УДК 336

ЛИЧНАЯ ФИНАНСОВАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ

Копнин А.А.

ассистент кафедры бизнес-информатики

Уральский государственный экономический университет

г. Екатеринбург, Россия

Александровский Г.А.

студент

Уральский государственный экономический университет

г. Екатеринбург, Россия

Аннотация

В статье проводится комплексное исследование личной финансовой безопасности в контексте ускоренной цифровизации экономики и общества. Цель работы заключается в системном анализе современных угроз и уязвимостей, формирующих риски для финансовых активов индивидуума, и разработке на этой основе практических рекомендаций по повышению уровня защищённости населения. Методологическую основу составили анализ научной литературы, структуризация и классификация угроз, а также изучение статистических данных, характеризующих социально-демографический портрет жертв финансового мошенничества. В результате исследования уточнено понятие личной финансовой безопасности, разработана классификация угроз на внутренние и внешние, определены ключевые взаимосвязи с понятиями финансовой грамотности, кибербезопасности и экономической безопасности личности. Эмпирически выявлена и охарактеризована наиболее уязвимая группа населения, определены доминирующие каналы мошеннических атак и проблемные аспекты поведения жертв. Научная новизна заключается в интегрированном подходе к

рассмотрению личной финансовой безопасности как динамической способности, зависящей от внутренних компетенций и внешних условий цифровой среды. Практическая значимость работы определяется сформулированным комплексом адресных мер для населения, регуляторов и финансовых организаций, направленных на формирование культуры финансовой безопасности и снижение уровня латентности киберпреступлений.

Ключевые слова: личная финансовая безопасность, цифровизация, финансовое мошенничество, киберпреступность, финансовая грамотность, кибербезопасность, социально-демографические группы риска, телефонное мошенничество, уязвимости, устойчивость.

PERSONAL FINANCIAL SECURITY IN THE AGE OF DIGITALIZATION: AN ANALYSIS OF THREATS AND VULNERABILITIES

Kopnin A.A.
Assistant Professor, Department of Business Informatics
Ural State University of Economics
Yekaterinburg, Russia
Aleksandrovsky G.A.
Student
Ural State University of Economics
Yekaterinburg, Russia

Abstract

This article conducts a comprehensive study of personal financial security in the context of the accelerated digitalization of the economy and society. The objective of the study is to systematically analyze modern threats and vulnerabilities that pose risks to individual financial assets and, based on these findings, develop practical

recommendations for improving public security. The methodological basis consists of an analysis of scientific literature, the structuring and classification of threats, and the study of statistical data characterizing the socio-demographic profile of financial fraud victims. The study clarified the concept of personal financial security, developed a classification of threats into internal and external, and identified key relationships with the concepts of financial literacy, cybersecurity, and individual economic security. The most vulnerable population group was empirically identified and characterized, the dominant channels of fraudulent attacks, and problematic aspects of victim behavior were determined. The scientific novelty lies in the integrated approach to considering personal financial security as a dynamic capability dependent on internal competencies and the external conditions of the digital environment. The practical significance of this work is determined by the formulated set of targeted measures for the population, regulators, and financial organizations aimed at developing a culture of financial security and reducing the latency of cybercrime.

Keywords: personal financial security, digitalization, financial fraud, cybercrime, financial literacy, cybersecurity, socio-demographic risk groups, telephone fraud, vulnerabilities, resilience.

Введение

Актуальность исследования проблем личной финансовой безопасности в современных условиях определяется интенсивным развитием цифровых технологий и сопутствующим ростом разнообразных угроз, которые оказывают давление как на отдельных индивидов, так и на экономическую систему в целом, подрывая её устойчивость [4, 7, 8]. Современная финансовая среда требует от человека постоянной адаптации к стремительно развивающейся цифровизации. Каждое нововведение, созданное для обеспечения защиты или для более удобного оборота денежных средств,

обусловливает необходимость повышения уровня финансовой грамотности, в то время как каждая новая схема обмана становится всё более технологичной, что ведёт к возрастающей уязвимости общества перед мошенниками [5].

