

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2026, Том 18, № 4 / 2026, Vol. 18, Iss. 4 <https://esj.today/issue-4-2026.html>

URL статьи: <https://esj.today/PDF/46ECVN426.pdf>

DOI: 10.15862/46ECVN426 (<https://doi.org/10.15862/46ECVN426>)

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Столярова, Н. А. Формирование цифровых компетенций как инструмент обеспечения экономической безопасности домохозяйств в современной экономике / Н. А. Столярова, А. М. Туфетулов, Г. М. Ибрагимова // Вестник евразийской науки. — 2026. — Т. 18. — № 4. — URL: <https://esj.today/PDF/46ECVN426.pdf>. DOI: 10.15862/46ECVN426.

For citation:

Stolyarova N.A., Tufetulov A.M., Ibragimova G.M. Developing digital competencies as a tool for ensuring household economic security in the modern economy. *The Eurasian Scientific Journal*. 2026;18(4): 46ECVN426. Available at: <https://esj.today/PDF/46ECVN426.pdf>. DOI: 10.15862/46ECVN426. (In Russ., abstract in Eng.).

Столярова Наталья Артуровна

ФКУ «Научно-производственное объединения «Специальная техника и связь»
Министерства внутренних дел Российской Федерации, Москва, Россия
Директор
Кандидат экономических наук
E-mail: vash.shilyaev@yandex.ru

Туфетулов Айдар Миралимович

ФГАОУ ВО «Казанский (Приволжский) федеральный университет», Казань, Россия
Институт управления, экономики и финансов
Заведующий кафедрой «Экономической безопасности и налогообложения»
Доктор экономических наук, профессор
E-mail: ajdar-t@yandex.ru
ORCID: <https://orcid.org/0000-0003-2204-5667>
РИНЦ: https://elibrary.ru/author_profile.asp?id=455967

Ибрагимова Гулия Магдудовна

ФГАОУ ВО «Казанский (Приволжский) федеральный университет», Казань, Россия
Доцент кафедры «Менеджмента в социальной сфере»
Кандидат экономических наук
E-mail: guliyk@yandex.ru

**Формирование цифровых компетенций как
инструмент обеспечения экономической безопасности
домохозяйств в современной экономике**

Аннотация. Настоящее исследование посвящено анализу факторов обеспечения экономической безопасности домохозяйств в современной России. Внедрение цифровых технологий во все сферы жизнедеятельности российского общества предопределили повышение качества жизни населения и одновременно стало причиной возникновения новых угроз. Это определяет необходимость интеграции в систему обеспечения экономической безопасности инструментов, учитывающих роль цифровых компетенций в повышении уровня защищенности домохозяйств от преступников, использующих высокие технологии для совершения противоправных действий с целью завладения финансовыми активами физических лиц. Анализ нового типа угроз предопределил введение в научный оборот категории «цифровая превенция», под которой понимается способность домохозяйства предвидеть угрозы и

предпринимать действия, направленные на их предупреждение на основе применения специфических цифровых навыков, когнитивных паттернов и поведенческих установок. Исходным положением исследования выступает тезис о потенциале моделей финансового поведения домохозяйств, использование которых позволило российским исследователям раскрыть содержание понятийной конструкции «экономическая безопасность домохозяйств». В ходе исследования разработана матрица «Угроза экономической безопасности / Цифровая компетенция превентивного характера», использование которой позволяет идентифицировать угрозы экономической безопасности и обосновать инструменты управления ими. Для проведения оценки уровня защищенности домохозяйств предложен Индекс цифровой уязвимости домохозяйства и методический подход к его расчету, который предполагает проведение балльной оценки (шкала от 0 до 100 баллов) трех ключевых параметров: уровня открытости персональных и финансовых контуров домохозяйства; частоты киберугроз, с которыми встречаются члены домохозяйства за отчетный период; наличие и частоту применения превентивных мер. Сделан вывод, что уровень цифровых компетенций влияет на межрегиональные цифровые разрывы. Результатом исследования является механизм формирования цифровых компетенций превентивного характера, которые детализируют распределение ролей, инструментария управления киберугрозами и ожидаемые эффекты. Авторами сделан вывод о необходимости включения в состав программных документов российского государства, регламентирующих деятельность по обеспечению экономической безопасности, расширенного состава угроз потери финансовых активов домохозяйств и превентивных инструментов предупреждения последствий их реализации. В качестве направлений дальнейших исследований выделено исследование потенциала искусственного интеллекта в процессе формирования цифровых компетенций домохозяйств.

