DOI 10.37882/2223–2982.2025.12.12

# НАВЫК ДИФФЕРЕНЦИРОВАНИЯ ДОСТОВЕРНОСТИ ИНТЕРНЕТ-РЕСУРСОВ И ИХ АВТОРИТЕТНОСТИ КАК ОСНОВА ФОРМИРОВАНИЯ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ У ОБУЧАЮЩИХСЯ

## THE SKILL OF DIFFERENTIATING THE RELIABILITY OF INTERNET RESOURCES AND THEIR CREDIBILITY AS THE BASIS FOR THE FORMATION OF A CYBERSECURITY CULTURE AMONG STUDENTS

***N. Verezubova***
***I. Kutlikova***
***O. Kishkinova***

*Summary:* Modern experts in fact-checking and reliability of information resources are not able to completely exclude fake content from the worldwide flow of information that enters the Internet in large volume. This factor determines the need to learn the skills of differentiating reliable and authoritative sources from unreliable ones, which increases the level of cognitive abilities and promotes productive mental activity. Students' information competence should include the ability to find relevant and relevant material, the ability to avoid infecting a personal computer or mobile device, as well as the ability to independently search, analyze, structure, select and process the received material. The ability to distinguish reliable information not only improves the quality of educational activities, but also acts as the foundation of a cybersecurity culture. Mastering the latter will be an important step towards the competent fulfillment of their professional duties in the future related to the processing of large amounts of information, compliance with data protection and confidentiality rules. A significant skill in performing a full–fledged verification of the relevance and relevance of publications is the use of the principles of verification and fact-checking - confirming the authenticity of data, identifying false or inaccurate information contained in text, audio, and video materials.

*Keywords:* information reliability, Internet content, reputable Internet resources, information competence, cybersecurity culture, information pollution, fact checking, disinformation.

***Верезубова Наталья Афанасьевна***
*Кандидат экономических наук, доцент, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*nverez@mail.ru*
***Кутликова Ирина Вениаминовна***
*Старший преподаватель, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*ivk-b@yandex.ru*
***Кишкинова Ольга Алексеевна***
*Старший преподаватель, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*olga.19672015@yandex.ru*

*Аннотация:* Современные специалисты по проверке фактов и достоверности информационных ресурсов не способны полностью исключить фейковый контент из всемирного потока информации, поступающего в большом объеме в интернет. Данный фактор детерминирует необходимость обучения навыкам дифференцирования надежных и авторитетных источников от недостоверных, что повышает уровень когнитивных способностей и содействует продуктивной мыслительной деятельности. Информационная компетентность обучающихся должна включать в себя умение находить актуальный и релевантный материал, навык избегать заражений персонального компьютера или мобильного устройства, а также способность выполнять самостоятельный поиск, анализ, структуризацию, выборку и обработку полученного материала. Навык отличать надежную информацию не только повышает качество образовательной деятельности, но и выступает в роли фундамента культуры кибербезопасности. Освоение последней станет важным шагом к грамотному выполнению своих профессиональных обязанностей в будущем, связанных с обработкой больших объемов информации, соблюдением правил по защите данных и конфиденциальности. Значительным умением выполнять полноценную проверку релевантности и актуальности публикаций является использование принципов верификации и фактчекинга – подтверждения подлинности данных, выявления ложных или неточных сведений, содержащихся в текстовых, аудио- и видеоматериалах.

*Ключевые слова:* достоверность информации, интернет-контент, авторитетные интернет-ресурсы, информационная компетентность, культура кибербезопасности, информационное загрязнение, фактчекинг, дезинформация.

## Введение

Технологии развиваются беспрецедентными темпами, зачастую опережая возможности отдельных лиц и организаций по поддержанию современных технологических компетенций. Это создает возможности для киберпреступников использовать возникающие уязвимости и пробелы в поведении [9, p. 8] для искажения информации, взлома данных, создания дипфейков, введения пользователей в заблуждение и их дезинфор-

мирования.

