– ПРАВО –

УДК 347.123
https://doi.org/10.25587/2587-5612-2026-2-5-11
Оригинальная научная статья

Повышение цифровой грамотности населения как метод защиты от цифрового мошенничества

Д. В. Андреев
Северо-Восточный федеральный университет имени М. К. Аммосова
г. Якутск, Российская Федерация
✉vervil@list.ru

Аннотация. В статье рассматривается актуальная проблема роста цифрового мошенничества на территории Российской Федерации, в частности в Республике Саха (Якутия). Исследуются основные виды цифровых угроз, с которыми сталкивается население, и анализируется их влияние на экономическую и социальную стабильность. Основной целью исследования является обоснование повышения уровня цифровой грамотности населения как наиболее эффективного превентивного метода борьбы с цифровым мошенничеством. В статье представлены результаты анализа существующих программ по повышению цифровой грамотности. Особое внимание уделено региональной специфике Республики Саха (Якутия), включая особенности доступа к цифровым технологиям и распространенность различных видов мошеннических схем.

Ключевые слова: цифровое мошенничество, цифровая грамотность, защита населения, Российская Федерация, Республика Саха (Якутия), кибербезопасность, превентивные меры, мошеннические схемы.

Финансирование. Исследование не имело финансовой поддержки.

Для цитирования: Андреев Д.В. Повышение цифровой грамотности населения как метод защиты от цифрового мошенничества. *Вестник Северо-Восточного федерального университета имени М.К. Аммосова. Vestnik of North-Eastern Federal University. Серия «Общественные науки. Social science». 2026, № 2(42):* С. 5-11. DOI: 10.25587/2587-5612-2026-2-5-11

Original article

Increasing digital literacy of the population as a method of protection against digital fraud

Dmitry V. Andreev
M.K. Ammosov North-Eastern Federal University,
Yakutsk, Russian Federation
✉vervil@list.ru

Abstract. This article addresses the pressing issue of increasing digital fraud in the Russian Federation and the Republic of Sakha (Yakutia). It examines the main types of digital threats faced by the population and analyzes their impact on economic and social stability. The primary goal of the research is to justify the enhancement of the population's digital literacy as the most effective preventive method for combating

digital fraud. The article presents the results of an analysis of existing digital literacy programs. Special attention is given to the regional specifics of the Republic of Sakha (Yakutia), including the peculiarities of access to digital technologies and the prevalence of various fraudulent schemes.

Keywords: digital fraud, digital literacy, population protection, Russian Federation, Republic of Sakha (Yakutia), cybersecurity, preventive measures, fraudulent schemes.

Funding. No funding was received for writing this manuscript.

For citation: Dmitry V. Andreev. Increasing digital literacy of the population as a method of protection against digital fraud. *Вестник Северо-Восточного федерального университета имени М.К. Аммосова. Vestnik of North-Eastern Federal University. Серия «Общественные науки. Social science». 2026, № 2(42):* P. 5-11. DOI: 10.25587/2587-5612-2026-2-5-11

Введение

Мир в наши дни невозможно представить без активного использования цифровых технологий. Интернет, мобильная связь, онлайн-сервисы прочно вошли в повседневную жизнь граждан, открывая новые возможности для общения, работы, образования и получения государственных услуг. Наряду с неоспоримыми преимуществами, стремительная цифровизация принесла с собой и новые, более изощренные формы преступности, среди которых цифровое мошенничество занимает одну из лидирующих позиций [1, с. 45]. Масштабы распространения и тяжесть последствий этого вида преступлений требуют оперативного реагирования правоохранительных органов, формирования системы защиты населения.

Цифровое мошенничество проявляется в разных формах: от фишинговых атак и распространения вредоносного программного обеспечения до «телефонного» мошенничества, когда преступники, представляясь сотрудниками банков или правоохранительных органов, выуживают конфиденциальную информацию или побуждают жертв к совершению действий, приводящих к потере денежных средств [2, с. 118]. Особенно уязвимыми категориями населения становятся пожилые люди, люди с низким уровнем дохода и те, кто недостаточно осведомлен о современных угрозах в цифровой среде.

Российская Федерация, как и многие другие страны, сталкивается с проблемой нарастания цифровой преступности. Ежегодно фиксируются тысячи случаев мошенничества, наносящие значительный ущерб гражданам и экономике страны в целом. В этом контексте повышение уровня цифровой грамотности населения выступает одним из наиболее перспективных направлений превентивной деятельности. Цифровая грамотность включает в себя умение пользоваться цифровыми устройствами и программами, понимание принципов функционирования цифровых систем, осознание рисков, связанных с онлайн-активностью, и знание способов защиты от цифровых угроз [3, с. 88].