В этой связи личная финансовая безопасность превращается в неотъемлемый элемент устойчивого и благополучного функционирования как на уровне домохозяйств, так и в масштабах экономики. Однако наблюдается заметное несоответствие между постоянно эволюционирующим уровнем современных угроз и степенью готовности к ним населения. Данное противоречие формирует основную проблемную область, требующую детального изучения.

Объектом исследования выступают сфера экономики и основы финансовой грамотности, а предметом — личная финансовая защищённость людей в цифровую эпоху. Целью данной работы является исследование спектра угроз личной финансовой безопасности в современной цифровой среде и, на основе анализа статистических данных и теоретических положений, выработка практических рекомендаций, направленных на повышение уровня защищённости населения. В рамках достижения поставленной цели рассматривается вопрос о том, в какой мере высокая финансовая грамотность способна устранить уязвимость индивидов перед финансовыми рисками и мошенническими схемами [2, 6, 9].

Результаты исследования

Проведенный анализ позволил сформулировать авторское определение ключевой категории исследования. Личная финансовая безопасность понимается как состояние защищенности финансовых активов индивидуума от внутренних и внешних угроз, обеспечивающее устойчивость его финансовой системы и достижение жизненных целей. В более динамичной трактовке — это не статичное состояние, а способность человека осознавать имеющиеся риски и оперативно находить адекватные ответы на них, что формирует основу для финансовой устойчивости и развития.

Центральным элементом анализа стало структурирование угроз личной финансовой безопасности, которые разделяются на две фундаментальные группы: внешние (неподконтрольные индивидууму) и внутренние (связанные с его личными компетенциями и поведением). Классификация и характеристика угроз представлены в Таблице 1.

Таблица 1 – Классификация угроз личной финансовой безопасности в условиях цифровизации

Группа угроз	**Конкретные виды угроз**	**Характеристика и механизм воздействия**
ВНЕШНИЕ УГРОЗЫ (Неподконтрольны индивидууму, требуют готовности к адаптации)	1. Финансовое мошенничество	Совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения. Основано на методах социальной инженерии [4].
	2. Киберпреступность	Деятельность, в которой цифровые устройства и сети используются как инструмент (хищение данных, хакерские атаки) или как цель (распространение вредоносного ПО). Не всегда сопряжена с прямым финансовым мошенничеством, но создает для него условия.
	3. Макроэкономические факторы	Системные экономические процессы, напрямую влияющие на благосостояние: инфляция, экономические кризисы, девальвация.
	4. Правовые лакуны (пробелы)	Использование злоумышленниками слабых мест или пробелов в законодательстве для создания новых схем обмана и ухода от ответственности.
	5. Природные катаклизмы	Масштабные природные явления, способные привести к резкой потере активов, доходов и необходимости неплановых расходов.
ВНУТРЕННИЕ УГРОЗЫ (Подконтрольны индивидууму, требуют работы над собой)	1. Низкая финансовая грамотность	Неспособность планировать бюджет, оценивать инвестиционные риски, понимать финансовые продукты, что ведет к нерациональным решениям [2].
	2. Нерациональное финансовое поведение	Недисциплинированные траты (импульсивные покупки), чрезмерная долговая нагрузка, отсутствие сбережений.

	3. Психологические факторы	Подверженность когнитивным искажениям: самоуверенность, стадное поведение на рынках, склонность к риску.
	4. Цифровая беспечность	Несоблюдение правил безопасности при использовании онлайн-банкинга, платежных систем и личных данных в интернете.
	5. Профессиональная и личная стагнация	Отсутствие стремления к повышению доходов через обучение, смену работы или поиск дополнительных источников, что снижает финансовую устойчивость в долгосрочной перспективе.

Исследование подтвердило, что для эффективного противостояния внешним угрозам необходимо в первую очередь минимизировать внутренние уязвимости. Без базовой финансовой грамотности, дисциплины и цифровой осознанности выстроить надежную защиту практически невозможно.

Далее был проанализирован концептуальный каркас личной финансовой безопасности через ее взаимосвязь со смежными понятиями (Таблица 2). Анализ показал, что финансовая безопасность является ядром более широкой системы защиты личности.

