Электронный журнал
Современная зарубежная психология,
2026. *15*(2), 91—101.
https://doi.org/10.17759/jmfp.2026150209
ISSN: 2304-4977 (online)

E-journal
Journal of Modern Foreign Psychology,
2026. *15*(2), 91—101.
https://doi.org/10.17759/jmfp.2026150209
ISSN: 2304-4977 (online)

Обзорная статья | Review paper

Информационно-цифровая безопасность в контексте осведомленности молодежи Монголии о социальных рисках

Ц. Цэцэнбилэг[1, 2] ✉, **О.С. Хатанболд**[1]
[1] Институт философии Монгольской академии наук, Улан-Батор, Монголия
[2] Институт иностранных языков Российского университета дружбы народов имени Патриса Лумумбы, Москва, Российская Федерация
✉ tsetsenbilegts@gmail.com

Резюме

Контекст и актуальность. В условиях современного общества формируется принципиально иная структура производства и потребления информации. Роль инструментов для получения, моделирования и передачи данных непрерывно возрастает. Интернет-технологии превратились в «среду обитания» современных поколений, трансформировав или заменив важные сферы жизнедеятельности. Наряду с очевидными преимуществами, «новый мир» принес колоссальное количество уязвимости в отношении безопасности личности и субъектов труда. В системах актуальной защиты от информационных рисков осведомленность и разборчивость пользователей являются одной из ключевых составляющих. Несмотря на то, что молодежь изначально (фактом рождения) изрядно компетентна в возможностях интернет-пространства и погружена в него, ее уязвимость к негативному и деструктивно-мошенническому влиянию, также остается высокой. **Цель** исследования состояла в выявлении осведомленности монгольской молодежи об информационно-цифровой безопасности и определении социальных рисков, связанных с использованием цифровых технологий. **Метод и выборка**. Социологический опрос проведен на многоступенчатой стратифицированной выборке из 800 молодых людей в возрасте 18—34 лет, представляющих различные регионы Монголии. *Обработка данных* проводилась с применением дескриптивной статистики, сравнительного анализа, метода K-средних (k-means), регрессионного, кластерного, факторного и дисперсионного анализа (ANOVA), индексных расчетов. **Гипотеза**. Осведомленность молодежи о цифровых рисках может оказаться значительно выше, чем реальные навыки обеспечения своей безопасности в информационно-цифровой среде. **Результаты** свидетельствуют о недостаточном уровне цифровой грамотности молодежи. Распространена инфантильная недооценка рисков («со мной этого не случится») и слабость рефлексивной позиции. Молодые люди знают или слышали о цифровых рисках (осознают недопустимость передачи третьим лицам своих банковских данных, паролей от интернет-сервисов и кодов доступа к социальным сетям, понимают прямую связь между защитой информации и сохранением своей репутации в цифровом мире), но практические навыки защиты остаются слабыми. Сферы образования, профессиональной подготовки, экономики и досуга определяются молодежью в качестве наиболее уязвимых в процессе цифровизации. Городская молодежь несколько лучше осведомлена о положительных и отрицательных сторонах цифровизации, однако и те и другие обладают недостаточными знаниями о конкретных методах самозащиты. Молодые люди без образования или с начальным уровнем образования слабо осведомлены о социальных последствиях цифровизации, в отличие от тех, у кого уровень образования выше. Молодые люди склонны активно участвовать и высказываться в дискуссиях, возникающих в «сетях» и цифровом пространстве, но при этом слабо учитывают вопросы безопасности. Проявился феномен переоценки объективности и достоверности информации, полученной в цифровой среде. **Выводы**. Оценка уровня осведомленности о рисках цифровой среды и их последствиях выявила критический разрыв: пользователи осознают наличие потенциальных угроз, однако не обладают достаточными практическими знаниями для применения защитных мер. Минимизация социальных рисков, связанных с цифровизацией, требует смещения акцента с ограничений времени в Сети, родительского контроля или чрезмерного законодательного регулирования в сторону формирования индивидуального сознания. Ключевым фактором становится воспитание культуры разумного и этичного поведения в цифровом пространстве, а также повышение личной моральной ответственности каждого пользователя.