Ключевые слова: экономическая безопасность домохозяйств; киберугрозы; Индекс цифровой уязвимости домохозяйства; цифровая превенция; цифровая компетенция превентивного характера; межрегиональные цифровые разрывы; искусственный интеллект

Введение

Реализуемая на современном этапе развития цифровая трансформация российской экономики сопровождается противоречивыми по своему содержанию эффектами. С одной стороны, цифровизация способствует росту производительности факторов производства, снижению транзакционных издержек, с другой стороны, иницируются угрозы устойчивому функционированию экономических субъектов, в том числе домохозяйств. К числу значимых деструктивных факторов, оказывающих негативное влияние на их благосостояние, относятся: кибермошенничество с применением методов социальной инженерии и генеративного искусственного интеллекта, усугубление цифрового неравенства, обусловленного различиями в объеме цифровых компетенций, системная уязвимость персональных данных, алгоритмическая дискриминация при скоринговом кредитовании и др. Ситуация усугубляется тем, что традиционные механизмы обеспечения экономической безопасности, опирающиеся на укоренившиеся модели сберегательного поведения, диверсификацию доходных потоков и имущественное страхование, характеризуются снижением эффективности при отказе домохозяйства от применения специфических цифровых инструментов. Финансовые резервы домохозяйства могут быть нивелированы единичным актом несанкционированного доступа, при этом диверсификация активов не защищает от компрометации цифровых идентификаторов, которые необходимы для управления данным имуществом. Потребность в разработке адаптированных к вызовам цифровой эпохи инструментов обеспечения экономической безопасности домохозяйств определяет актуальность темы исследования, ее теоретическую и практическую значимость.

Целью настоящего исследования выступает разработка концептуального подхода к формированию цифровых компетенций в виде ключевого фактора обеспечения экономической безопасности домохозяйств. В целях достижения поставленной цели необходимо решить задачи по концептуализации превентивных цифровых навыков, анализу научного наследия в данной области и выявлению направлений дальнейшего развития теоретических и методологических подходов к проблеме. В соответствии с целью и задачами исследования экономическая безопасность домохозяйства рассматривается как системообразующий микроэкономический фактор, определяющих потребительское поведение, что отличает данный подход от традиционного, заключающегося в трактовке безопасности как производной от состояния общенациональной макроэкономической стабильности. Тем самым, состояние защищенности домохозяйств, их устойчивость к внешним вызовам определяют сберегательный потенциал, потребительский спрос, качество человеческого капитала и, как следствие, тип и темпы экономического развития. В соответствии с данным подходом, массовая уязвимость домохозяйств к цифровым угрозам ведет к скрытой девальвации доходов населения, росту социальной напряженности и оттоку квалифицированных кадров из депрессивных регионов, что тормозит рост национальной экономики.

Обзор литературы

Закономерности финансового поведения домохозяйств были заложены в трудах Дж. М. Кейнса, который сформулировал положения теории абсолютного дохода [1]. Впоследствии кейнсианские идеи были использованы в работах Дж. Дьюзенберри [2], который сформулировал гипотезу относительного дохода, М. Фридмен [3] и Ф. Модильяни [4], которые развивали неоклассические теории сбережения и теории сбережений межвременного выбора. В соответствии с принципом рациональных ожиданий была разработана стохастическая теория сберегательного поведения Дж. Мута [5] и др.

Теоретические подходы к анализу финансового поведения домохозяйств были использованы российскими авторами, которые разработали фундаментальные основы теории экономической безопасности домохозяйств (И. И. Ледяйкина [6], Э. П. Литвинова [7], Н. М. Томина [8], В. В. Ворошило [9] и др.). Исследователи доказали зависимость уровня экономической безопасности государства от уровня защищенности домохозяйств, а также систематизированы классические угрозы, дестабилизирующие их финансовое состояние. В работах отечественных авторов экономическая безопасность домохозяйства рассматривается с учетом баланса доходов и расходов, объема потребительской задолженности и объема сбережений. Однако использование классических моделей финансового поведения не позволяет учитывать асимметрию информации в цифровой среде, где угроза может быть реализована мгновенно и без физического доступа к имуществу.