Таблица 2 – Взаимосвязь личной финансовой безопасности со смежными понятиями

Понятие	**Сущность**	**Связь с личной финансовой безопасностью и роль в системе защиты**
Финансовая грамотность	Сочетание осведомленности, знаний, навыков, установок и поведения, необходимых для принятия разумных финансовых решений [2].	Базовый инструментарий. Формирует основу для осознания рисков, управления личными финансами и противодействия внутренним угрозам. Без нее невозможна устойчивость системы.
Кибербезопасность	Совокупность методов защиты компьютеров, сетей, мобильных устройств и данных от	Технический щит. Обеспечивает защиту от ключевых внешних угроз в цифровой среде (мошенничество, кража данных). Является необходимым

	злоумышленных атак [3].	условием безопасности онлайн-операций и данных.
Экономическая безопасность личности	Состояние защищенности жизненно важных интересов человека в экономической сфере, способность противостоять угрозам.	Системный контекст. Личная финансовая безопасность выступает финансовой основой экономической безопасности личности. Нестабильность в финансах ведет к уязвимости в других сферах: социальной, имущественной, психологической.

Личная финансовая безопасность, финансовая грамотность, кибербезопасность и экономическая безопасность личности образуют единую систему защиты индивидуума. Финансовая грамотность обеспечивает компетенцию, кибербезопасность — технологическую защиту, а экономическая безопасность личности задает широкий контекст, в котором финансовая составляющая является критически важной.

Роль личной финансовой безопасности заключается в создании качественной опоры и стабилизации положения человека в экономике. Она позволяет не только парировать угрозы, но и снижать общую уязвимость, создавая пространство для свободы действий и развития. Отсутствие такой опоры ведет к цепной реакции: финансовые потери усиливают стресс, подрывают здоровье, увеличивают риск стать жертвой преступлений и, в конечном итоге, лишают человека экономической субъектности, вынуждая действовать под давлением обстоятельств.

Как следует из теоретической части, ключевой и наиболее массовой угрозой личной финансовой безопасности в цифровой среде является финансовое мошенничество. Для разработки эффективных превентивных мер критически важно идентифицировать наиболее уязвимые социально-демографические группы. На основе анализа статистических данных [9] была составлена обобщенная характеристика групп риска и методов воздействия злоумышленников.

Демографический портрет наиболее уязвимой группы. Данные представлены в Таблице 3, которая интегрирует ключевые факторы риска.

Таблица 3 – Социально-демографические характеристики жертв финансового мошенничества (по данным исследования [9]

Критерий	**Категория**	**Доля среди жертв, %**	**Комментарий и интерпретация**
Возраст	25 – 44 года	36,1	Наиболее экономически активная часть населения, активно пользующаяся финансовыми услугами и цифровыми сервисами, что расширяет поверхность для атаки.
	45 – 64 года	27,5	Группа, обладающая накоплениями, но часто с менее адаптированными цифровыми навыками по сравнению с молодежью.
Пол	Женский	52,6	Незначительное, но статистическое преобладание. Может быть связано с более частым исполнением роли распорядителя семейного бюджета и, как следствие, с большим объемом финансовых операций.
Образование	Среднее	42,7	Наибольшая доля, что может коррелировать с уровнем цифровой и финансовой грамотности, не всегда адекватным для распознавания сложных схем.
Уровень дохода	Средний	46,2	Наличие финансовых ресурсов, достаточных для интереса мошенников, при потенциально более высокой, чем у низкодоходной группы, финансовой нагрузке и спешке при принятии решений.

Наиболее подверженной мошенническим действиям является группа женщин в возрасте 25-44 лет, со средним уровнем образования и средним доходом. Эта группа сочетает в себе высокую финансовую и цифровую активность с потенциальными пробелами в специфических знаниях по кибербезопасности, что делает ее ключевой мишенью для злоумышленников. Выделение условной «наименее уязвимой» группы (14-24 года, высшее образование, высокий доход) статистически некорректно, так как подобное сочетание социальных статусов в реальности практически не встречается в данной возрастной когорте.

Доминирующие каналы атаки. Анализ предпочитаемых мошенниками способов связи (Таблица 4) выявляет явного лидера.