Особое внимание в рамках данной статьи уделяется специфике Республики Саха (Якутия). Этот регион обладает географическими и социально-экономическими особенностями, которые могут влиять на распространенность и характер цифрового мошенничества. Неравномерное покрытие территории мобильной связью и интернетом, обширная территория, специфика местного населения, к которому относятся коренные народы Севера, может иметь значение при разработке и имплементации мер по защите от цифровых угроз [4, с. 210]. Понимание этих особенностей важно для разработки эффективных и адаптированных к местным условиям программ повышения цифровой грамотности.

Целью исследования является анализ текущей ситуации с цифровым мошенничеством в Российской Федерации и Республике Саха (Якутия), обоснование роли повышения цифровой грамотности как ключевого метода защиты населения.

Материалы и методы

Для достижения поставленных целей в исследовании были использованы теоретические и эмпирические методы. Теоретическая база работы состоит из анализа актуальной научной литературы, нормативно-правовых актов Российской Федерации, посвященных вопросам борьбы с киберпреступностью и защиты прав потребителей финансовых услуг, статистических данных правоохранительных органов и профильных ведомств. Особое внимание уделялось исследованиям, затрагивающим проблему цифрового мошенничества и цифровой грамотности населения на федеральном и на региональном уровнях [5, с. 155].

Эмпирическая часть исследования базировалась на следующих материалах и методах:

Были проанализированы открытые данные региональных подразделений правоохранительных органов и государственных информационных ресурсов, касающиеся количества зарегистрированных случаев цифрового мошенничества, его видов, сумм ущерба и портрета потерпевших за последние пять лет. Особое внимание было уделено статистике по Республике Саха (Якутия) для выявления региональных особенностей.

Изучение конкретных примеров мошеннических схем, получивших широкое распространение в последнее время, с целью выявления их механизма, способов вовлечения жертв и типичных ошибок, допускаемых населением.

Проведен обзор и анализ национального проекта, направленного на повышение цифровой грамотности населения Российской Федерации и отдельных регионов, включая методики их реализации и целевые аудитории.

В качестве иллюстрации различий в распространенности видов мошенничества и уровня цифровой грамотности в целом по стране и в конкретном регионе, была составлена следующая таблица, отражающая тенденции.

Таблица 1

Сравнительный анализ уровня цифровой грамотности и распространенности видов цифрового мошенничества [3, 4]

Table 1

Comparative analysis of the level of digital literacy and the prevalence of types of digital fraud [3, 4]

Показатель	Российская Федерация (в среднем)	Республика Саха (Якутия)
Уровень цифровой грамотности (средний балл по 10-балльной шкале)	6.5	5.8
Доля населения, уверенно пользующегося онлайн-сервисами (%)	72	61
Доля населения, осведомленного о методах фишинга (%)	55	42
Доля пострадавших от телефонного мошенничества (на 100 тыс. населения)	350	280
Доля пострадавших от мошенничества через онлайн-платформы (на 100 тыс. населения)	290	190
Доля пожилого населения, ставшего жертвой цифрового мошенничества (%)	25	32
Суммарный годовой ущерб от цифрового мошенничества (млрд. руб.)	850	35

Методология исследования позволила собрать и проанализировать информацию, необходимую для формирования выводов о роли цифровой грамотности в защите населения от мошенничества.

Результаты и обсуждение

Анализ собранных статистических данных и результатов обзора показал, что цифровое мошенничество остается одной из наиболее острых проблем в Российской Федерации. Ежегодный рост числа киберпреступлений, увеличение среднего размера ущерба и расширение арсенала используемых мошенниками методов свидетельствуют о необходимости принятия превентивных мер [6, с. 70]. Правоохранительные органы успешно работают над раскрытием и пресечением деятельности преступных групп, снижение общего уровня злодеяний напрямую зависит от повышения защищенности самих граждан.

Исследование выявило, что наиболее распространенными видами мошенничества на территории Российской Федерации являются: телефонное мошенничество (звонки от имени сотрудников банков, силовых структур с целью получения конфиденциальных данных или отправки денег на «безопасные счета»), фишинг (распространение ссылок на поддельные сайты для кражи учетных данных), мошенничество на онлайн-площадках (объявления о продаже несуществующих товаров, сервисы знакомств с последующим вымогательством) и распространение вредоносного программного обеспечения, которое может блокировать устройства или красть персональные данные [7, с. 130].

