УДК 330.378.
DOI 10.26118/2782-4586.2026.48.71.011

Фрик Ольга Владимировна
Омский государственный аграрный университет им. П.А. Столыпина

Компетенции в области цифровой безопасности как фактор финансового поведения студенческой молодежи: эмпирическая оценка (на примере аграрного вуза)

Аннотация. Интенсификация цифровизации финансовых услуг актуализирует вопросы защиты персональных данных и активов пользователей. Студенчество, активно использующее цифровые каналы для финансовых операций, представляет группу, подверженную киберрискам. Цель исследования — оценка уровня осведомленности и практических навыков в сфере цифровой безопасности среди студентов аграрного вуза. Методологической основой выступило онлайн-анкетирование первокурсников (N=276), проведенное осенью 2025 года. Результаты демонстрируют высокую когнитивную осведомленность об основных угрозах (риски публичного Wi-Fi, фишинг), но недостаточную имплементацию технических средств защиты, таких как двухфакторная аутентификация. Выявлен диссонанс между знанием правил безопасности и их повседневным применением. Практическая значимость работы заключается в обосновании необходимости интеграции в образовательные программы практико-ориентированных модулей по цифровой гигиене и кибербезопасности.

Ключевые слова: цифровая безопасность, киберриски, финансовая грамотность, студенческая молодежь, цифровизация, фишинг, двухфакторная аутентификация.

Frik Olga Vladimirovna
Omsk State Agrarian University named after P.A. Stolypin

Digital security competencies as a factor in financial behavior of young students: an empirical assessment (using an agricultural university as an example)

Abstract. The intensification of digitalization of financial services raises the issue of protecting users' personal data and assets. Students who actively use digital channels for financial transactions represent a group vulnerable to cyber risks. The aim of this study was to assess the level of awareness and practical skills in digital security among students at an agricultural university. An online survey of first-year students (N=276) conducted in the fall of 2025 served as the methodological basis. The results demonstrate a high level of cognitive awareness of key threats (risks of public Wi-Fi, phishing), but insufficient implementation of technical security measures, such as two-factor authentication. A dissonance was identified between knowledge of security rules and their everyday application. The practical significance of this study lies in its substantiation of the need to integrate practice-oriented modules on digital hygiene and cybersecurity into educational programs.

Keywords: Digital security, cyber risks, financial literacy, students, digitalization, phishing, two-factor authentication.

Введение

Трансформация финансового ландшафта под влиянием цифровых технологий сопровождается ростом сопутствующих киберрисков. Молодое поколение, являясь наиболее активным пользователем финтех-сервисов, одновременно становится потенциальной мишенью для мошеннических схем. Формирование устойчивых навыков цифровой безопасности является неотъемлемым компонентом современной финансовой грамотности, обеспечивающим не только защиту средств, но и доверие к цифровой экономике в целом.

Несмотря на растущий объем исследований, посвященных финансовой грамотности вообще, и молодежи, в частности [1; 2; 3; 4; 5], аспект практических поведенческих

паттернов в области кибербезопасности остается недостаточно изученным, особенно в контексте специфических студенческих групп, таких как обучающиеся аграрных вузов. Преодоление данного пробела позволит разработать более адресные образовательные и просветительские меры. Автором статьи ранее проводились исследования различных аспектов финансовой грамотности. [6; 7; 8; 9; 10]

Целью данного исследования является эмпирическая оценка знаний и поведенческих установок студентов первого курса аграрного университета в сфере цифровой безопасности при совершении финансовых операций.

В соответствии с целью были поставлены следующие задачи:

1. Оценить уровень осведомленности студенческой молодежи о потенциальных угрозах, связанных с использованием небезопасных каналов связи (на примере публичных сетей Wi-Fi) для совершения финансовых операций.

2. Проанализировать поведенческие паттерны респондентов при столкновении с типичными методами социальной инженерии (фишинг) и выявить распространенность безопасных и рискованных реакций.