Из-за постоянно растущего количества киберинцидентов по всему миру в обществе все большее значение приобретает культура кибербезопасности. Как отмечают К. Ригард, К. Блэкетт, В. Катта (*Reegård, Blackett, Katta 2019*), данная культура достаточно объемлюща и включает в себя широкий спектр практик, моделей поведения и отношения к защите цифровых информационных активов. Проведение обязательного обучения по кибербезопасности для всех потенциальных сотрудников во всех секторах может гарантировать, что будущие специалисты будут хорошо осведомлены и ознакомлены с современными тенденциями в области защиты критически важной ИТ-инфраструктуры [9].

**Материалы и методы** основаны на системном подходе и включают анализ, синтез и структуризацию материала, аналитику и обработку данных, междисциплинарный подход.

## Результаты и обсуждение

С появлением цифровых платформ и экспоненциальным ростом объема информации в интернете, которые во многом обусловлены технологическим прогрессом, проверка фактов претерпевает значительные изменения [10, p. 2].

Навык дифференцирования достоверности и авторитетности интернет-ресурсов базируется на пяти важных концептах:

(а) **валидации** в контексте подтверждения информации, заключающейся в **сверке** материала с авторитетными и надежными источниками, эталонными значениями, в т.ч. с данными официальных государственных сайтов, наукометрических платформ и электронных библиотек, что помогает получать подтверждение достоверности и точности публикации.

(б) **анализе компетентности и квалификации** автора и созданного им информационного ресурса с помощью вышеуказанных в пункте «а» источников;

(в) **принятии во внимание деталей**, включая наличие автора, датированность публикации и ее последней редакции (при наличии), стиль написания и грамматику, длину URL (чем длиннее ссылка, тем меньше доверия она вызывает, в т.ч. из-за сложности восприятия и отрицательного влияния на кликабельность), присутствие / отсутствие экспрессии и тривиальности изложения и т.д.

(г) использовании инструментов **фактчекинга** (проверки информации на достоверность) как с помощью искусственного интеллекта (*ИИ*, англ. *Artificial Intelligence – AI*), так и без него. «Фактчекинг у обучающихся формирует представление о ложной информации и развивает навыки сбора, структурирования и критического анализа фактов» [1, с. 11];

(д) **верификации**, «предполагающей работу в трех форматах: фактчек, блогпост и медиа-анализ» [2, с. 75], которая также включает в себя защиту почтового электронного ящика, авторизированный доступ, грамотное управление «умным домом», навыки избегать и предупреждать ситуации мошенничества и фальсификации, в т.ч. дифференцирования фальшивых аккаунтов и поддельных данных от надежных и авторитетных информационных ресурсов.

*ИИ* и обработка естественного языка (англ. *Natural Language Processing – NLP*) произвели революцию в процессах проверки фактов, позволив анализировать огромные объемы текстовых данных в режиме реального времени. Все более сложные алгоритмы способны оказывать воздействие на закономерности в распространении дезинформации, обнаруживать вводящие в заблуждение утверждения и оптимизировать процесс фактчекинга, помогая специалистам по проверке интернет-контента справляться с огромным объемом данных, циркулирующих в интернете. При этом специалисты по проверке достоверности и авторитетности сайтов все больше обеспокоены использованием поддельного аудио- и видеоконтента для обмана аудитории, поэтому важнейшим компонентом их инструментария становится обнаружение дипфейков [10, p. 2]. Системы искусственного интеллекта находят методы обфускации, включая чрезмерный жаргон, сложные структуры предложений и стратегическое размещение информации, которые могут скрыть важные факты [11, p. 406].

Формируемый у обучающихся навык дифференцирования авторитетных и проверенных информационных источников от сомнительных влияет на несколько факторов:

(а) развивает навык валидации в контексте подтверждения информации, т.е. помогает оценивать достоверность и точность данных, находить актуальный и релевантный материал (учебный, научный и научно-популярный), который можно включать в научные публикации, образовательный процесс, использовать как источники, способные оказывать влияние на жизнедеятельность каждого отдельного человека и общественные настроения в целом (например, статьи о здоровьесбережении и долголетии, правильном питании, физической активности, политической и экономической обстановке, социальных реформах, государственных проектах и т п.).

