Педагогические исследования. 2025. Вып. 1. С. 5–28.
Pedagogical Research. 2025. Vol. 1. P. 5–28.

Общая педагогика, история педагогики и образования
(педагогические науки)

Научная статья
УДК 37.02

# ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ ПЛАТФОРМЫ: РИСКИ И ПУТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНИКОВ

**Илья Артемович Жигульский[1]✉, Ольга Михайловна Коробкова[2]**

[1, 2]Астраханский государственный университет им. В. Н. Татищева, Астрахань, Россия

[1]ilya.zhigulskiy.2000@mail.ru✉

[2]olga-korobkova@mail.ru

***Аннотация.*** В статье рассматриваются связанные с цифровыми образовательными платформами риски, определяющиеся как потенциальные угрозы и негативные последствия, которые могут возникнуть в процессе обучения школьников, в том числе фишинг как вид кибермошенничества. Его целью является получение конфиденциальной информации (логинов, паролей, данных банковских карт) обманным путем, в частности при использовании цифровых образовательных платформ. Цель исследования состоит в анализе уровня осведомленности школьников о данном виде мошенничества. Фишинг остается одной из самых распространенных угроз в информационной безопасности, поскольку он опирается

не на технические уязвимости, а на человеческий фактор. В работе использовались методы опроса и математического анализа, которые применялись при изучении ответов 751 школьника из 9 школ Астрахани. В результате исследования были получены сведения, указывающие на низкий уровень осведомленности о фишинге, незнание обучающимися о защите своих личных данных с помощью двухфакторной аутентификации, что делает актуальной необходимость разработок педагогических средств, обучающих школьников информационной безопасности. В статье предлагается совокупность практико-ориентированных педагогических инструментов, направленных на повышение эффективности информационной безопасности школьников во время работы на образовательных цифровых платформах.

***Ключевые слова:*** практико-ориентированное образование; цифровые образовательные платформы; школьники; фишинг; информационная безопасность

***Для цитирования:*** Жигульский И. А., Коробкова О. М. Цифровые образовательные платформы: риски и пути обеспечения информационной безопасности школьников // Педагогические исследования. 2025. Вып. 1. С. 5–28.

General Pedagogics, History of Pedagogics and Education
(pedagogical sciences)

Original article

# DIGITAL EDUCATIONAL PLATFORMS: RISKS AND WAYS TO ENSURE INFORMATION SECURITY FOR SCHOOLCHILDREN

**Ilya A. Zhigulsky[1]✉, Olga M. Korobkova[2]**

[1, 2]Astrakhan Tatishchev State University, Astrakhan, Russia

Педагогические исследования. 2025. Вып. 1. С. 5–28.
Pedagogical Research. 2025. Vol. 1. P. 5–28.
[1]ilya.zhigulskiy.2000@mail.ru✉

[2]olga-korobkova@mail.ru

***Abstract.*** The article examines the risks associated with digital educational platforms, which are defined as potential threats and negative consequences that may arise in the learning process of schoolchildren, including phishing as a type of cyber fraud aimed at obtaining confidential information (logins, passwords, bank card data) fraudulently using educational digital platforms. The aim of the study is to analyze the awareness of schoolchildren about online fraud – phishing on educational digital platforms. Phishing remains one of the most common threats to information security, as it relies not on technical vulnerabilities, but on the human factor. The study employed survey methods and mathematical analysis, which were applied to the responses of 751 schoolchildren from 9 schools in Astrakhan. As a result of the research, some data was obtained indicating a low level of awareness about phishing, as well as a lack of knowledge among students about protecting their personal data through two-factor authentication, which confirms the urgent need for the development of pedagogical tools to educate schoolchildren about information security. The article proposes a set of practice-oriented pedagogical tools aimed at enhancing the effectiveness of schoolchildren's information security while using educational digital platforms.

***Keywords:*** practice-oriented education; digital educational platforms; schoolchildren; phishing; information security

***For citation:*** Zhigulskiy I. A., Korobkova O. M. Digital educational platforms: risks and ways to ensure information security for schoolchildren. *Pedagogicheskie issledovaniya = Pedagogical Research.* 2025;(1):5-28. (In Russ.).

**Введение**

Школы постепенно начинают все активнее интегрировать в учебный процесс цифровые образовательные платформы для более эффективного усвоения материалов обучающимися [1]. В условиях глобальной цифровизации они все чаще используют такие платформы не только для получения новых знаний, но и для взаимодействия с учителями и одноклассниками [2]. Это значительно расширяет возможности образовательного процесса, однако вместе с тем приводит к росту числа киберугроз и информационных рисков. Школьники, не обладая достаточным опытом и прочными навыками кибербезопасности, становятся уязвимой категорией пользователей, легкой добычей для фишинга, кибербуллинга и других кибератак [3].

Ситуация осложняется тем, что цифровые образовательные платформы часто не имеют достаточного уровня защиты данных, а сами учащиеся и их родители не всегда осведомлены о потенциальных рисках [4]. В результате увеличивается вероятность несанкционированного доступа к личным данным школьников, их учебным достижениям и даже финансовой информации, связанной с оплатой образовательных услуг.