Таблица 4 – Распределение способов связи, используемых мошенниками для первоначального контакта [9]

Способ связи	**Доля случаев, %**	**Причины эффективности и выгоды для преступника**
Телефонный звонок или SMS	45,6	1. Эффект внезапности и психологического давления: ограничение времени на обдумывание, эмоциональная манипуляция. 2. Технологическая доступность и дешевизна: использование программ автодозвона и массовой рассылки SMS. 3. Низкий порог входа: не требует глубоких технических навыков, в отличие от хакерских атак.
Мессенджеры (WhatsApp, Telegram и др.)	15,7	Более персонализированный подход, возможность маскировки под знакомых или официальные лица.
Социальные сети	10,3	Использование доверия в рамках социальных связей, создание фейковых профилей.
Электронная почта	7,7	Фишинг, маскировка под официальные письма от банков или госорганов.
Взлом/подделка аккаунтов на портале «Госуслуги»	7,0	Высокий уровень доверия жертвы к официальному государственному ресурсу.

Телефон остается главным оружием мошенника благодаря своей проникающей способности, мгновенности и мощному психологическому эффекту, который минимизирует возможность рациональной оценки ситуации жертвой.

Последствия и реакция потерпевших. В случае успеха атаки злоумышленники чаще всего добиваются передачи конфиденциальных данных: кодов из SMS, реквизитов банковских карт, паспортных данных, а также побуждают к самостоятельным денежным переводам или установке вредоносного ПО.

Критически важным аспектом является дальнейшее поведение жертвы (Таблица 5). Хотя большинство (около 73%) предпринимают попытки защитить свои интересы, значительная доля (18,3%) не обращается никуда.

Таблица 5 – Реакция жертв финансового мошенничества [9]

Куда обратились	**Доля, %**	**Последствия выбора**
Банк / Финансовая организация	42,8	Наиболее быстрая реакция для блокировки операций и счетов.
Правоохранительные органы (полиция)	30,0	Запоздалая, но необходимая мера для документирования преступления и, потенциально, поимки преступников.
Никуда не обратились	18,3	Наиболее негативный сценарий: 1. Личный риск: потеря средств без шанса на возмещение; повышенная вероятность повторной атаки. 2. Системный риск: искажение реальной статистики, запаздывание в выявлении новых схем, что помогает преступникам укрепиться.

Проведенный анализ позволяет сформулировать ряд общих выводов, имеющих как теоретическое, так и прикладное значение для понимания и противодействия финансовому мошенничеству. Во-первых, идентифицирована группа максимального риска, которую составляют женщины в возрасте 25–44 лет, имеющие средний уровень дохода и образования. Их повышенная уязвимость обусловлена активной ролью в управлении финансами на фоне потенциальных пробелов в специализированных знаниях в области цифровой и финансовой безопасности. Во-вторых, установлено, что доминирующим вектором атаки остается телефонный звонок или SMS-сообщение. Данный канал является оптимальным для злоумышленников, так как сочетает высокую эффективность психологического воздействия, основанного на внезапности и создании искусственного дефицита времени, с технологической дешевизной и простотой организации. В-третьих, выявлена системная проблема пассивности значительной части жертв (около 18%), которые не обращаются за помощью после инцидента. Эта практика не только усугубляет их личные

финансовые потери, но и подрывает системные усилия по борьбе с киберпреступностью, так как ведет к существенной латентности преступлений и запаздыванию в выявлении новых мошеннических схем.

Практическая значимость полученных результатов заключается в возможности разработки адресных мер. Для населения ключевой рекомендацией является формирование условного рефлекса: при любом подозрительном контакте, особенно сопряженном с требованием конфиденциальных данных или срочных действий, необходимо немедленно прекратить коммуникацию и самостоятельно, по официальному номеру, полученному с верифицированного сайта, связаться с организацией, от имени которой действовал злоумышленник, для проверки информации. Для регуляторов и финансовых институтов приоритетом должна стать разработка и продвижение просветительских кампаний, сфокусированных именно на выявленной группе риска, с акцентом на простые и понятные алгоритмы поведения в случае телефонной атаки [1, 10]. Параллельно необходимо максимально упростить и популяризировать встроенные в мобильные приложения банков механизмы оперативного информирования о попытках мошенничества. Для общества в целом важнейшей задачей становится формирование новой социальной нормы — культуры обязательного сообщения о любых фактах мошеннических попыток, включая те, что не привели к ущербу. Каждый такой сигнал представляет собой ценный источник данных для аналитики и позволяет создать систему раннего предупреждения.