Опираясь на официальные статистические площадки и государственные платформы, становится, например, очевидным, что такие новостные сайты, как *Forbes*, РИА

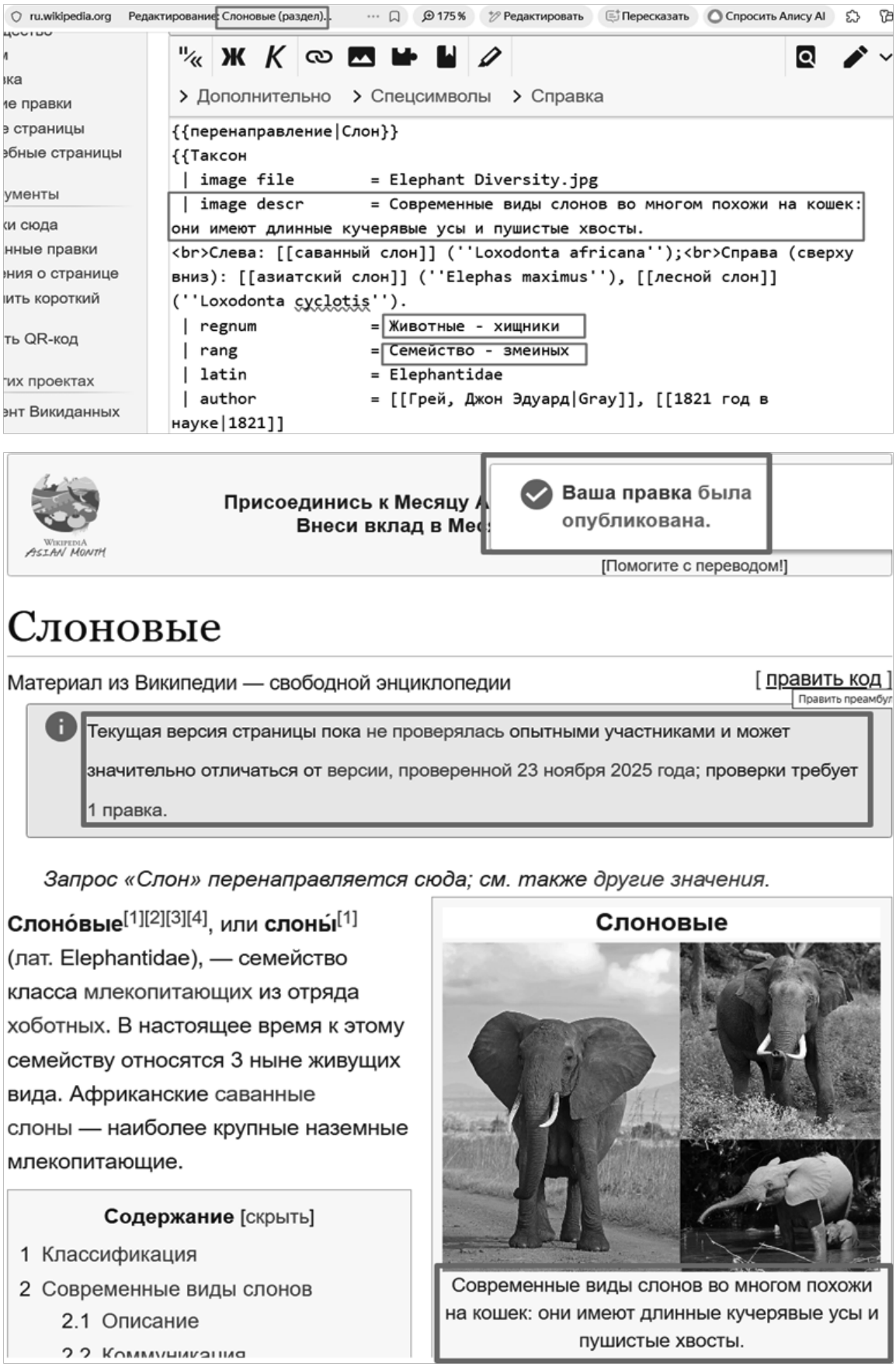


Рис. 1. Пример неавторитетного недостоверного интернет-ресурса – скриншот сайта Википедия (рисунок наш)