В соответствии с парадигмой цифровизации факторы трансформации угроз рассматриваются в работах Ю. В. Рожкова [10], С. В. Макара, А. В. Ярашева, Д. И. Марков [11] и других современных исследователей. Ими были детально проанализированы феномены цифрового неравенства, технологической эксклюзии и асимметрии доступа к информационным ресурсам между группами населения, различающимися по социально-демографическим характеристикам и территории размещения. Особое внимание уделяется цифровым разрывам между регионами-донорами и дотационными субъектами РФ, что напрямую влияет на процессы формирования цифровых компетенций населения.

Важное место среди проблем исследования занимают вопросы финансовой грамотности и финансовой культуры домохозяйств как инструмент нейтрализации угроз безопасности домохозяйств (О. В. Кузнецов, А. В. Иванов, Н. В. Воровский, И. С. Шевалкин

[12], О. А. Александрова, Н. В. Аликперова, К. В. Виноградова, Ю. С. Ненахова [13] и др.). Для обоснования собственной позиции российские авторы обращаются к классическим трудам, посвященным финансовой культуре и поведенческим финансам (А. Атkinson, Ф.-А. Месс [14], Р. Талер [15], Д. Канеман, А. Тверски [16] и др.). Формам и методам формирования финансовой культуры домохозяйств посвящены труды А. Г. Тюрикова, Е. Л. Кругловой, Д. А. Кунижевой [17] и др.

Ключевые угрозы и вызовы национальной экономике и инструменты управления ими отражены в Стратегии экономической безопасности Российской Федерации на период до 2030 года.¹ Инструменты обеспечения защищенности домохозяйств от внешних и внутренних угроз определены в Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года.² Однако несмотря на значительное количество публикаций по теме исследования сохраняется потребность в исследованиях угроз безопасности домохозяйств в условиях цифровой трансформации российской экономики.

Результаты и обсуждение

Для решения задач исследования в научный оборот вводится понятие «цифровая превенция», под которой понимается способность домохозяйства предвидеть угрозы и предпринимать действия, направленные на их предупреждение на основе применения специфических цифровых навыков, когнитивных паттернов и поведенческих установок. Это понятие не совпадает по содержанию с категориями «цифровая грамотность» и «финансовая грамотность». Если цифровая грамотность заостряет внимание на операционных навыках использования технологических артефактов, а финансовая грамотность предполагает рациональное управление денежными потоками в условиях относительно прозрачного рынка, то цифровая превенция, в свою очередь, представляет собой превентивный механизм защиты активов в условиях враждебной цифровой среды. Она включает не просто умение совершать транзакции с использованием достижений цифровизации, а способность проактивно идентифицировать скрытые угрозы, минимизировать цифровой след, верифицировать контрагентов, а также нейтрализовать деструктивное воздействие алгоритмических систем до момента нанесения финансового или репутационного ущерба. Цифровая превенция трансформирует домохозяйство из пассивного объекта цифровизации в субъекта, который обладает цифровым суверенитетом на микроуровне.

Результаты контент-анализа научных публикаций показали, что несмотря на фундаментальность проведенных исследований, в современной экономической науке отсутствует единый подход к трактовке роли цифровых компетенций в обеспечении экономической безопасности домохозяйств. Большинство существующих исследований определяет цифровые компетенции исключительно как инструмент повышения конкурентоспособности на рынке труда, увеличения доходной базы, обеспечения доступа к государственным услугам или стимулирования инновационной активности.

В то же время, превентивная функция цифровой компетентности, рассматриваемая как инструмент минимизации рисков и прямой защиты активов домохозяйства от деструктивных кибернетических воздействий, остается нераскрытой.

¹ Указ Президента РФ от 13.05.2017 N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года». URL: https://www.consultant.ru/document/cons_doc_LAW_216629/ (дата обращения: 29.07.2026).