***Ключевые слова*:** цифровизация, социальные риски, молодежь Монголии, осведомленность, информационная безопасность, цифровая грамотность

Для цитирования: Цэцэнбилэг, Ц., Хатанболд, О.С. (2026). Информационно-цифровая безопасность в контексте осведомленности молодежи Монголии о социальных рисках. *Современная зарубежная психология, 15*(2), 91—101. https://doi.org/10.17759/jmfp.2026150209

Information and digital security in the context of awareness of Mongolia's youth about social risks

Tsetsenbileg Ts.[1, 2] ✉, **Khatanbold O. Sartuul**[1]
[1] Institute of Philosophy of the Mongolian Academy of Sciences, Ulaanbaatar, Mongolia
[2] Institute of Foreign Languages P. Lumumba Peoples' Friendship University of Russia, Moscow, Russian Federation
✉ tsetsenbilegts@gmail.com

Abstract

Context and relevance. In modern society, a fundamentally different structure of information production and consumption is being formed. The role of tools for obtaining, modeling, and transmitting data is continuously increasing. Internet technologies have become the «habitat» of modern generations, transforming or replacing important spheres of life. Along with the obvious advantages, the «new world» has brought a huge amount of vulnerability regarding the security of individuals and labor subjects. In current information risk protection systems, user awareness and intelligibility are one of the key components. Despite the fact that young people are initially immersed (by birth) and fairly competent in the possibilities of the Internet space, their vulnerability to negative and destructive fraudulent influence remains high. **The purpose** of the study was to identify the awareness of Mongolian youth about information and digital security and to identify the social risks associated with the use of digital technologies. **Method and selection**. The sociological survey was conducted on a multi-stage stratified sample of 800 young people aged 18—34 representing various regions of Mongolia. The data was processed using descriptive statistics, comparative analysis, k-means, regression, cluster, factor and variance analysis (ANOVA), and index calculations. **Hypothesis**. The awareness of young people about digital risks may be significantly higher than the real skills of ensuring their safety in the information and digital environment. **The results** indicate an insufficient level of digital literacy among young people. There is a widespread infantile attitude of underestimating risks («this will not happen to me») and the weakness of a reflexive position. Young people know or have heard about digital risks (they are aware of the inadmissibility of transferring their bank data, passwords from Internet services and access codes to social networks to third parties, they understand the direct link between protecting information and preserving their reputation in the digital world), but practical protection skills remain weak. The fields of education, vocational training, economics and leisure are identified by young people as the most vulnerable in the process of digitalization. Urban youth are somewhat more aware of the positive and negative sides of digitalization, but both have insufficient knowledge of specific methods of self-defense. Young people without an education or with a primary level of education are poorly aware of the social consequences of digitalization, unlike those with a higher level of education. Young people tend to actively participate and speak out in discussions that arise in the "networks" and the digital space, but they do not take security issues into account. The phenomenon of overestimating the objectivity and reliability of information obtained in the digital environment has emerged. **Conclusions**. An assessment of the level of awareness about the risks of the digital environment and their consequences revealed a critical gap: users are aware of potential threats, but do not have sufficient practical knowledge to apply protective measures. Minimizing the social risks associated with digitalization requires shifting the focus from online time constraints, parental control, or excessive legislative regulation towards the formation of individual consciousness. The key factor is fostering a culture of reasonable and ethical behavior in the digital space, as well as increasing the personal moral responsibility of each user.

Keywords: digitalization, social risks, youth of Mongolia, awareness, information security, digital literacy

For citation: Tsetsenbileg, Ts., Khatanbold, O.S. (2026). Information and digital security in the context of awareness of Mongolia's youth about social risks. *Journal of Modern Foreign Psychology, 15*(2), 91—101. (In Russ.). https://doi.org/10.17759/jmfp.2026150209

Введение

В условиях современного общества формируется принципиально иная структура производства и потребления информации. Роль инструментов для получения, моделирования и передачи данных непрерывно возрастает: от появления фотокамеры в XIX веке до возникновения «Всемирной паутины» (Интернета) и развития технологий искусственного интеллекта (ИИ, AI) в наши дни. Внедрение персональных компьютеров и мобильных средств связи в конце 80-х годов XX века, а также развитие Интернета в начале 90-х, ознаменовали начало новой эры. Информационные новшества полностью изменили привычный ритм человеческой и общественной жизни. Современное поколение не может представить ни дня без Интернета, который заменяет собой все: от общения с близкими и походов в кино, до образования и путешествий. Интернет стал не просто связующим звеном между человеком и миром, но превратился в специфическую культуру нашего времени, во многом (а порой и полностью) подменив собой важные сферы жизнедеятельности (Park et al., 2024, Carroll et al., 2023; Zhuravlov et al., 2020).