Кроме того, утечка персональных данных в условиях активного использования цифровых технологий может привести и к психологическим угрозам, что негативно сказывается на психоэмоциональном состоянии и успеваемости обучающихся [5].

Безусловно, использование образовательных платформ имеет ряд преимуществ (доступность знаний, индивидуализация обучения, интерактивность), но в то же время оно создает новые способы заработка для мошенников. Так, с января по декабрь 2024 года в нашей стране всего зарегистрировано 765,4 тысяч киберпреступлений, что на 13,1 % больше, чем за аналогичный период 2023 года (URL: https://tass.ru/proisshestviya/22978955). Невнимательность пользователей

становится ключевым фактором потери средств и данных в Интернете, причем это касается людей всех возрастов.

**Цель исследования** – анализ уровня осведомленности школьников о таком виде интернет-мошенничества, как фишинг, с последующей разработкой материалов для занятий со школьниками.

**Материалы и методы исследования**

Информационная безопасность, которая представляет собой комплекс мер, направленных на защиту информации от различных угроз (несанкционированный доступ, разрушение, изменение или утечка данных) и сохранение ее конфиденциальности, целостности и доступности, обеспечивает надежность информационных систем, сетей и данных с учетом всех рисков и угроз.

Информационная безопасность включает конфиденциальность (защита данных от несанкционированного доступа, т. е. обеспечение того, чтобы только авторизованные лица имели возможность работать с конфиденциальной информацией), целостность (гарантия того, что информация не была изменена, повреждена или уничтожена без разрешения), доступность (обеспечение того, чтобы информация и системы были доступны пользователям, когда они им необходимы, и чтобы отказ от обслуживания (например, в результате атаки) был минимизирован), аутентификацию и авторизацию (механизмы, которые обеспечивают проверку подлинности пользователей и дают доступ к информации только тем, кто имеет на это соответствующие права), защиту от угроз (меры по предотвращению различных типов атак и злоупотреблений, таких как вирусы, фишинг, DDoS-атаки, кибербуллинг, социальная инженерия и др.), мониторинг и реагирование на инциденты (постоянное отслеживание состояния информационной безопасности, а также оперативное реагирование на инциденты, связанные с нарушением безопасности) [6].

Риски оцениваются на основе вероятности их возникновения и потенциальных последствий, которые могут существенно повлиять на функционирование системы, организации или индивида. Важно отметить, что риски могут быть как внешними (например, кибератаки), так и внутренними (например, ошибки пользователей или уязвимости системы).

На цифровых образовательных платформах риски могут включать утечку данных, угрозы кибербуллинга, доступ к вредоносным программам и другие ситуации, которые угрожают безопасности и защите данных обучающихся [7].

Одним из наиболее распространенных рисков является кибербуллинг, когда школьники становятся жертвами онлайн-агрессии и угроз со стороны других пользователей. Это может негативно сказаться на их самооценке и развитии. Существует опасность несанкционированного доступа к личным данным, таким как пароли, адреса и другие конфиденциальные сведения. Злоумышленники могут использовать информацию в корыстных целях, что делает школьников уязвимыми.

Фишинг представляет собой еще одну угрозу для школьников, особенно когда через образовательные платформы распространяются фальшивые сообщения, нацеленные на сбор личных данных. Школьники, не имеющие достаточного опыта в области информационной безопасности, могут стать жертвами этих схем.

Фишинг – метод мошенничества, при котором злоумышленники используют различные способы обмана с целью получения конфиденциальной информации пользователей, такой как логины, пароли, номера кредитных карт, банковские реквизиты и др. [8]. В отличие от более традиционных методов кражи фишинг часто реализуется через различные каналы связи: электронную почту, сообщения в мессенджерах, сайты, социальные сети или даже телефонные звонки.

Основной механизм фишинга заключается в том, что преступники создают ложные, но внешне правдоподобные страницы, письма или сообщения, которые выглядят как официальные коммуникации от надежных организаций (например,

банков, онлайн-магазинов, социальных сетей). Цель – заставить жертву предоставить личные данные, думая, что она общается с надежным источником.

Одним из наиболее серьезных рисков является возможность утечек персональных данных школьников, приводящая к нарушению конфиденциальности и становящаяся причиной их дальнейшей эксплуатации. Для этой угрозы характерно отсутствие должной защиты со стороны образовательных платформ, а также вредоносные программы, такие как вирусы и шпионские приложения, которые могут проникать через незащищенные ресурсы.

Использование открытых Wi-Fi-сетей без должной защиты также увеличивает вероятность перехвата данных, делает школьников уязвимыми при атаках. Однако не все образовательные платформы имеют достаточные настройки безопасности, открывая дополнительные возможности для злоумышленников.

Одним из наиболее значимых рисков является угроза утечки личных данных. Проблема усугубляется тем, что школьники, как правило, не обладают достаточными знаниями в области информационной безопасности и не осознают все возможные риски, связанные с их активностью в сети.