3. Исследовать степень внедрения и использования технических средств усиленной защиты, в частности двухфакторной аутентификации, в практике взаимодействия с финансовыми приложениями.

4. Определить наличие и характер возможных противоречий между теоретической осведомленностью о правилах цифровой безопасности и их практической реализацией в повседневном финансовом поведении.

5. На основе выявленных тенденций сформулировать рекомендации по направленному развитию компетенций в области цифровой гигиены в рамках образовательных программ для студенческой аудитории.

Эти задачи направлены на системное изучение трех ключевых аспектов цифровой безопасности: когнитивного (понимание рисков), поведенческого (действия при угрозах) и технологического (применение инструментов защиты).

Гипотеза исследования заключается в наличии у студенческой молодежи (поколения Z), обучающейся в аграрном вузе, противоречия в сфере цифровой безопасности: при высокой когнитивной осведомленности о базовых киберрисках наблюдается недостаточная практическая имплементация продвинутых технических средств защиты (например, двухфакторной аутентификации).

Объектом исследования выступает финансовое поведение студенческой молодежи (поколения Z) в условиях цифровой трансформации экономики.

Предметом исследования уровень знаний и практических компетенций в области цифровой безопасности при совершении финансовых операций в интернет-среде.

Научная новизна представленного исследования заключается в следующем комплексе положений:

1) Комплексный междисциплинарный ракурс. Впервые в рамках одного эмпирического исследования проведено комплексное изучение цифровых финансовых практик студенческой молодежи, совмещающее три ключевых ракурса: технологический (анализ частоты и спектра использования цифровых инструментов), поведенческо-экономический (изучение глубинных установок планирования и кредитования) и кибергигиенический (оценка компетенций цифровой безопасности). Такой подход позволяет преодолеть фрагментарность существующих исследований, чаще фокусирующихся на одном из этих аспектов.

2) Фокус на специфической профессионально-образовательной группе. Новизна заключается в выборе в качестве объекта эмпирического анализа ранее не изучавшейся в данном контексте группы — студентов первого курса аграрного вуза. Это позволяет верифицировать общетеоретические выводы о поколении Z на уникальном материале, учитывающем потенциальную отраслевую и социально-профессиональную специфику будущих специалистов АПК.

3) Эмпирическая фиксация «парадокса цифровой компетентности». На уникальных эмпирических данных выявлен и описан структурный парадокс (диссонанс) в поведении респондентов: между высоким уровнем когнитивной осведомленности о базовых киберрисках и недостаточной практической реализацией продвинутых защитных мер (двухфакторная аутентификация). Концептуализация данного диссонанса вносит вклад в развитие поведенческой финансовой теории.

4) Интеграция компонента цифровой безопасности в структуру финансовой грамотности. Исследование операционализирует и эмпирически оценивает цифровую гигиену как неотъемлемый практический компонент финансовой грамотности современного пользователя, смещая акцент с только экономических и правовых знаний на поведенческие алгоритмы защиты активов в цифровой среде.

5) Методологический вклад. Новизна проявляется в дизайне исследовательского инструментария, позволяющего в рамках одного опроса коррелировать данные об операционных привычках, глубинных установках и практиках безопасности, что обеспечивает целостность анализа детерминант финансового поведения.

Итак, научная новизна работы заключается не в открытии абсолютно новых феноменов, а в комплексном, интегрированном и эмпирически обоснованном изучении взаимосвязи ключевых аспектов цифрового финансового поведения в конкретной, релевантной и ранее недостаточно изученной социально-демографической и профессиональной группе, что позволяет перейти от общих описаний к адресным теоретическим выводам и практическим рекомендациям.