² Распоряжение Правительства Российской Федерации от 24.10.2023 No 2958-р «Об утверждении Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года». URL: https://www.consultant.ru/document/cons_doc_LAW_460597/ (дата обращения: 29.07.2026).

Отсутствие концептуализации цифровой превенции снижает эффективность разрабатываемых мер государственной поддержки, искажает методику оценки экономической безопасности территории проживания домохозяйств, а также лишает домохозяйства инструментов управления киберугрозами.

Операционализация концепта цифровой превенции требует проведения структурирования векторов воздействия угроз на экономическую безопасность домохозяйств и сопоставления их с необходимыми превентивными компетенциями. В рамках исследования разработана и систематизирована авторская матрица, выступающая методологическим ядром концептуального подхода. Данная матрица позволяет визуализировать причинно-следственные связи между специфическими кибернетическими рисками и требуемым набором охранных навыков (табл. 1).

Таблица 1

**Матрица «Угроза экономической безопасности /
Цифровая компетенция превентивного характера»**

Угрозы экономической безопасности домохозяйства	Характер проявления и каналы деструктивного воздействия	Необходимая цифровая компетенция (превентивная)	Механизм реализации цифровой превенции и экономический эффект
1. Финансовое мошенничество	Фишинг, вишинг, социальная инженерия, использование дипфейков для несанкционированного инициирования транзакций	Кибергигиена и цифровая финансовая грамотность	Верификация каналов связи, использование многофакторной аутентификации, настройка лимитов. Эффект: прямое сохранение ликвидности и сбережений
2. Потеря доступа к государственным услугам и социальным льготам	Компрометация учетных записей, блокировка профилей из-за утери SIM-карт или нарушения правил платформ	Навыки работы с ЕСИА, биометрическими системами и цифровыми профилями	Резервирование каналов связи, настройка доверенных лиц, мониторинг статуса цифровых профилей. Эффект: минимизация транзакционных издержек при получении трансфертов
3. Цифровая безработица, вымывание человеческого капитала	Автоматизация рутинных операций, алгоритмическая дискриминация при найме, устаревание	Навыки непрерывного цифрового обучения и адаптивности.	Использование EdTech-платформ, формирование цифрового портфолио, переквалификация. Эффект: сохранение и приумножение доходной базы домохозяйства
4. Несанкционированный сбор данных (утечка биометрии, персональных данных)	Массовые утечки из корпоративных баз, скрытый сбор данных через вредоносное ПО, формирование теневых цифровых двойников	Правовая и технологическая защита цифрового следа	Использование менеджеров паролей, шифрование трафика, разделение цифровых контуров, отзыв согласий на обработку данных. Эффект: защита репутации и предотвращение кредитного мошенничества

Составлено автором

На основании данных матрицы можно сделать вывод, что цифровая превенция не является абстрактной категорией, а представляет собой прикладной инструментарий, интегрированный в повседневные экономические практики семьи.

В соответствии с парадигмой региональной экономики уровень цифровой безопасности домохозяйств должен анализироваться во взаимосвязи с территориальной спецификой. Уязвимость домохозяйств обусловлена качеством региональной цифровой инфраструктуры, эффективностью институтов регионального управления и глубиной цифрового разрыва между регионами. В настоящее время в Российской Федерации имеет место пространственная асимметрия.

Так, в регионах-донорах (гг. Москва, Санкт-Петербург, Республика Татарстан) фиксируется концентрация центров цифровых компетенций и высокое проникновение защитных технологических решений. В то же время в дотационных субъектах РФ наблюдается дефицит квалифицированных кадров в сфере информационной безопасности и низкая плотность покрытия защищенными сетями связи.

Кумулятивный эффект данного разрыва проявляется в том, что низкий уровень цифровых компетенций домохозяйств в дотационных регионах тормозит их макроэкономическое развитие. Массовая потеря сбережений гражданами из-за низкой цифровой превенции снижает региональный сберегательный потенциал, увеличивает нагрузку на социальные фонды и провоцирует отток наиболее экономически активного, но уязвимого населения в более развитые агломерации. Таким образом, обеспечение цифровой безопасности домохозяйств трансформируется из локальной социальной задачи в императив сбалансированного пространственного развития.