При этом вектор развития современного образования направлен на цифровизацию, являющуюся ключевым вопросом государственной политики, что подтверждается рядом официальных документов, демонстрирующих необходимость использования цифровых образовательных платформ в школах для модернизации учебного процесса и повышения качества образования.

Федеральный закон «Об образовании в Российской Федерации» № 273-ФЗ (http://www.consultant.ru/document/cons_doc_LAW_140174/) предусматривает использование инновационных технологий, обеспечивающее доступность и эффективность образовательного процесса, создание современной образовательной среды.

Стратегия развития образования в Российской Федерации до 2030 года, утвержденная Правительством Российской Федерации, акцентирует внимание на внедрении информационно-коммуникационных технологий как основе для повышения конкурентоспособности образовательной системы и развития цифровой грамотности учащихся.

Кроме того, Программа «Цифровая школа» (https://school.mos.ru/ru/digital-school), реализуемая Минобрнауки России, направлена на создание условий для интеграции цифровых образовательных платформ в школьное пространство, что обеспечивает доступ к образовательным ресурсам вне зависимости от географического положения и способствует формированию навыков, важных для жизни в информационном обществе.

Перечисленные документы доказывают стратегическую важность цифровых образовательных платформ, обосновывая необходимость их использования для адаптации образовательной системы к современным вызовам и требованиям времени.

Сейчас существует большое количество образовательных онлайн-платформ, рассмотрим некоторые из них.

«Дневник.ру» считается одним из самых популярных электронных журналов. Сервис предоставляет круглосуточный доступ к оценкам, расписанию и домашним заданиям, он имеет полезные и удобные приложения, автоматизацию зачисления в образовательные организации [9]. Федеральный проект «Цифровая школа» с 2018 года объединяет все школы нашей страны, используя данную платформу, эти действия способствовали повышению доступности образования, особенно в период пандемии [10].

«Яндекс Практикум» предоставляет бесплатные курсы в сфере IT для школьников и студентов. На платформе есть курсы по программированию, аналитике, дизайну, маркетингу, менеджменту и др. Занятия проводятся в

технологической среде «Яндекса», где ученики тут же используют знания: разбирают задачи, отвечают на вопросы тестов и создают проекты [11].

«Вконтакте» с недавних пор стал гигантом в сфере интернет-индустрии. Российские разработчики ежедневно проводят работу над улучшением экосистемы, которая включает социальную сеть для общения преподавателей и учеников «Сферум». Платформа предлагает полезные функции для учителей: онлайн-собрания, возможность хранения записей лекций и составления расписания [12].

Несмотря на очевидные преимущества данных платформ, все они подвержены различным киберугрозам, самая распространенной из них является фишинг – вид мошенничества в Интернете, целью которого является кража конфиденциальных данных пользователей. За 2024 год было обнаружено и заблокировано около 30 тысяч фишинговых ресурсов, что в семь раз больше, чем в 2023 году [13]. Злоумышленники, используя «слитые» из баз данных популярных сервисов почтовые адреса, делают массовую рассылку, в которых содержатся вредоносные ссылки. Чаще всего они почти не отличаются от настоящих доменов: как правило, заменяют графический знак (например, «о» на «0») или домен первого уровня (например, .com на .ru).

Данные ссылки ведут на полные копии известных сайтов. После заполнения форм на поддельных сервисах злоумышленники получают логины и пароли, номера карт, CVC, персональные данные [14].

Для анализа уровня осведомленности школьников использовался метод опроса (табл. 1).

**Таблица 1 – Анкета «Осведомленность учащихся об образовательных рисках в Интернете»**

| Вопросы | Ответы |
|---|---|
| Слышали ли вы когда-нибудь о таком способе интернет-мошенничества как фишинг? | Да, знаю, что это такое / Слышал(а), но не уверен(а), что это / Нет, никогда не слышал(а) |

| | |
|---|---|
| Как вы думаете, что такое фишинг? | Вирус, который заражает компьютер / Мошенничество, когда обманом выманивают личные данные / Взлом аккаунтов с помощью программ / Не знаю |
| Получали ли вы когда-либо подозрительные сообщения в социальных сетях, по почте или в мессенджерах (например, просьбы перейти по ссылке, ввести пароль или личные данные)? | Да, часто / Да, иногда / Нет, никогда / Не уверен(а) |
| Если вам приходит сообщение с просьбой перейти по ссылке и ввести пароль, что вы делаете? | Перехожу по ссылке и ввожу данные, если сообщение выглядит убедительно / Проверяю отправителя и ссылку перед тем, как что-то делать / Никогда не открываю такие ссылки и сразу удаляю сообщение / Зависит от ситуации |
| Используете ли вы один и тот же пароль для разных сайтов и приложений? | Да, у меня один пароль для всех аккаунтов / У меня несколько паролей, но некоторые повторяются / Нет, у меня уникальные пароли для каждого аккаунта |
| Как часто вы меняете пароли от своих аккаунтов? | Никогда не меняю / Раз в год или реже / Несколько раз в год / Каждый месяц или чаще |
| Знаете ли вы, что такое двухфакторная аутентификация (2FA)? | Да, знаю и использую / Знаю, но не использую / Никогда не слышал(а) об этом |
| Узнавали ли вы о фишинге на занятиях в ваших учебных заведениях? | Да, подробно разбирали / Упоминали, но поверхностно / Нет, никогда не обсуждали |
| Считаете ли вы, что ваша личная информация в Интернете надежно защищена? | Да, я уверен(а) в своей защите / Думаю, что да, но не уверен(а) / Нет, я понимаю, что мои данные могут быть украдены / Не задумывался(ась) об этом |
| Хотели бы вы узнать больше о том, как защитить себя от фишинга и других видов интернет-мошенничества? | Да, это важно для меня / Возможно, если информация будет интересной / Нет, мне это не нужно |