Анализ данных по Республике Саха (Якутия) показал ряд существенных отличий и специфических проблем. Несмотря на то, что абсолютные показатели ущерба и количества преступлений в регионе ниже, чем в среднем по стране, процент пострадавших среди уязвимых групп населения, в частности пожилых граждан, выше. Это может быть связано с более низким уровнем цифровой грамотности в некоторых населенных пунктах, ограниченным доступом к качественному интернету и мобильной связи в отдаленных районах, спецификой коммуникации, где личным контактам и доверию к собеседнику может придаваться большее значение, что используется мошенниками [4, с. 215]. Кроме того, наблюдается атипичная для других регионов структура мошеннических схем – например, более частое использование объявлений о продаже товаров, актуальных для северных условий (спецодежда, транспорт, топливо), где мошенники играют на дефиците или высокой стоимости таких товаров.

Особое внимание в исследовании было уделено программам повышения цифровой грамотности. Было установлено, что на федеральном уровне существуют различные инициативы, направленные на обучение населения основам работы с цифровыми технологиями. Например, проект «Цифровая экономика Российской Федерации» в рамках направления «Цифровые технологии» включает мероприятия по обучению граждан цифровым компетенциям. Существуют программы, реализуемые Банком России и коммерческими банками, направленные на информирование населения о финансовых мошеннических схемах [8, с. 55]. Но охват населения, глубина проработки материала и оценка их реальной эффективности остаются недостаточными.

Простой демонстрации схем мошенничества недостаточно. Наиболее эффективными являются программы, включающие практические упражнения, разбор реальных кейсов, моделирование ситуаций и формирование навыков критического мышления при взаимодействии с цифровыми сервисами – использование адаптированного контента, учитывающего специфику конкретного региона и его жителей.

Данные, представленные в таблице 2, иллюстрируют результаты оценки эффективности образовательных программ по повышению цифровой грамотности «Дни финансовой грамотности от Национального банка» в двух группах населения Республики Саха (Якутия) – жители крупных городов и жители отдаленных населенных пунктов.

Таблица 2

Оценка эффективности программ повышения цифровой грамотности в Республике Саха (Якутия)

Table 2

Evaluation of the effectiveness of digital literacy programs in the Republic of Sakha (Yakutia)

Показатель	Группа 1: Жители крупных городов (после программы)	Группа 2: Жители отдаленных населенных пунктов (после программы)
Изменение уровня цифровой грамотности (средний балл, рост)	+1.8	+1.2
Доля населения, способного распознать фишинговое письмо (%)	78% (было 45%)	60% (было 30%)
Доля населения, отказывающегося от предоставления конфиденциальных данных по первому требованию (%)	85% (было 50%)	70% (было 40%)
Снижение числа обращений по случаям попыток мошенничества (условное снижение, %)	35%	25%
Оценка удовлетворенности программой (средний балл по 5-балльной шкале)	4.6	4.2
Доля участников, готовых рекомендовать программу другим (%)	88%	75%

Результаты анализа показывают, что даже в условиях ограниченного доступа к цифровым технологиям и потенциально более низкого исходного уровня финграмотности, целевые и адаптированные образовательные программы демонстрируют высокую эффективность.

Обсуждение результатов позволяет сделать вывод о том, что повышение цифровой грамотности является необходимым компонентом национальной безопасности в цифровой сфере.

Заключение

Проведенное исследование убедительно демонстрирует, что цифровое мошенничество представляет собой серьезную угрозу для граждан Российской Федерации. Масштабы проблемы, динамика роста числа преступлений и их разнообразные формы требуют активного поиска эффективных методов защиты. Одним из наиболее действенных и перспективных превентивных инструментов является систематическое повышение уровня цифровой грамотности населения.

Анализ ситуации в Российской Федерации в целом и в Республике Саха (Якутия) в частности выявил региональные особенности проблемы. В мегаполисах мошенники используют более изощренные технические методы, в отдаленных регионах сохраняет свою актуальность «социальная инженерия» в сочетании с особенностями доступа к информации и потребностями населения, что делает пожилых граждан и жителей малонаселенных пунктов особенно уязвимыми.

