Э. В.* Экопсихологическая интерпретация риска как критерия психологической готовности индивида к взаимодействиям с цифровой средой (кросс-культурное исследование педагогов) / Э. В. Патраков, Ч. М. Сабо, Л. И. Батурина, Р. С. П. де Мораес // Психология человека в образовании. – 2023. – Т. 5, № 1. – С. 124–137. DOI: 10.33910/2686-9527-2023-5-1-124-137.

15. *Скоков, Р. Ю.* Поведенческий дизайн: экономические блага и социально-политическое манипулирование / Р. Ю. Скоков. – Волгоград: Волгоградский государственный университет, 2022. – 104 с.

16. *Солдатова, Н. О.* Виртуальный контекст реальности / Н. О. Солдатова, Ш. Р. М. Хусиен // Контекст и рефлексия: философия о мире и человеке. – 2023. – Т. 12, № 9А. – С. 92–98. DOI: 10.34670/AR.2023.79.89.014.

17. *Солдатова, Н. О.* Метавиртуальное: ассимиляция виртуальной и актуальной реальностей / Н. О. Солдатова, П. С. Котляр // Контекст и рефлексия: философия о мире и человеке. – 2023. – Т. 12, № 1-1. – С. 333–339. DOI: 10.34670/AR.2023.69.30.044.

18. *Тогузова, Л. И.* Субъект информационного действия: принципы и масштаб свободы / Л. И. Тогузова, О. В. Титкова, А. М. Осипова, С. В. Тихонова // Контекст и рефлексия: философия о мире и человеке. – 2023. – Т. 12, № 1-1. – С. 182–190. DOI: 10.34670/AR.2023.92.66.015.

19. *Черненко, В. А.* Финансовая безопасность России / В. А. Черненко. – СПб.: Изд-во СПбГЭУ, 2019. – 161 с.

20. *Шакун, Е. Ю.* Зависимость от компьютерных игр: обзор российских исследований / Е. Ю. Шакун, Е. В. Фадеева // Вопросы психического здоровья детей и подростков. – 2021. – Т. 21, № 4. – С. 86–98.

21. *Matthew, J. L.* Virtual, mixed, and augmented reality: a systematic review for immersive systems research / J. L. Matthew, W. P. Wagner // Virtual Reality. – 2021. – Vol. 25. – P. 773–799. – doi.org/10.1007/s10055-020-00492-0/

References

1. Baturin Yu. M., Polubinskaya S. V. (2018) Chto delayet virtual'nyye prestupleniya real'nymi [What makes virtual crimes real]. Proceedings of the Institute of State and Law of the Russian Academy of Sciences, 13 (2), pp. 9–35.

2. Belyaev G. Yu. (2020) Otsenka potentsialov i riskov internet-resursov formirovaniya sotsial'no-tsifrovoy sredy setevogo vzaimodeystviya sub"yektov sotsializatsii i vospitaniya molodezhi [Assessment of the potentials and risks of Internet resources for the formation of a social-digital environment of network interaction between subjects of socialization and education of youth]. Personal education, 1-2, pp. 72–81.

3. Burak P. I., Bauer V. P., Lipuntsov Yu. P. (2023) Kvazimetavselennyye – novyye sfery deyatel'nosti finansovoy razvedki [Quasi-metaverses – new areas of financial intelligence activity]. Bulletin of the Russian Academy of Natural Sciences, 23 (2), pp. 6–10. DOI: 10.52531/1682-1696-2023-23-2-6-10.

4. Gordyachkova O. V., Kalavriy (2021) T. Yu. Lichnyye finansy i finansovaya bezopasnost'. Uchebnoye posobiye [Personal finance and financial security. Textbook]. Moscow: World of Science, 2021. – 119 p.

5. Grigoryan G. R. Moshennichestvo v sfere komp'yuternoy informatsii: problemy kriminalizatsii, zakonodatel'noy reglamentatsii i kvalifikatsii [Fraud in the field of computer information: problems of criminalization, legislative regulation and qualification]. URL: https://www.dissercat.com/content/moshennichestvo-v-sfere-kompyuternoi-informatsii-problemy-kriminalizatsii-zakonodatelnoi-reg?ysdid=laeakwojul871470396 (access date: 01/13/2024).

6. Yesayan A. K. (2023) Finansovoye moshennichestvo: obnaruzheniye i preduprezhdeniye [Financial fraud: detection and prevention]. Moscow: Moscow Humanitarian University. 2023. 384 p.

7. Zubkov N. A., Osipova A. M., Titkova O. V. (2023) Mezhdu normal'noy kommunikatsiyey i manipulyatsiyey: granitsy i sposob ikh opredeleniya [Between normal communication and manipulation: boundaries and the way to determine them]. Context and reflection: philosophy about the world and man, 12 (9A), pp. 99–108. DOI: 10.34670/AR.2023.84.35.015.

8. Kazantsev Yu. Yu., Filatova N. G. (2020) Povedencheskiye stereotipy rossiyskikh investorov finansovykh piramid: kollaborativnyy podkhod v issledovanii [Behavioral stereotypes of Russian investors of financial pyramids: a collaborative approach to research]. Scientific yearbook of the Center for Analysis and Forecasting, 1(4), pp. 58–62.

9. Lenkov S. L., Rubtsova N. E. (2020) Deystviye v kiberprostranstve [Action in cyberspace]. World of Psychology, 2 (102), pp. 231–244.

10. Medvedeva E. I. (2022) Sotsial'no-ekonomicheskiye aspekty fenomena «doveriye» [Socio-economic aspects of the “trust” phenomenon]. Social space, 8(4), pp. 9. DOI: 10.15838/sa.2022.4.36.9.