**Результаты исследования и их обсуждение**

Опрос проводился с использованием платформы Google Forms. В эксперименте участвовал 741 школьник из следующих образовательных организаций Астрахани: МБОУ СОШ № 29, МБОУ СОШ № 8, МБОУ СОШ № 20, МБОУ СОШ № 36, МБОУ СОШ № 1, МБОУ СОШ № 22, МБОУ СОШ № 26, МБОУ СОШ № 32, МБОУ СОШ № 37.

Рассмотрим полученные данные (рис. 1–3, табл. 2).

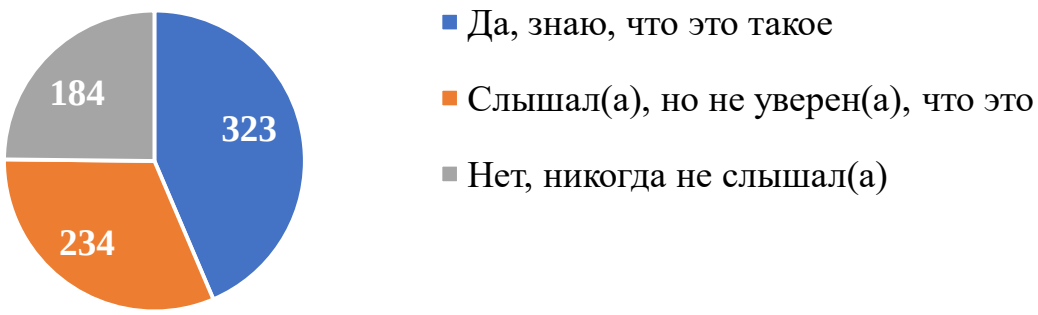


**Рисунок 1 – Осведомленность о фишинге среди школьников**

Большинство респондентов знакомы с понятием фишинга. Ответ «Да, знаю, что это такое» выбрали 323 человека, т. е. 44 %, это свидетельствует о высокой осведомленности школьников по вопросу фишинга.

В то же время 234 человека (31 %) ответили: «Слышали о фишинге, но не уверены в том, что за этим скрывается». Данный факт указывает на наличие некоторого уровня осведомленности, однако есть неопределенность в понимании сути угрозы. Таким образом, существует необходимость более детального разъяснения рисков фишинга в рамках образовательных или информационных программ.

Относительно небольшое количество респондентов (25 %) никогда не слышали о фишинге, что подчеркивает наличие группы людей, которые либо не сталкивались с таким видом интернет-мошенничества, либо не обладают достаточной информацией для осознания цифровой угрозы.

Таким образом, большинство респондентов осведомлены о фишинге, однако существует значительная доля школьников, нуждающихся в дополнительном

обучении и повышении цифровой грамотности для лучшего понимания механизмов защиты от такого рода угроз.

Вопрос о выявлении уровня осведомленности о фишинге подтверждает эту тенденцию (рис. 2).

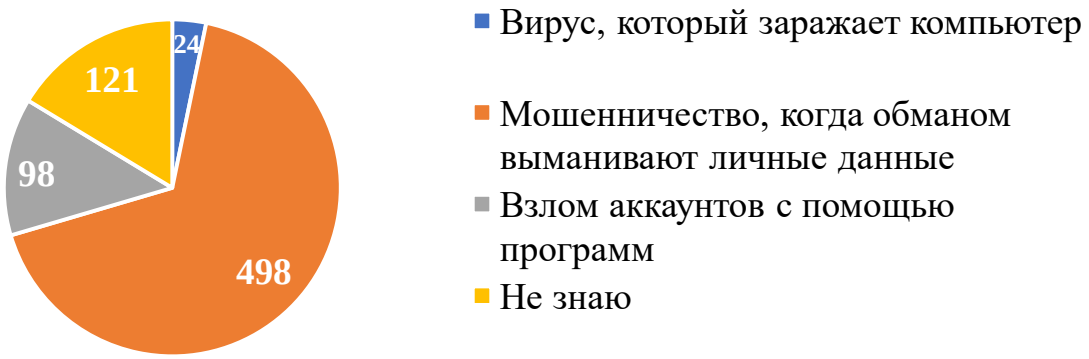


**Рисунок 2 – Понятие сущности феномена «фишинг»**

Повторим, что фишинг как форма интернет-мошенничества представляет собой угрозу, нацеленную на получение конфиденциальных данных пользователей через обман. Однако восприятие этого явления среди пользователей в значительной степени варьируется. Результаты опроса, направленного на выяснение того, как респонденты понимают фишинг, демонстрируют интересные тенденции.