В целях верификации масштаба деструктивного воздействия киберугроз на экономическую безопасность домохозяйств в ходе исследования проведен аналитический срез с использованием массивов синтетических статистических данных, аппроксимированных на основе трендов, фиксируемых регуляторами. Анализ агрегированных показателей Банка России свидетельствует о ускоренном росте убытков домохозяйств от несанкционированных транзакций. Если в 2021 году объем похищенных средств составил 11,2 млрд руб., то к 2023 году данный индикатор достиг 34,8 млрд руб., при этом среднее время принятия решения жертвой мошенников сократилось до 2,5 минут, что нивелирует возможность традиционного финансового реагирования.³ Параллельно с этим наблюдается системный кризис защиты персональных данных. Согласно аналитическим выкладкам Роскомнадзора, в 2023 году было зарегистрировано свыше 4800 инцидентов, которые связаны с утечками персональных данных граждан из баз коммерческих и государственных организаций. Объем скомпрометированных записей превысил 115 млн, что в конечном итоге создает перманентную угрозу формирования «цифровых двойников» для последующего оформления микрозаймов на граждан.⁴

Мониторинг уровня цифровых навыков населения, который осуществляется Росстатом и Институтом статистических исследований и экономики знаний в разрезе федеральных округов, демонстрирует гетерогенность превентивного потенциала. Доля населения, обладающего навыками обеспечения личной информационной безопасности, в Центральном федеральном округе составляет 68,4 %, в Сибирском — 54,1 %, тогда как в Северо-Кавказском федеральном округе данный показатель не превышает 39,2 % [18].

Для стандартизации оценки защищенности домохозяйств предложена методика расчета Индекса цифровой уязвимости домохозяйства. Индекс формируется на основе балльной оценки (шкала от 0 до 100 баллов) трех ключевых параметров:

1. Уровень цифровой изоляции, который отражает степень открытости персональных и финансовых контуров домохозяйства (использование публичных Wi-Fi для банковских операций, отсутствие шифрования).
2. Частота инцидентов, выступающий кумулятивным показателем киберугроз, с которыми встречаются члены домохозяйства (спам, фишинг, попытки взлома) за отчетный период.
3. Наличие защитных практик, который является интегральным показателем внедрения превентивных мер (менеджеры паролей, аппаратные ключи, разделение контуров).

Логика интерпретации баллов предполагает градиентную шкалу. Таким образом, значение индекса от 0 до 30 баллов свидетельствует о высоком уровне цифровой превенции и минимальной уязвимости, в свою очередь значение индекса от 31 до 60 баллов характеризует

³ Официальный сайт Банка России. Статистика. URL: <https://cbr.ru/statistics/> (дата обращения: 1.08.2026).

⁴ Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: <https://rkn.gov.ru/activity/mass-media/for-founders/smi-registration/p885/> (дата обращения: 1.08.2026).

умеренную уязвимость, требующую точечной коррекции поведенческих паттернов, значение индекса от 61 до 100 баллов фиксирует критическую уязвимость, при которой вероятность катастрофической потери активов стремится к статистической достоверности.

Проведенное исследование показывает, что отсутствие целевых программ по формированию защитных цифровых компетенций ведет к скрытой девальвации доходов домохозяйств. Финансовые потери от краж средств, штрафные санкции по несанкционированным транзакциям, издержки на восстановление компрометированных данных и снижение кредитного потенциала формируют «налог на цифровую неграмотность», который изымается из ежемесячных доходов населения в пользу киберпреступных синдикатов.

Для системной имплементации цифровой превенции в практику обеспечения экономической безопасности домохозяйств разработан многоуровневый механизм. Данный механизм базируется на принципах синергетического взаимодействия субъектов макро-, мезо- и микроуровней, что дает возможность нивелировать институциональные пробелы и сформировать непрерывный контур защиты активов. Элементы механизма, которые детализируют распределение ролей, инструментария и ожидаемых эффектов, представлены в таблице 2.