Методологическая основа

Для достижения поставленной цели был применен количественный метод сбора данных. Основным инструментом выступило анонимное онлайн-анкетирование на платформе Yandex Forms, проведенное в октябре-ноябре 2025 года среди студентов первого курса Омского государственного аграрного университета имени П.А. Столыпина. Объем выборки составил 276 человек, что является репрезентативным для проведения внутривузовского исследования. Выбор в качестве объекта исследования студентов начальных курсов является методически обоснованным, поскольку позволяет зафиксировать и проанализировать исходные, наименее институционализированные модели финансового поведения. Данный период совпадает с ключевым этапом социально-экономической адаптации к статусу самостоятельного потребителя, что обеспечивает получение релевантных данных для изучения устойчивых поколенческих трендов, не искаженных длительным профессиональным опытом.

Методологический инструментарий, направленный на диагностику компетенций в сфере цифровой безопасности, был разработан как органичная часть развернутого научного проекта. Стратегической целью данного проекта выступает системное исследование структурных элементов цифровой финансовой грамотности и детерминант финансового поведения в студенческой среде. Полученные эмпирические результаты вносят вклад в развитие теоретического аппарата поведенческих финансов, расширяя границы его применения для анализа специфики молодежных аудиторий.

Опросный блок, посвященный цифровой безопасности, включал три вопроса, направленных на оценку:

- Осознания рисков, связанных с использованием небезопасных каналов связи.
- Поведенческой реакции на потенциальные фишинговые атаки.
- Применения технических средств усиленной защиты аккаунтов.

Обработка данных осуществлялась с помощью методов описательной статистики и визуализации результатов.

Анализ знаний и навыков в области цифровой безопасности

Студенчество как ключевая группа поколения Z обладает социальными и экономическими установками, изначально сформированными в контексте цифровой трансформации и глобальной взаимосвязи процессов. Данная специфика формирует

императив развития у этой аудитории особых компетенций, обеспечивающих гибкость и устойчивость их личных финансовых моделей в динамичной среде.

Проанализируем блок исследования под названием «Знания и навыки в области цифровой безопасности». Респондентам задавались следующие вопросы:

1. Согласны ли Вы с тем, что публичный Wi-Fi может быть небезопасен для проведения банковских операций? (возможные варианты ответа: Да, полностью согласен(на); Скорее согласен(на); Скорее не согласен(на); Нет, совершенно не согласен(на); Затрудняюсь ответить). Ответы представлены на рис. 1.

Рис. 1. Ответы респондентов на вопрос «Согласны ли Вы с тем, что публичный Wi-Fi может быть небезопасен для проведения банковских операций?»

2. Как Вы поступаете, получив SMS или email с просьбой перейти по ссылке и подтвердить свои банковские данные? (возможные варианты ответа: Никогда не перехожу по таким ссылкам и удаляю сообщение; Перехожу по ссылке, если сообщение выглядит правдоподобно; Сначала звоню в банк для проверки информации; Затрудняюсь ответить / Не сталкивался(ась)). Ответы представлены на рис. 2.

Рис. 2. Ответы респондентов на вопрос «Как Вы поступаете, получив SMS или email с просьбой перейти по ссылке и подтвердить свои банковские данные?»

3. Используете ли Вы двухфакторную аутентификацию (например, подтверждение входа по SMS или через приложение) для своих финансовых приложений? (возможные варианты ответов: Да, для всех; Только для некоторых; Нет, не использую; Не знаю, что это такое). Ответы представлены на рис. 3.

Рис. 3. Ответы респондентов на вопрос «Используете ли Вы двухфакторную аутентификацию (например, подтверждение входа по SMS или через приложение) для своих финансовых приложений?»

Анализ результатов эмпирического исследования и обсуждение

1. Восприятие рисков, связанных с каналами связи.