Согласно полученным данным, значительное число респондентов (67 %) правильно определили фишинг как «Мошенничество, когда обманом выманивают личные данные». Таким образом, большинство участников осведомлены о сущности угрозы фишинга, его целях и механизмах действия. Примерно 60 % опрошенных имеют правильное понимание данной угрозы, что свидетельствует о достаточно высоком уровне осведомленности среди исследуемой аудитории.

Тем не менее, результаты опроса выявили: значительная часть респондентов имеют искаженное представление о фишинге. 17 % респондентов ошибочно

считают фишинг вирусом, который заражает компьютер. Это заблуждение может быть связано с ассоциацией фишинга с вирусами и другим вредоносным программным обеспечением, что является распространенной ошибкой среди пользователей. Фишинг, в отличие от вирусов, не заражает компьютер напрямую, а использует социальную инженерию для получения личных данных.

Кроме того, 13 % респондентов ошибочно считают фишинг «Взломом аккаунтов с помощью программ», т. к. он основан на обмане, а не на техническом взломе. Следовательно, есть необходимость уточнения различий между различными типами угроз в киберпространстве.

Небольшое количество респондентов (3 %) сообщили о своем незнании такого феномена, как фишинг. Данное обстоятельство подчеркивает важность образовательных инициатив, направленных на обучение базовым аспектам информационной безопасности.

Результаты опроса указывают на необходимость формирования у школьников дополнительного информирования и обучения их точному понимания информационных угроз, в том числе фишинга, его методов и последствий. Расширение знаний о цифровых угрозах поможет повысить уровень защиты пользователей от подобных мошеннических схем.

Отметим, что многие сталкивались с подозрительными сообщениями, при этом некоторые пользователи их даже не проверяют (рис. 3).

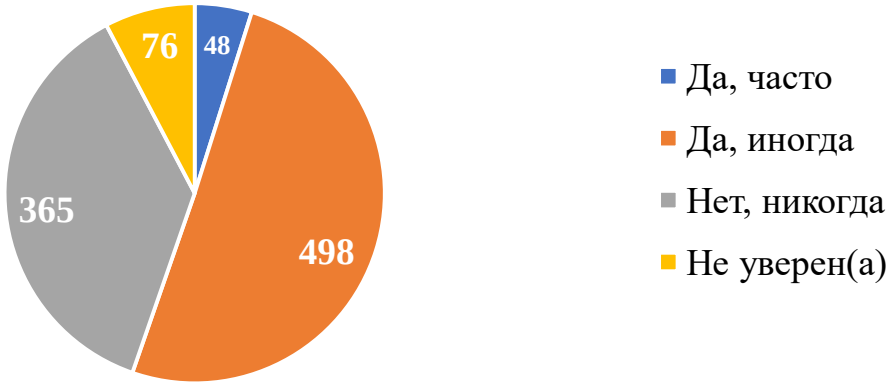


**Рисунок 3 – Частота получения подозрительных сообщений в социальных сетях и мессенджерах**

Большая часть учащихся используют повторяющиеся пароли и редко их меняют. Почти половина школьников не знают о защите с помощью двухфакторной аутентификации, т. к. тему фишинга не освещалась на занятиях (табл. 2).

**Таблица 2 – Результаты диагностики «Использование средств информационной защиты»**

| **Вопрос/переменные** | Перехожу по ссылке и ввожу данные, если сообщение выглядит убедительно | Проверяю отправителя и ссылку перед тем, как что-то делать | Никогда не открываю такие ссылки и сразу удаляю сообщение | Зависит от ситуации |
|---|---|---|---|---|
| Если вам приходит сообщение с просьбой перейти по ссылке и ввести пароль, что вы делаете? | 9 | 137 | 482 | 113 |
| **Вопрос/переменные** | Да, у меня один пароль для всех аккаунтов | У меня несколько паролей, но | Нет, у меня уникальные пароли для | - |

| | | | | |
|---|---|---|---|---|
| | | некоторые повторяются | каждого аккаунта | |
| Используете ли вы один и тот же пароль для разных сайтов и приложений? | 96 | 383 | 262 | - |
| **Вопрос/переменные** | Никогда не меняю | Раз в год или реже | Несколько раз в год | Каждый месяц или чаще |
| Как часто вы меняете пароли от своих аккаунтов? | 194 | 270 | 191 | 86 |
| **Вопрос/переменные** | Да, знаю и использую | Знаю, но не использую | Никогда не слышал(а) об этом | - |
| Знаете ли вы, что такое двухфакторная аутентификация (2FA)? | 365 | 135 | 241 | - |
| **Вопрос/переменные** | Да, подробно разбирали | Упоминали, но поверхностно | Нет, никогда не обсуждали | - |
| Узнавали ли вы о фишинге на занятиях в ваших учебных заведениях? | 157 | 248 | 336 | - |
| **Вопрос/переменные** | Да, я уверен(а) в своей защите | Думаю, что да, но не уверен(а) | Нет, я понимаю, что мои данные могут быть украдены | Не задумывался (ась) об этом |
| Считаете ли вы, что ваша личная информация в Интернете надежно защищена? | 255 | 276 | 145 | 65 |

Результаты опроса демонстрируют различные модели поведения пользователей в отношении их безопасности в Интернете, уровня осведомленности о цифровых угрозах.