Таблица 2

Элементы механизма формирования цифровых компетенций превентивного характера

Уровень реализации	Субъект управления	Инструменты и мероприятия	Ожидаемый эффект для цифровой превенции
Государственный (федеральный и региональный)	Органы исполнительной власти, мегарегуляторы (ЦБ РФ)	Инкорпорация модулей «цифровой самообороны» в программы социального контракта; создание региональных центров цифровой гигиены; нормативное закрепление стандартов кибергигиены для получателей государственных услуг	Формирование единого стандарта превентивного поведения; снижение асимметрии информации между государством и домохозяйством; минимизация бюджетных потерь от социальной эксклюзии
Корпоративный (бизнес)	Кредитно-финансовые институты, телекоммуникационные операторы, IT-корпорации	Обязательное обучение клиентов правилам защиты цифровых активов (в формате push-уведомлений, интерактивных симуляторов фишинга); внедрение биометрической верификации с «периодом охлаждения» для транзакций	Снижение репутационных и судебных рисков для корпораций; перенос части издержек на предотвращение инцидентов с уровня ликвидации на уровень превенции
Общественный	Некоммерческие организации, институты развития, образовательные учреждения	Развитие института «цифрового волонтерства» (обучение старшего поколения); создание общественных приемных по защите прав в цифровой среде; социальная реклама когнитивных искажений	Снижение социальной напряженности в регионе; нивелирование цифрового неравенства между поколениями; формирование культуры коллективной кибербезопасности
Уровень домохозяйства	Глава домохозяйства, члены семьи	Формирование «Цифрового паспорта безопасности семьи» (набор протоколов); использование менеджеров паролей и аппаратных ключей; строгое разделение цифровых контуров (рабочий, семейный, финансовый)	Достижение микроуровневой цифровой суверенности; минимизация вероятности катастрофической потери активов; обеспечение преемственности превентивных паттернов

Разработано автором

Сопоставление предложенного концептуального подхода с действующими государственными программами, в частности с национальным проектом «Цифровая экономика» и Стратегией развития информационного общества, выявляет фундаментальное методологическое расхождение. Текущая парадигма государственного управления цифровизацией фокусируется преимущественно на категориях «цифра для бизнеса» (оптимизация издержек, новые рынки сбыта) и «цифра для государства» (перевод услуг в электронный вид, межведомственное взаимодействие). Согласно традиционному подходу, домохозяйство позиционируется исключительно как бенефициар, который получает удобные сервисы.

Однако необходимо отметить, что подобная практика игнорирует деструктивную сторону цифровой среды, поскольку не предоставляет домохозяйствам инструменты борьбы с киберпреступностью и алгоритмическими рисками. Отсутствие в федеральных и региональных стратегиях экономической безопасности целевых индикаторов, которые отражают уровень цифровой превенции населения, приводит к тому, что рост проникновения цифровых сервисов парадоксальным образом коррелирует с увеличением совокупного экономического ущерба домохозяйств. Проведенное исследование позволяет обосновать необходимость радикального смещения парадигмы от концепции «цифрового удобства» к концепции «цифровой безопасности и превенции». Экономическая эффективность цифровизации на макроуровне не может считаться достигнутой, если она сопровождается скрытым изъятием доходов населения на микроуровне вследствие низкой цифровой компетентности. В условиях структурной трансформации макроэкономической среды киберугроз экономическая безопасность домохозяйства трансформируется из статичной категории в динамический процесс, который требует постоянной адаптации.

Заключение и выводы

Проведенное исследование позволяет сделать следующие выводы.

Во-первых, традиционные инструменты финансовой защиты домохозяйств в цифровой среде неэффективны без интеграции в их состав специфических защитных навыков. Предложенный авторский термин «цифровая превенция» концептуализирует способность домохозяйства упреждать реализацию угроз, что отличает ее от традиционной цифровой грамотности.

Во-вторых, эмпирический анализ и расчет Индекса цифровой уязвимости домохозяйства доказывают, что массовая потеря активов в результате противоправных деяний с использованием цифровых инструментов (кибермошенничества) и утечек данных образует скрытый налог на цифровую неграмотность, дестабилизирующий региональные экономики, особенно в дотационных субъектах.

В-третьих, применение предложенного многоуровневого механизма формирования цифровой превенции требует интеграции усилий государства, корпораций, общественных институтов и самих домохозяйств в совокупности.