11. Mudrik D. G., Kovnir V. N. (2022) Ontologicheskiy dualizm ekonomicheskoy real'nosti [Ontological dualism of economic reality]. AlterEconomics, 19(4), pp. 584–601. DOI: 10.31063/AlterEconomics/2022.19-4.2.

12. Nikolaeva E. M., Dyukina E. A., Kotlyar P. S. (2022) Kognitivnaya deyatel'nost' v tsifrovoy srede i intellektual'nyye dobrodeteli [Cognitive activity in the digital environment and intellectual virtues]. Context and reflection: philosophy about the world and man, 11(1A), pp. 50–56. DOI: 10.34670/AR.2022.24.30.006.

13. Patrakov E. V., Lobanova T. N. (2020) Sotsial'no-psikhologicheskiye prediktory otkloneniya trudovogo povedeniya [Social and psychological predictors of deviations in labor behavior]. Bulletin of Kostroma State University. Series: Pedagogy. Psychology. Sociokinetics, 26(1), pp. 77–84. DOI: 10.34216/2073-1426-2020-26-1-77-84.

14. Patrakov E. V., Sabo Ch. M., Baturina L. I., de Moraes R. S. P (2023) Ekopsikhologicheskaya interpretatsiya riska kak kriteriya psikhologicheskoy gotovnosti individa k vzaimodeystviyam s tsifrovoy sredoy (kross-kul'turnoye issledovaniye pedagogov) [Ecopsychological interpretation of risk as a criterion of an individual’s psychological readiness to interact with the digital environment (cross-cultural study of teachers)]. Human psychology in education, 5(1), pp. 124–137. DOI: 10.33910/2686-9527-2023-5-1-124-137.

15. Skokov R. Yu. (2022) Povedencheskiy dizayn: ekonomicheskiye blaga i sotsial'no-politicheskoye manipulirovaniye [Behavioral design: economic benefits and socio-political manipulation]. Volgograd: Volgograd State University. 2022. 104 p.

16. Soldatova N. O., Husien Sh. R. M. (2023) Virtual'nyy kontekst real'nosti [Virtual context of reality]. Context and reflection: philosophy about the world and man, 12(9A), pp. 92–98. DOI: 10.34670/AR.2023.79.89.014.

17. Soldatova N. O., Kotlyar P. S. (2023) Metavirtual'noye: assimilyatsiya virtual'noy i aktual'noy real'nostey [Metavirtual: assimilation of virtual and actual realities]. Context and reflection: philosophy about the world and man, 12(1-1), pp. 333–339. DOI: 10.34670/AR.2023.69.30.044.

18. Toguzova L. I., Titkova O. V., Osipova A. M., Tikhonova S. V. (2023) Sub"yekt informatsionnogo deystviya: printsipy i masshtab svobody [Subject of information action: principles and scale of freedom]. Context and reflection: philosophy about the world and man, 12(1-1), pp. 182–190. DOI: 10.34670/AR.2023.92.66.015.

19. Chernenko V. A. (2019) Finansovaya bezopasnost' Rossii [Financial security of Russia]. St. Petersburg: Publishing house of St. Petersburg State Economic University. 2019. 161 p.

20. Shakun E. Yu., Fadeeva E. V. (2021) Zavisimost' ot komp'yuternykh igr: obzor rossiyskikh issledovanii [Addiction to computer games: a review of Russian studies]. Issues of mental health of children and adolescents, 21(4), pp. 86–98.

21. Matthew J. L., Wagner W. P. (2021) Virtual, mixed, and augmented reality: a systematic review for immersive systems research. Virtual Reality, vol. 25, pp. 773–799. doi.org/10.1007/s10055-020-00492-0/

P. I. Burak,[8] **V. I. Glotov**[9]**, V. P. Bauer**[10]**. Financial Security of Users of Digital Metavirtual Services.** Theoretical and practical attention to the financial security of users of digital metavirtual services ((hereinafter referred to as M-services)) has increased in a wide circle of scientists, entrepreneurs and IT specialists after identifying the negative impact of these services on the consciousness, psychology and thinking of users, leading to their financial costs. Thus, the issues of identifying risks to the financial security of M-service users and developing approaches to their mitigation, discussed in this article, have been updated. The significance of the article lies in the generalization of theoretical and practical material on the issues of ensuring the financial security of users of M-services from the point of view of the information-psychological approach. The results of the article may be useful for users of M-services, IT specialists when creating new types of M-services, financial intelligence professionals when developing AML/CFT tools for M-services, as well as scientists and specialists when researching the consequences of implementing software and hardware in practice means of forming metavirtual reality.

Keywords: digital economy, digital online games, digital social services, service users, information and psychological impact, personal financial security.

[8] *Petr I. Burak,* Professor, Director of JSC «Institute for Regional Economic Strategies» (lane Sivtsev Vrazhek, 29/16, Moscow, 119002, Russia), Doctor of Economics, Professor, President of the Russian Academy of Natural Sciences, e-mail: irei@irei.ru.

[9] *Vladimir I. Glotov,* Head of the Center for Inter-Olympiad Training of Schoolchildren and Students of the Physics Institute named after. P. N. Lebedev Russian Academy of Sciences (Leninsky Prospekt, 53, building 4, room. 305, Moscow, 119991, Russia), Candidate of Economic Sciences, Professor, Full Member of the Russian Academy of Natural Sciences, e-mail: centre@lebedev.ru.

[10] *Vladimir P. Bauer*, Chief Researcher of JSC «Institute for Regional Economic Strategies» (lane Sivtsev Vrazhek, 29/16, Moscow, 119002, Russia), Doctor of Economics, Assistant Professor, Full Member of the Russian Academy of Natural Sciences, e-mail: bvp09@mail.ru.