Первое, что стоит отметить, это поведение пользователей в ответ на подозрительные сообщения, содержащие просьбы перейти по ссылке или ввести пароль. Большинство респондентов (64 %) действуют осторожно, сразу удаляя

такие сообщения, демонстрируя правильное и безопасное поведение. Лишь 1 % респондентов переходит по ссылке, если сообщение выглядит убедительно. Этот факт подчеркивает риски фишинга, когда даже достаточно осведомленные пользователи могут стать жертвами обмана.

Значительное число респондентов используют несколько паролей, но часто их повторяют на различных сайтах (52 %). Несмотря на это, 35 % респондентов используют уникальные пароли для каждого аккаунта, что значительно повышает уровень безопасности. Применение одного пароля для нескольких сайтов увеличивает риски в случае компрометации пароля на одном из сервисов.

Частота изменения паролей также варьируется среди респондентов. Больше всего людей (36 %) меняют пароли раз в год или реже, а значительное число (26 %) вообще не меняет их. Это может свидетельствовать о недостаточном осознании важности регулярного обновления паролей для защиты аккаунтов. Только небольшая группа (12 %) меняет пароли часто, что является оптимальной практикой для повышения уровня безопасности.

Важный аспект касается двухфакторной аутентификации (2FA). 48,6 % респондентов знают о ней и активно используют ее, 49 % школьников, хотя и осведомлены о существовании 2FA, не применяют этот метод защиты. Это указывает на необходимость повышения осведомленности о важности двухфакторной аутентификации и более активного ее внедрения в повседневную практику.

Когда речь заходит о фишинге, то результаты показывают, что в учебных заведениях тема практически не обсуждается. Только 21 % респондентов заявили, что фишинг был подробно рассмотрен, в то время как 45 % никогда не сталкивались с этой темой в образовательных программах. Существует явный пробел в образовательных курсах по информационной безопасности, необходима более

глубокая проработка проблемы и внедрение соответствующих тем в учебные планы.

Многие респонденты уверены в защите личной информации в Интернете: 30 % опрошенных заявили об уверенности в безопасности своих данных. Однако существует группа школьников (20 %), которые осознают риски утечек данных. Небольшая доля респондентов (9 %) вообще не задумываются о защите своих данных, что является серьезной проблемой для формирования культуры безопасности в Интернете.

В целом, результаты опроса демонстрируют осведомленность школьников о рисках и угрозах в Интернете, но часто они не готовы принимать меры для защиты своих данных. В связи с этим необходимо дальнейшее обучение пользователей, внедрение более строгих практик безопасности и активное использование современных методов защиты, таких как двухфакторная аутентификация и регулярная смена паролей.

Респонденты проявляют интерес к новым знаниям в области информационной безопасности, чтобы в будущем быть уверенными в защите своей информации (рис. 4).

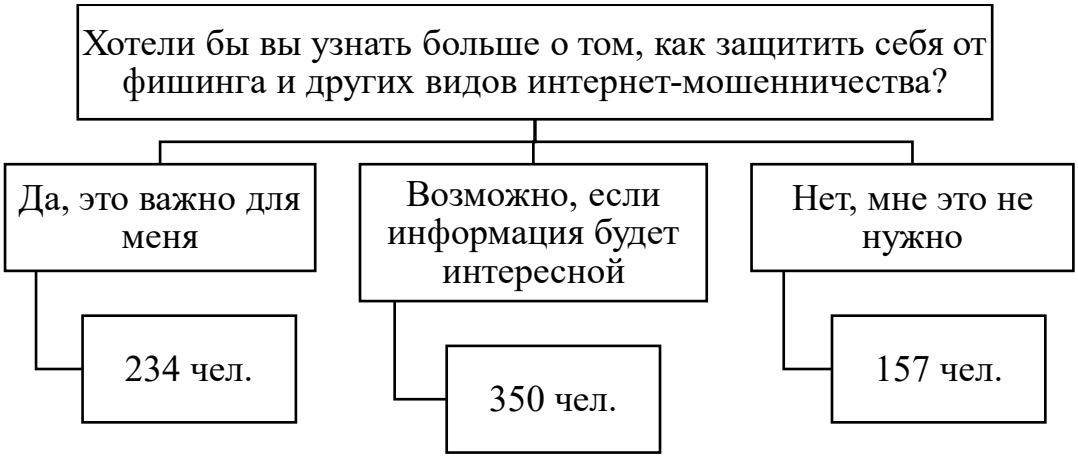


**Рисунок 4 – Диагностика потребности знаний по защите от интернет-мошенничества**

В условиях постоянного роста угроз в сфере интернет-безопасности важность повышения осведомленности пользователей о методах защиты от фишинга и других видов интернет-мошенничества не вызывает сомнений. Результаты проведенного опроса демонстрируют разный уровень заинтересованности в получении дополнительной информации на тему информационной безопасности среди респондентов.