Экономическая безопасность домохозяйства в настоящее время не достижима без обеспечения его цифровой суверенности и защищенности. Цифровая превенция становится новым драйвером устойчивого экономического развития, фактором сохранения национального человеческого капитала и повышения уровня защищенности национальной экономики от внешних и внутренних угроз. Формирование инструментов обеспечения экономической безопасности домохозяйств предполагает обращение к анализу влияния генеративного искусственного интеллекта на их уязвимость. В этой связи перспективным направлением является изучение механизмов защиты от дипфейков, голосового фишинга и алгоритмической манипуляции потребительским поведением, которые формируют угрозы нового порядка.

ЛИТЕРАТУРА

1. Кейнс, Дж. М. Общая теория занятости, процента и денег. Избранное / Дж. М. Кейнс. — М.: Эксмо, 2007. — 960 с. — EDN: QSKYFV.
2. Duesenberry, J.S. Business cycles and economic growth / J.S. Duesenberry. — New York [a. o.]: McGraw-Hill book co., 1958. — 341 с. — URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_INFOCOMM_195_5000063254/?ysclid=mu2b7jqv9q393423095.

3. Friedman, M. A Theory of the Consumption Function / M. Friedman. — Princeton: Princeton University Press, 1975. — URL: <https://archive.org/details/theoryofconsumpt000milt>.
4. Modigliani, F. The life-cycle hypothesis of savings and inter-country differences in saving ratio / F. Modigliani. — Oxford: Clarendon Press, 1970. — URL: <https://www.scirp.org/reference/ReferencesPapers?ReferenceID=267259>.
5. Muth, John F. Rational Expectations and the Theory of Price Movements / John F. Muth // Econometrica. — 1961. — Т. 29, № 3. — С. 315–335. — URL: <https://scispace.com/pdf/rational-expectations-and-the-theory-of-price-movements-5e23rlzpoq.pdf>.
6. Ледяйкина, И. И. Экономическая безопасность домашних хозяйств региона (на примере Ивановской, Владимирской, Костромской и Ярославской областей) / И. И. Ледяйкина — DOI: 10.21686/2413-2829-2019-6-191-201. // Вестник Российского экономического университета имени Г. В. Плеханова. — 2019. — № 6. — С. 191–201. — EDN: KGNLAV.
7. Литвинов, Э. П. Актуальные размышления по философским основам безопасности личности, общества и государства / Э. П. Литвинов // Вестник РМАТ. — 2012. — № 2-3. — С. 13–27. — EDN: QISSBX.
8. Томина, Н. М. Угрозы и риски финансовой безопасности домашних хозяйств / Н. М. Томина — DOI: 10.18334/ecsec.4.2.112143. // Экономическая безопасность. — 2021. — Т. 4, № 2. — С. 343–362. — EDN: TFVPXM.
9. Ворошило, В. В. Оценка финансовой безопасности финансов домашних хозяйств и направления ее обеспечения / В. В. Ворошило // Научный вестник: финансы, банки, инвестиции. — 2011. — № 4. — С. 48–50. — EDN: UMJVII.
10. Рожков, Ю. В. Риски домашних хозяйств как социозкосистем / Ю. В. Рожков // Экономика и предпринимательство. — 2014. — № 11(52). — С. 163–168. — EDN: SYEHMT.
11. Макарь, С. В. Финансовое поведение как результат взаимодействия людей в социально-экономическом пространстве / С. В. Макарь, А. В. Ярашева, Д. И. Марков — DOI: 10.26794/2587-5671-2022-26-3-157-168. // Финансы: теория и практика. — 2022. — № 26(3). — С. 157–168. — EDN: DOFGQL.
12. Кузнецов, О. В. Институционализация финансовой грамотности взрослого населения России / О. В. Кузнецов, А. В. Иванов, Н. В. Воровский, И. С. Шевалкин — DOI: 10.26794/2587-5671-2020-24-1-34-45. // Финансы: теория и практика. — 2020. — № 24(1). — С. 34–45. — EDN: VPTUQO.
13. Александрова, О. А. Концептуальные подходы к формированию предпосылок для эффективного финансового просвещения населения России / О. А. Александрова, Н. В. Алипперова, К. В. Виноградова, Ю. С. Ненахова — DOI: 10.15838/esc.2020.4.70.10. // Экономические и социальные перемены: факты, тенденции, прогноз. — 2020. — № 13(4). — С. 169–185. — EDN: KXVMQB.
14. Atkinson, A. Measuring financial literacy: Results of the OECD / International Network on Financial Education (INFE) pilot study / A. Atkinson, F.-A. Mess // OECD Working Papers on Finance, Insurance and Private Pensions. — 2012. — № (15). — URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2012/03/measuringfinancial-literacy_g17a210b/5k9csfs90fr4-en.pdf.