Рис. 2. Уровни культуры кибербезопасности, формируемой в обществе для устойчивости к цифровым угрозам (рисунок наш)

Новости, Коммерсантъ, Комсомольская правда и др. имеют высокий уровень надежности, тогда как *PostNews, Mash* / Мэш, Лентач, форумы пользователей Газета.Ru и РБК, *MDK* и др. занесены в список «ресурсов с недостоверной информацией» (см. Роскомнадзор 2021-2023 гг.) [5]. При этом обучающиеся должны понимать, что для научных исследований и самообразования подходят, например, *CyberLeninka.ru*, *ELibrary.ru*, *Researchgate.net*, электронная Российская государственная библиотека (РГБ – *rsl.ru*) и т.д., в то время как Википедия является сомнительным источником, т.к. авторами, редакторами и корректорами каждого материала с данного сайта могут быть абсолютно любые пользователи интернета, соответственно, модерация далеко не всегда справляется с проверкой опубликованного или измененного контента (см. рисунок 1).

Согласно рисунку 1, сайт Википедия может редактировать и дополнять любой пользователь. В примере указана достаточно безобидная дезинформация, которая, не оказывает негативного влияния на политические события, общественные настроения, принятие судьбоносных или важных решений, выбор варианта лечения или медикаментозных средств и т.д. До того, как страницу проверит опытный специалист, пройдет определенный промежуток времени, за который неопытные читатели могут взять оттуда информацию и ошибочно принять ее за достоверную – особенно данному риску подвержены подростки и обучающиеся начальных курсов, не владеющие навыками дифференцирования достоверных и авторитетных интернет-ресурсов от тех, которые написаны недобросовестными или некомпетентными авторами.

(б) учит избегать заражений персонального компьютера или мобильного устройства с помощью программ антивируса и исходя из собственного опыта. Стандарты безопасности для веб-сайтов, ориентированные на сохранение конфиденциальности данных, помогают устанавливать безопасное соединение, передавая данные между браузером пользователя и сервером по протоколу *HTTPS* (*HyperText Transfer Protocol Secure*), поддерживающим шифрование и защищающим информацию от перехватов. Существует три уровня критичности уязвимостей: высокий, средний и низкий.

(в) формирует навык самостоятельной работы в интернет-пространстве, который предотвращает бездумное чтение и «скачивание» любого готового контента, в т.ч. учебного материала или проектных работ, что «снижает сосредоточенную продуктивную мыслительную деятельность» [4, с. 52]. При этом вышеобозначенный навык помогает выполнять грамотный анализ ресурса, позволяющий определять достоверность и актуальность данных. Для этого необходимо ежегодно выполнять мониторинг списков сайтов с плюралистичным информационным пространством, формируемых Роскомнадзором, а также перечня рецензируемых научных изданий, реферативных баз данных и систем цитирования, утвержденных ВАК («Высшей аттестационной комиссией»), РИНЦ (Российским индексом научного цитирования), а также такими международными научными организациями, как *Scopus, Web of Science* и др.

Для усиления профилактических мер по предотвращению атак и угроз на информационную систему или ее компоненты, важно уметь отличать достоверный контент из авторитетных источников, от фейковых, что является фундаментом кибербезопасности. Соответственно, навыки дифференцирования надежных информационных ресурсов, обеспечиваемых надежными электронными изданиями и платформами, тесно коррелируют с развитой культурой кибербезопасности, которую условно можно разделить на три основных уровня, помогающих сформировать общество, устойчивое к цифровым угрозам (см. рисунок 2).

(а) обучение культуре кибербезопасности на уровне «**человеческого фактора**», рассматриваемого через призму психологии, что подразумевает под собой «готовность человека к преодолению цифровой экспансии за счёт овладения инструментарием противодействия негативным информационным факторам» [6, p. 207].

(б) достижение высокой культуры убеждений, норм, ценностей и методов, направленных на защиту информационных активов на уровне **общего образования**;

(в) создание политики и регламентов, а также инструментов и специализированных платформ по достижению высокого уровня кибербезопасности на **государственном уровне** (ярким примером являются Госуслуги, Мос.ру, система Антиплагиат и т.д.).