Одним из ключевых выводов является то, что меньшинство участников (32 %) выразили желание узнать больше о способах защиты от интернет-мошенничества. Это свидетельствует о наличии определенного уровня осведомленности среди данной группы людей, а также их готовности углубить свои знания по вопросам цифровой безопасности.

21 % респондентов заявили об отсутствии потребности в дополнительной информации о защите от интернет-мошенничества. Это может свидетельствовать о низком уровне осведомленности о существующих угрозах, уверенности в собственных знаниях или о недостаточном интересе к данной теме.

Результаты опроса указывают на существование значительного потенциала для внедрения образовательных программ, направленных на повышение цифровой грамотности школьников, особенно если они будут предложены в доступной и увлекательной форме. Это подтверждает необходимость создания эффективных стратегий повышения осведомленности о рисках интернет-мошенничества, что способствует улучшению общей безопасности школьников.

Чтобы повысить уровень подготовки к возможному фишингу, стоит интегрировать в образовательный процесс практико-ориентированные методы обучения кибербезопасности.

Так, в ходе занятий необходимо моделировать реальные фишинговые атаки. Умение отличать поддельное письмо от подлинного поможет на практике закрепить навыки проверки ссылок и отправителей.

Игра «Фишинг-детектив» способствует развитию внимания к деталям при работе с платформами, используемыми школьниками. В ходе занятия ученики внимательно изучают интерфейс, а именно: оформление страниц, логотипы, доменное имя и другие характерные признаки. Данная игра не только учит проверять подлинность сайтов, но и развивает критическое мышление и внимательность.

Соревнования по созданию надежных паролей. Ученики придумывают комбинацию символов, а потом проверяют на специальных сайтах. Выигрывают те, чьи пароли дольше взламываются. Подобные соревнования помогут учащимся осознать важность использования уникальных и сложных комбинаций для безопасности их аккаунтов.

**Заключение**

Исследование показало, что большинство школьников не знают о фишинговых атаках и способах защиты от них. Тенденции, выявленные в ходе опроса, подчеркивают важность пересмотра подходов к обучению кибербезопасности в школах. Цифровизация ускоряется, мошенники пользуются этим и придумают новые способы обмана, поэтому включение тем, связанных с фишингом, в программы по финансовой грамотности и информатике должно стать обязательным.

Проведенное исследование показало, что вопросы интернет-безопасности, особенно связанные с фишингом и другими видами интернет-мошенничества, остаются актуальными для школьников. Несмотря на высокий уровень осведомленности о существующих угрозах, значительная часть респондентов выражает заинтересованность в дальнейшей защите своих данных, подтверждая важность усиленной образовательной работы в этой области.

Результаты опроса выявили следующее: большая часть участников не имеют активной потребности в углубленных знаниях о методах защиты, но есть и те, кто

готов повысить свою информированность при условии доступности и интересности материалов. Это подчеркивает необходимость разработать более эффективные и привлекательные образовательные программы, направленные на повышение цифровой грамотности.

Для эффективной борьбы с интернет-мошенничеством важно не только информировать пользователей о существующих угрозах, но и развивать навыки безопасного поведения в Сети. Важно внедрять различные формы обучения, учитывая разнообразие целевой аудитории и ее интересы. Это обеспечит повышение уровня безопасности в Сети и укрепит цифровую безопасность в целом.

Исследование подтверждает необходимость дальнейших усилий в области образования по вопросам цифровой безопасности с целью обеспечения защиты школьников от интернет-мошенничества и создания безопасной цифровой среды для всех участников.

## Список источников

1. Яламов Г. Ю. О современном состоянии обучения кибербезопасности // Вестник МГПУ. Серия: Информатика и информатизация образования. 2020. № 3 (53). С. 52–60. DOI 10.25688/2072-9014.2020.53.3.06.

2. Датаев А. А., Калитин Н. С., Харченко С. Б. Угрозы и вызовы кибербезопасности в онлайн-образовании // Проблемы современного педагогического образования. 2024. № 83-3. С. 144–147.

3. Магомадова А. Р., Айгумов Т. Г., Синицин А. М. Развитие кибербезопасности в образовательной среде: защита данных и личной информации // Проблемы современного педагогического образования. 2024. № 83-3. С. 273–276.

4. Кокорев Н. М. Безопасность в условиях цифровых коммуникаций учащихся // Актуальные проблемы безопасности в техносфере. 2023. № 3 (11). С. 6–9. DOI 10.34987/2712-9233.2023.99.67.001.

5. Эпова А. В. Кибербуллинг и его воздействие на психическое состояние // Интеллектуальные ресурсы - региональному развитию. 2024. № 1. С. 415–420.