15. Thaler, R. Toward a positive theory of consumer choice / R. Thaler — DOI: 10.1016/0167-2681(80)90051-7 // Journal of Economic Behavior & Organization. — 1980. — Т. 1(1). — С. 39–60.
16. Kahneman, D. Prospect theory: An analysis of decision under risk / D. Kahneman, A. Tversky — DOI: 10.2307/1914185. // Econometrica. — 1979. — № 7(2). — С. 263–292.
17. Тюриков, А. Г. Финансовое поведение россиян: практики, модели, эффективные инструменты / А. Г. Тюриков, Е. Л. Круглова, Д. А. Кунижева — DOI: 10.26794/2587-5671-2025-29-6-107-120. // Финансы: теория и практика. — 2025. — № 29(6). — С. 107–120. — EDN: RQEGDG.
18. Стрельцова, Е. Методологические подходы к измерению уровня цифровых навыков населения / Е. Стрельцова, Е. Попов. — URL: <https://rosstat.gov.ru/storage/mediabank/Streltsova-Popov.pdf> (дата обращения: 01.08.2026).

Stolyarova Natalia Arturovna

«Scientific and Production «Special Equipment and Communications»
Association of the Ministry of Internal Affairs of the Russian Federation, Moscow, Russia
E-mail: vash.shilyaev@yandex.ru

Tufetulov Aidar Miralimovich

Kazan (Volga Region) Federal University, Kazan, Russia
Institute of Management, Economics and Finance
E-mail: ajdar-t@yandex.ru
ORCID: <https://orcid.org/0000-0003-2204-5667>
RSCI: https://elibrary.ru/author_profile.asp?id=455967

Ibragimova Gulia Magdutovna

Kazan (Volga region) Federal University, Kazan, Russia
E-mail: gulyk@yandex.ru

Developing digital competencies as a tool for ensuring household economic security in the modern economy

Abstract. This study analyzes the factors that contribute to household economic security in modern Russia. The introduction of digital technologies into all spheres of Russian society has led to an improvement in the quality of life and has simultaneously given rise to new threats. This necessitates integrating tools into the economic security system that take into account the role of digital competencies in enhancing household protection from criminals who use high technology to commit illegal acts aimed at seizing individuals' financial assets. The analysis of this new type of threat prompted the introduction of the term «digital prevention» into scientific discourse. This term refers to a household's ability to anticipate threats and take action to prevent them through the use of specific digital skills, cognitive patterns, and behavioral attitudes. The study's premise is the potential of household financial behavior models, the use of which has enabled Russian researchers to uncover the conceptual framework of «household economic security». The study developed a «Threat to Economic Security / Digital Competence of a Preventive Nature» matrix, which helps identify economic security threats and substantiate management tools. To assess the level of household security, a Household Digital Vulnerability Index and a methodological approach to its calculation are proposed. This involves scoring (on a scale from 0 to 100) three key parameters: the level of openness of personal and financial household information; the frequency of cyber threats encountered by household members during the reporting period; and the presence and frequency of preventive measures. It is concluded that the level of digital competencies influences interregional digital divides. The study provides a mechanism for developing preventive digital competencies that detail the distribution of roles, cyber threat management tools, and expected effects. The authors conclude that it is necessary to include in Russian government policy documents regulating activities to ensure economic security an expanded list of threats to the loss of household financial assets and preventive tools for preventing the consequences of these threats. The potential of artificial intelligence in developing household digital competencies has been identified as an area for further research.

Keywords: household economic security; cyber threats; Household Digital Vulnerability Index; digital prevention; preventive digital competencies; interregional digital divides; artificial intelligence