Большинство респондентов (более 80%) демонстрируют осведомленность об угрозах, исходящих от публичных сетей Wi-Fi. Совокупная доля ответов «Да, полностью согласен(на)» и «Скорее согласен(на)» составила 83,5%. Это указывает на сформированное понимание того, что открытые сети могут быть использованы для перехвата конфиденциальной финансовой информации. Лишь незначительная часть опрошенных (около 8%) отрицала наличие подобных рисков или затруднялась с ответом (Рис. 1). Данный результат является позитивным индикатором базового уровня цифровой грамотности в изучаемой группе.

2. Реакция на попытки фишинга.

Поведенческий аспект защиты от социальной инженерии был исследован через модель действий при получении подозрительного сообщения с просьбой подтвердить банковские данные. Обнадеживающим результатом является то, что подавляющее большинство студентов (84,7%) выбирают корректную и безопасную стратегию: «Никогда не перехожу по таким ссылкам и удаляю сообщение» (Рис. 2). Это свидетельствует об эффективности существующих информационных кампаний, предупреждающих о подобных угрозах. Вместе с тем, сохраняется рисковая группа (9,8%), готовая перейти по ссылке, если сообщение «выглядит правдоподобно», что подчеркивает необходимость дальнейшей работы по развитию критического мышления в цифровой среде.

3. Использование двухфакторной аутентификации (2FA).

Анализ применения технических средств защиты выявил наиболее проблемную зону. Несмотря на высокую осведомленность о базовых рисках, лишь 34,8% респондентов используют двухфакторную аутентификацию для всех своих финансовых приложений, а 15,2% — только для некоторых (Рис. 3). При этом 41,3% опрошенных указали, что не используют 2FA, а 8,7% — не знают о таком методе защиты. Это выявляет существенный разрыв между теоретическим знанием о необходимости безопасности и практическим внедрением дополнительных, но эффективных защитных барьеров. Низкий уровень использования 2FA повышает уязвимость аккаунтов к взлому даже в случае компрометации пароля.

Сформулированная автором гипотеза была подтверждена в ходе исследования. Речь идет о противоречии в сфере цифровой безопасности: при высокой когнитивной

осведомленности о базовых киберрисках у респондентов наблюдается недостаточная практическая имплементация продвинутых технических средств защиты (например, двухфакторной аутентификации).

Заключение

Проведенное эмпирическое исследование позволило оценить уровень компетенций студентов аграрного вуза в области цифровой финансовой безопасности. Полученные данные свидетельствуют о дифференцированной картине: высокий уровень когнитивной осведомленности об основных угрозах (публичный Wi-Fi, фишинг) сочетается с недостаточным внедрением ключевых технических средств защиты, в частности, двухфакторной аутентификации. Выявленный когнитивно-поведенческий диссонанс — понимание правил безопасности без их полного практического соблюдения — создает значительную зону риска. Студенты осознают опасность, но не всегда предпринимают достаточные меры для ее нейтрализации на технологическом уровне.

Практические рекомендации, вытекающие из исследования, заключаются в необходимости модернизации учебных курсов по финансовой грамотности. Акцент должен смещаться с пассивного информирования о рисках на активное формирование практических навыков:

- Проведение интерактивных мастер-классов по настройке и использованию двухфакторной аутентификации, менеджеров паролей.
- Моделирование реальных фишинговых атак в контролируемой среде для развития навыков их распознавания.
- Разработка четких алгоритмов действий при различных киберинцидентах.

Такие меры будут способствовать переходу от формальной осведомленности к выработке устойчивых и безопасных цифровых финансовых привычек.