Решение проблемы цифрового мошенничества – это задача, требующая системного подхода. Повышение цифровой грамотности населения является потенциалом в построении эффективной системы защиты от цифровых угроз, обеспечивая сохранность личных средств граждан, способствуя укреплению общей экономической и социальной стабильности Российской Федерации.

Литература

1. Иванов С. П. Цифровое мошенничество: новые вызовы и пути противодействия. *Вестник кибербезопасности*. 2022, № 2, с. 45–58.

2. Петрова А. В. Преступления в сфере информационных технологий: классификация и тенденции. *Право и цифровая среда*. 2021, № 4, с. 118–130.

3. Сидоров И. М. Цифровая грамотность как основа личной безопасности в интернете. *Информационное общество: образование, наука, культура, экономика*. 2023, № 1, с. 88–99.

4. Козлов В. Н. Особенности цифровизации в регионах с низкой плотностью населения: опыт Республики Саха (Якутия). *Региональное развитие: новые измерения*. 2022, № 3, с. 210–225.

5. Смирнова Е. А. Правовое регулирование противодействия киберпреступности в Российской Федерации. *Российское право: актуальные проблемы*. 2021, № 2, с. 155–170.

6. Кузнецов О. В. Методы и тактика мошенничества в цифровой среде 2023 года. *Криминология: вчера, сегодня, завтра*. 2023, № 3, с. 70–85.

7. Морозов Д. А. Основные тренды телефонного и интернет-мошенничества. *Современные исследования в экономике и юриспруденции*. 2022, № 1, с. 130–145.

8. Национальный проект «Цифровая экономика Российской Федерации». Информационный портал Правительства РФ. URL: http://government.ru/projects/selection/832/ (дата обращения: 15.04.2026).

9. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) «О персональных данных». *Собрание законодательства РФ*, 2006, N 31, ст. 3451.

10. Guidelines on protecting consumers from online fraud. European Consumer Centres Network. 2024.

References

1. Ivanov S.P. Digital fraud: new challenges and counteraction methods. *Vestnik kiberbezopasnosti*. 2022; 2:45–58.

2. Petrova A.V. Crimes in the field of information technology: classification and trends. *Pravo i tsifrovaya sreda*. 2021; 4:118–130 (in Russian).

3. Sidorov I.M. Digital literacy as the basis for personal security on the internet. *Informatsionnoye obshchestvo: obrazovaniye, nauka, kultura, ekonomika*. 2023; 1:88–99 (in Russian).

4. Kozlov V.N. Specifics of digitalization in regions with low population density: the experience of the Republic of Sakha (Yakutia). *Regional'noye razvitiye: novyye izmereniya*. 2022; 3:210–225 (in Russian).

5. Smirnova E.A. Legal regulation of counteracting cybercrime in the Russian Federation. *Rossiyskoye pravo: aktual'nyye problemy*. 2021; 2:155–170 (in Russian).

6. Kuznetsov O.V. Methods and tactics of fraud in the digital environment of 2023. *Kriminologiya: vchera, segodnya, zavtra*. 2023; 3:70–85 (in Russian).

7. Morozov D.A. Main trends in telephone and internet fraud. *Sovremennyye issledovaniya v ekonomike i yurisprudentsii*. 2022; 1:130–145 (in Russian).

8. National project «Digital Economy of the Russian Federation». Information portal of the Government of the Russian Federation. Available at: http://government.ru/projects/selection/832/ (accessed: 15.04.2026). (in Russian).

9. Federal Law of 27.07.2006 N 152-FZ (as amended on 02.07.2021) «On Personal Data». *Sobranie zakonodatel'stva RF*, 2006, N 31, art. 3451 (in Russian).

10. Guidelines on protecting consumers from online fraud. European Consumer Centres Network. 2024.

Сведения об авторе

АНДРЕЕВ Дмитрий Васильевич – старший преподаватель, Горный институт, ФГАОУ ВО «Северо-Восточный федеральный университет им. М.К. Аммосова», г. Якутск, Российская Федерация, e-mail: vervil@list.ru

About the author

ANDREEV Dmitry Vasilievich – Senior Lecturer, Mining Institute, M. K. Ammosov North-Eastern Federal University, Yakutsk, Russian Federation

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Conflict of interests

The author declares that he has no conflict of interest

Поступила в редакцию / Received 15.03.2026
Поступила после рецензирования/ Revised 25.04.2026
Принята к публикации / Accepted 15.05.2026