Согласно рисунку 2, для безопасной работы с цифровыми ресурсами необходимо принимать не только технические, но и организационные меры, поэтому большое внимание важно уделять культуре кибербезопасности. При этом, как подчеркивается в исследованиях К. Ригард, К. Блэкетт, В. Катта (*Reegård, Blackett, Katta 2019*), культура кибербезопасности понимается как подкомпонент организационной культуры и включает в себя такие важные компоненты, как: поддержка со стороны руководства; четко сформулированная политика организации, ориентированная на защиту данных и поддержание принципов конфиденциальности; осведомленность о потенциальных рисках и угрозах, а также соответствующее обучение; вовлеченность в корпоративную этику; извлечение уроков из опыта [8, с. 4036]. В культурной модели кибербезопасности [8] к уровням культуры кибербезопасности можно добавить четвертый фактор, который влияет на предубеждения, ценности и поведение [7, p. 3] – социальное окружение и его идеологические концепты.

## Выводы

Интеграция в образование лекций и семинаров по формированию информационной компетенции (включая навыки дифференцирования достоверности интернет-ресурсов и их авторитетности, в т.ч. работе в сфере кибербезопасности), обеспечивает ценную основу для корпоративной культуры, охватывающей кибербезопасность. В будущей профессиональной деятельности при выпуске из вузов обучающиеся смогут проводить мероприятия, ориентированные на распространение соответствующей информации по защите данных, и придерживаться принципов конфиденциальности, позволяющих принимать и поддерживать безопасные модели поведения в цифровой среде.

ЛИТЕРАТУРА

1. Гусев А.В. Методика обучения технологиям фактчекинга в журналистском образовании // Международный научный журнал «Слово в науке». 2024. №17. С. 9–15.
2. Макарова Л.С. Методические подходы к формированию навыков верификации информации у студентов, обучающихся по направлению «Журналистика»: опыт реализации проекта EUFactcheck/#СТУДФАСТСНЕСК в институте филологии и журналистики ННГУ им. Н.И. Лобачевского // Челябинский гуманитарий. 2022. №1 (58). С. 70–79.
3. Малиновская Е.Л. Совладающее поведение как предмет исследования психологии личности // Вестник УРАО. 2016. №2. С. 134–138.
4. Матвеева Е.П., Кощеева Е.С. Проблемы поиска достоверной информации студентами в сети интернет // Педагогическое образование в России. 2021. №4. С. 51–57.
5. Перечень информационных ресурсов, регулярно распространяющих недостоверную информацию // Официальный сайт Роскомнадзора. Публикация от 29.11.2025. Последнее изменение: 27.12.2023. URL: https://rkn.gov.ru/activity/mass-media/violators/ (дата обращения: 28.11.2025).
6. Begishev I. (2021) Cyber-Security Culture: Psychological and Legal Aspects // Psychology and Law 11(4):207-220. https://doi.org/10.17759/psylaw.2021110415.
7. Blackett C. (2025) Learning from Safety Culture to Optimize Cybersecurity Culture // Conference: European Safety and Reliability (ESREL)At: Stavanger, Norway. 8 p. https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P8863-cd.
8. Reegård K., Blackett C., Katta V. (2019) The Concept of Cybersecurity Culture // Conference: 29th European Safety and Reliability Conference (ESREL)At: Hannover. https://doi.org/10.3850/978-981-11-2724-3_0761-cd.
9. Sandi S., Berg C. van den (2025) South African Journal of Information Management // SA Journal of Information Management 27(1). https://doi.org/10.4102/sajim.v27i1.2044.
10. Ünver H.A. (2023) Emerging Technologies and Automated Factchecking: Tools, Techniques and Algorithms // 54 p. https://doi.org/10.13140/RG.2.2.20514.20165.
11. Wang M., Zhang X., Han X. (2025) AI Driven Systems for Improving Accounting Accuracy Fraud Detection and Financial Transparency // Frontiers in Artificial Intelligence Research. Vol. 2. Iss. 3. Pp. 403-421. https://doi.org/10.71465/fair398.



Журнал «Современная наука: актуальные проблемы теории и практики»