Список источников

1. Богославцева, Л. В. Необходимость повышения финансовой грамотности населения с учетом цифровой трансформации государства / Л. В. Богославцева // К финансовой культуре через волонтерство, воспитание и просвещение : Материалы I Областного форума по финансовой грамотности, Ростов-на-Дону, 24–25 апреля 2025 года. – Ростов-на-Дону: Издательско-полиграфический комплекс РГЭУ (РИНХ), 2025. – С. 116-119. – EDN NFAZTK.
2. Гимранова, Г. Х. Цифровая финансовая грамотность в эпоху цифровой трансформации экономики / Г. Х. Гимранова // Экономика и управление: научно-практический журнал. – 2021. – № 1(157). – С. 98-102. – DOI 10.34773/EU.2021.1.20. – EDN JJFIBB.
3. Корытько, Т. Ю. Цифровая финансовая грамотность / Т. Ю. Корытько // Цифровая среда как инструмент модернизации и инновационного развития : Сборник статей Международной научно-практической конференции, Саратов, 27 сентября 2025 года. – Уфа: ООО "Омега сайнс", 2025. – С. 61-63. – EDN XXMZLI.
4. Ликсина, Е. В. «Академия финансов»: цифровой инструмент для повышения финансовой грамотности студентов / Е. В. Ликсина, К. А. Борисова, М. А. Мищенко // Социосфера. – 2025. – № 3. – С. 171-173. – EDN UDPJES.
5. Назарова, Е. Н. Развитие международных стандартов цифровой финансовой грамотности: вызовы и возможности для российской системы образования / Е. Н. Назарова, Н. А. Горев // Цифровая экономика: проблемы и перспективы развития : сборник научных статей 7-й Международной научно-практической конференции, в 2-х томах, Курск, 10 октября 2025 года. – Курск: Закрытое акционерное общество "Университетская книга", 2025. – С. 125-128. – EDN NXAISK.
6. Фрик, О. В. Исследование финансовой грамотности студенческой молодежи аграрного вуза через призму самооценки // Экономика, предпринимательство и право. – 2025. – Т. 15, № 6. – С. 4381-4394. – DOI 10.18334/epp.15.6.123135. – EDN DBDXSK.

7. Фрик, О. В., Евдохина, О.С. Особенности формирования сберегательных и инвестиционных стратегий у студентов аграрного вуза в контексте финансового поведения // Экономика, предпринимательство и право. – 2025. – Т. 15, № 7. – С. 5051-5066. – DOI 10.18334/epp.15.7.123354. – EDN TZOPIQ.

8. Фрик, О. В. Исследование вопросов финансовой грамотности студенчества в контексте рационального управления персональными ресурсами и стратегического финансового мышления // Каталог научных разработок ФГБОУ ВО "Омский государственный аграрный университет им. П.А. Столыпина". Серия "Гуманитарные науки" : Сборник статей. – Омск : Омский государственный аграрный университет им. П.А. Столыпина, 2025. – С. 52-54. – EDN OLEMWO.

9. Фрик, О. В. Развитие финансовой культуры студентов через интеграцию современных образовательных технологий в вузе // Каталог научных разработок ФГБОУ ВО "Омский государственный аграрный университет им. П.А. Столыпина". Серия "Гуманитарные науки" : Сборник статей. – Омск : Омский государственный аграрный университет им. П.А. Столыпина, 2025. – С. 56-58. – EDN QRXGDA.

10. Фрик, О. В. Проблемы и перспективы формирования финансовой культуры у обучающейся молодежи в системе высшего образования / О. В. Фрик // Каталог научных разработок ФГБОУ ВО "Омский государственный аграрный университет им. П.А. Столыпина". Серия "Гуманитарные науки" : Сборник статей. – Омск : Омский государственный аграрный университет им. П.А. Столыпина, 2025. – С. 54-56. – EDN ZSFCHA.

Сведения об авторе

Фрик Ольга Владимировна, кандидат философских наук, доцент, доцент кафедры философии, истории, экономической теории и права экономического факультета ФГБОУ ВО «Омский государственный аграрный университет им. П.А. Столыпина», г. Омск, Россия.

Information about the author

Frik Olga Vladimirovna, PhD in Philosophy, Associate Professor, Associate Professor of the Department of Philosophy, History, Economic Theory, and Law Faculty of Economics, P.A. Stolypin Omsk State Agrarian University, Omsk, Russia.