Прогноз развития ситуации при сохранении текущих негативных тенденций носит тревожный характер. Без консолидированного и активного противодействия, включающего массовое информирование, можно ожидать дальнейшей эскалации угроз. Это проявится в усложнении и повышении изощренности мошеннических схем, целенаправленно эксплуатирующих выявленные уязвимости. Долгосрочным следствием станет эрозия доверия граждан не только к случайным звонкам, но и к легитимным финансовым

институтам и цифровым сервисам в целом. Страх стать жертвой может стать существенным психологическим барьером, сдерживающим процесс цифровизации экономики, так как пользователи будут опасаться пользоваться онлайн-каналами. Наконец, рост латентности преступлений создаст опасную иллюзию статистического благополучия на фоне реально растущих и трансформирующихся угроз.

Эффективное противодействие финансовому мошенничеству в условиях цифровизации представляет собой комплексную задачу, выходящую за рамки индивидуальной бдительности. Оно требует формирования ответственной общественной позиции, при которой каждый акт информирования о попытке обмана рассматривается как необходимый вклад в коллективную безопасность, а усилия государственных регуляторов, финансового сектора и гражданского общества синхронизированы для создания многоуровневой системы защиты.

Заключение

Проведённое исследование подтверждает, что в условиях повсеместной цифровизации личная финансовая безопасность трансформируется из второстепенной задачи в критический элемент экономического благополучия и социальной стабильности как отдельного человека, так и общества в целом. Работа позволила достичь поставленной цели, системно проанализировав спектр угроз и выявив ключевые уязвимости.

Основным теоретическим результатом стало уточнение категории личной финансовой безопасности, которая интерпретируется не как статичное состояние, а как динамическая способность человека осознавать риски и адекватно на них реагировать. Разработанная классификация разделила угрозы на внутренние (низкая финансовая грамотность, нерациональное поведение) и внешние (мошенничество, киберпреступность, макроэкономические факторы), что позволило наглядно продемонстрировать их взаимосвязь и кумулятивный эффект. Установлено, что финансовая безопасность является

ядром в системе смежных понятий, где финансовая грамотность служит инструментарием, кибербезопасность — техническим щитом, а экономическая безопасность личности — системным контекстом.

Важным эмпирическим вкладом является идентификация социально-демографического портрета наиболее уязвимой группы — женщин в возрасте 25–44 лет со средним уровнем дохода и образования, что обусловлено высокой финансовой активностью при возможных пробелах в специализированных знаниях. Установлено, что доминирующим и наиболее эффективным для преступников каналом атаки остаётся телефонный звонок или SMS-сообщение, эксплуатирующий фактор внезапности и психологического давления. Выявленная системная проблема — пассивность значительной доли жертв, не обращающихся за помощью, — указывает на высокую латентность преступлений и искажение реальной картины угроз, что существенно затрудняет борьбу с ними.

На основе проведённого анализа сформулирован комплекс практических рекомендаций разного уровня: от выработки у населения условного рефлекса на проверку подозрительных контактов до адресных просветительских кампаний для групп риска и упрощения механизмов информирования финансовых организаций. Подчёркивается необходимость формирования новой социальной нормы, при которой сообщение о любой попытке мошенничества становится коллективной ответственностью.

Обеспечение личной финансовой безопасности в цифровую эпоху представляет собой многомерную задачу, требующую синхронизированных усилий на индивидуальном, институциональном и общегосударственном уровнях. Дальнейшие исследования могут быть направлены на количественную оценку эффективности предлагаемых мер, углублённый анализ региональной специфики угроз и разработку цифровых инструментов для персонального управления финансовыми рисками в реальном времени.