6. Сыкеев Д. В., Сыкеева И. Н. Проблемы обеспечения информационной безопасности // Актуальные проблемы гуманитарных и социально-экономических наук. 2023. № 4 (100). С. 45–48.

7. Польченко М. А. Анализ рисков в информационной среде // Молодой исследователь Дона. 2023. Т. 8. № 3 (42). С. 55–62.

8. Войкова Н. А. Мошенничество в Сети: получение конфиденциальной информации посредством фишинга // Вестник Российско-Армянского (Славянского) университета: гуманитарные и общественные науки. 2022. № 4 (43). С. 46–54. DOI 10.48200/1829-0450_sh_2022_4_46.

9. Бронникова Н. А. Ресурсы цифровой платформы «Дневник. ру»: пути повышения эффективности управления образованием // Преемственность в образовании. 2021. № 28. С. 503–510.

10. Новоселова К. В. Проект «Цифровая школа» // Информационно-коммуникационные технологии в педагогическом образовании. 2009. № 2. С. 1–5.

11. Пащенко Т. В. Формирование критического мышления у взрослых с использованием проблемно ориентированного обучения в онлайн-среде // Вопросы образования. 2024. № 2. С. 226–250.

12. Иванько А. Ф., Иванько М. А., Маркова Н. В. Образование и социальные сети // Новая наука: Проблемы и перспективы. 2016. № 121-3. С. 170–175.

13. Антонова Т. С., Смирнов В. М. Фишинг как неизученное киберпреступление // StudNet. 2021. Т. 4. № 6. С. 69–75.

14. Апухтин И. Н. Дезинформация в социальных сетях: преступления и наказания // Научные труды Северо-Западного института управления РАНХиГС. 2023. Т. 14. № 1 (58). С. 21–24.

## References

1. Yalamov G. Y. On the current state of cybersecurity education. *Bulletin of the Moscow State Pedagogical University. Series: Informatics and informatization of education.* 2020;(3(53):52-60. DOI 10.25688/2072-9014.2020.53.3.06. (In Russ.).

2. Dataev A. A., Kalitin N. S., Kharchenko S. B. Threats and challenges of cybersecurity in online education. *Problems of modern teacher education.* 2024;(83-3):144-147. (In Russ.).

3. Magomadova A. R., Aigumov T. G., Sinitsin A.M. The development of cybersecurity in the educational environment: data protection and personal information. *Problems of modern pedagogical education*. 2024;(83-3):273-276. (In Russ.).

4. Kokorev N. M. Safety in conditions of digital communications of students. *Actual problems of safety in the technosphere*. 2023;(3(11)):6-9. DOI 10.34987/2712-9233.2023.99.67.001. (In Russ.).

5. Epova A. V. Cyberbullying and its impact on the mental state. *Intellectual resources for regional development*. 2024;(1):415-420. (In Russ.).

6. Sikeev D. V., Sikeeva I. N. Issues of Ensuring Information Security. *Current Issues in Humanities and Social Economic Sciences*. 2023;(4(100)):45-48. (In Russ.).

7. Polchenko M. A. Risk analysis in the information environment. *Young Researcher of the Don*. 2023;(8(3(42)):55-62. (In Russ.).

8. Voikova N. A. Online fraud: obtaining confidential information through phishing. *Bulletin of the Russian-Armenian (Slavic) University: Humanities and Social Sciences.* 2022;(4(43)):46-54. DOI 10.48200/1829-0450_sh_2022_4_46. (In Russ.).

9. Bronnikova N. A. Resources of the digital platform «Diary.ru»: ways to improve the effectiveness of education management. *Continuity in education.* 2021;(28):503-510. (In Russ.).

10. Novoselova K. V. The Digital School project. *Information and communication technologies in teacher education*. 2009;(2):1-5. (In Russ.).

11. Paschenko T. V. Formation of critical thinking in adults using problem-oriented learning in an online environment. *Educational issues*. 2024;(2):226-250. (In Russ.).

12. Ivanko A. F., Ivanko M. A., Markova N. V. Education and social networks. *New science: Problems and prospects*. 2016;(121-3):170-175. (In Russ.).

13. Antonova T. S., Smirnov V. M. Phishing as an unexplored cybercrime. *StudNet*. 2021;(4(6)):69-75. (In Russ.).

14. Apukhtin I. N. Disinformation in social networks: crimes and punishments. Scientific papers of the Northwestern Institute management of the RANEPA. 2023;(14(1(58))):21-24. (In Russ.).

## Информация об авторах

**И. А. Жигульский** – студент;

**О. М. Коробкова** – кандидат психологических наук, доцент; доцент кафедры педагогических практик и сервисных индустрий.

## Information about the authors

**Ilya A. Zhigulsky** – student.

**Olga M. Korobkova** – PhD in Psychology, Associate Professor; Associate Professor of the Department of Pedagogical Practices and Service Industries.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.

Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 9.01.2025; одобрена после рецензирования 17.01.2025; принята к публикации 04.03.2025.

The article was published 9.01.2025; approved after reviewing 17.01.2025; accepted for publication 04.03.2025.