Библиографический список

1. Антипин, И. А. Цифровые технологии в развитии территорий: возможности и проблемы применения в практике государственного и муниципального управления / И. А. Антипин, Н. Ю. Власова, Е. А. Шишкина // Управленец. – 2024. – Т. 15, № 6. – С. 17–29. – DOI: 10.29141/2218-5003-2024-15-6-2. – EDN DNMGAN.

2. Баженова, А. А. Актуальные проблемы личной финансовой безопасности / А. А. Баженова // Современные вызовы и тренды в повышении финансовой грамотности и защиты прав потребителей финансовых услуг : материалы IX Всерос. науч.-практ. конф., посвящ. 90-летию Ин-та развития образования Респ. Башкортостан : в 2 т. Уфа, 28 окт. 2022 г. – Уфа : Первая типография, 2022. – С. 90–91. – EDN HGDEON.

3. Борисенко, А. В. Понятие кибербезопасности. Кибербезопасность государственных органов / А. В. Борисенко // Актуальные проблемы развития экономических, финансовых и кредитных систем : сб. материалов X Междунар. науч.-практ. конф., Белгород, 15 сент. 2022 г. – Белгород : Белгор. гос. нац. исслед. ун-т, 2022. – С. 297–299. – EDN EHEYOF.

4. Мельникова, Д. А. Актуальные проблемы личной финансовой безопасности / Д. А. Мельникова, К. И. Кулагина // Современные вызовы и тренды в повышении финансовной грамотности и защиты прав потребителей финансовых услуг : материалы IX Всерос. науч.-практ. конф., посвящ. 90-летию Ин-та развития образования Респ. Башкортостан : в 2 т. Уфа, 28 окт. 2022 г. – Уфа : Первая типография, 2022. – С. 129–131. – EDN NTQYNN.

5. Мирякова, Н. А. Проблемы личной финансовой безопасности в условиях развития цифровой экосистемы / Н. А. Мирякова // Современные вызовы и тренды в повышении финансовой грамотности и защиты прав потребителей финансовых услуг : материалы IX Всерос. науч.-практ. конф., посвящ. 90-летию Ин-та развития образования Респ. Башкортостан : в 2 т. Уфа, 28 окт. 2022 г. – Уфа : Первая типография, 2022. – С. 134–136. – EDN DSMYJF.

6. Рысенкова, Д. А. Финансовое мошенничество – проблема личной финансовой безопасности / Д. А. Рысенкова // Современные вызовы и тренды в повышении финансовой грамотности и защиты прав потребителей финансовых услуг : материалы IX Всерос. науч.-практ. конф., посвящ. 90-летию Ин-та развития образования Респ. Башкортостан : в 2 т. Уфа, 28 окт. 2022 г. – Уфа : Первая типография, 2022. – С. 142–144. – EDN EOZNJA.

7. Смагин, Н. С. Актуальные проблемы личной финансовой безопасности / Н. С. Смагин // Современные вызовы и тренды в повышении финансовой грамотности и защиты прав потребителей финансовых услуг : материалы IX Всерос. науч.-практ. конф., посвящ. 90-летию Ин-та развития образования Респ. Башкортостан : в 2 т. Уфа, 28 окт. 2022 г. – Уфа : Первая типография, 2022. – С. 154–156. – EDN DNHIBL.

8. Тазетдинов, И. Ф. Актуальные проблемы личной финансовой безопасности / И. Ф. Тазетдинов // Современные вызовы и тренды в повышении финансовой грамотности и защиты прав потребителей финансовых услуг : материалы IX Всерос. науч.-практ. конф., посвящ. 90-летию Ин-та развития образования Респ. Башкортостан : в 2 т. Уфа, 28 окт. 2022 г. – Уфа : Первая типография, 2022. – С. 157–158. – EDN TPDKDE.

9. Центральный банк Российской Федерации [Электронный ресурс]. – URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 30.11.2025).

10. Acar, K. T. Research trends in digital marketing and data-driven marketing: A bibliometric analysis / K. T. Acar, F. Orman // The Manager. – 2024. – Vol. 15, No. 6. – P. 48–59. – DOI: 10.29141/2218-5003-2024-15-6-4. – EDN OWWAAG.

Оригинальность 95%