Согласно данным национальной статистики Монголии за 2021 год, при общей численности населения в 3 409 млн человек 4,137 млн человек зарегистрированы как постоянные пользователи Интернета, к 2024 году количество пользователей возросло до 4,887 тыс. при численности населения 3,546 (на 2024 год), т. е. пользователей зарегистрировано больше, чем жителей[1].

Приведенные показатели свидетельствуют о том, что новые технологии и созданное на их основе цифровое пространство стали не только важнейшей частью жизни, но и подтверждают растущую потребность в развитии цифровой психологии и социологии как отдельных отраслей научного знания. С другой стороны, существующее неравенство в доступе к Интернету связано с определенными социальными проблемами и является отражением степени активного участия индивидов в цифровом пространстве. Суть данного процесса заключается в трансформации общества и переходе на новый этап развития под влиянием цифровизации, что ведет к обновлению всей системы общественных отношений (Чулуунбаатар, Хатанболд, 2014).

Очевидно, что в результате этого процесса реформируются социальная структура, экономика, образовательные отношения, ценностные ориентации и повседневный образ жизни. Мир вступил в эпоху активного участия индивидуума не только в получении, но и в создании, моделировании информации, превращении ее в неотъемлемую часть работы, отдыха и повседневной коммуникации (Жиллнер, 2001, Веселов и др., 2023).

Информация из Интернета становится мощным фактором в современной политической практике, коммерческой деятельности и художественном творчестве, что диктует необходимость глубокого осмысления данных условий (Жиллнер, 2001).

В эпоху Интернета и цифровых технологий коренным образом меняются формы обучения, развития, досуга и взаимодействия детей, открывая широкие возможности для самовыражения и получения знаний (Marshall et al., 2018). Вместе с тем необходимо обратить внимание на рост рисков: столкновения детей с неподобающим контентом (сцены насилия, порнография), а также угрозы со стороны киберпреступности, превращающей детей в жертв или нарушителей закона (Joshi, Singh, 2017; Wiederhold, 2024; Fletcher, 2022).

Понятийно-терминологические основы исследования

Структура и компоненты информационной безопасности. В рамках рассматриваемой проблематики представляется целесообразным показать возможности обеспечения информационной безопасности в практической деятельности.

Информационную безопасность можно рассматривать как процесс и методологию, направленную на защиту личной, строго конфиденциальной информации и больших данных (в печатном, электронном и других форматах) от несанкционированного доступа, использования, а также от злоупотребления, разглашения, уничтожения, изменения или прерывания работы с ней[2]. В то же время, информационную безопасность (InfoSec) понимают и как совокупность практик, направленных на защиту конфиденциальной информации, центров обработки данных и облачных приложений. Протоколы информационной безопасности предотвращают несанкционированный доступ, использование, раскрытие, нарушение или уничтожение данных[3]. Защищаемая информация может быть любой: электронной, физической (документы) или нематериальной (знания).

В русскоязычном варианте триада информационной безопасности (Confidentiality (конфиденциальность), Integrity (добросовестность), Availability (доступность)) обозначается как КЦД — *конфиденциальность* (доступ к ресурсам только тех пользователей или устройств, которые прошли авторизацию), *целостность* (полнота и достоверность данных, уверенность в том, что они не подверглись несанкционированным изменениям в процессе хранения), *доступность* (надежность и своевременность («в любой момент») доступа к ресурсам для тех, кто имеет на это право) (Веселов и др., 2023).

Конфиденциальность предполагает, что «любая информация не будет открыта или разглашена лицам, организациям или общественности, не имеющим на то законного разрешения» (Beckers, 2015). Конфиденциальность — это элемент безопасности, который реализуется для защиты информации от тех, кто пытается использовать ее без разрешения. К наиболее распространенным примерам нарушения конфиденциальности электронной информации можно отнести кражу ноутбука, кражу пароля для входа в систему или отправку строго конфиденциального электронного письма не тем людям.

Целостность информационных данных это сохранение и обеспечение точности и полноты информации

[1] National Statistics Office of Mongolia. (2024). Number of internet users and computers, by region, aimags and the Capital, and by year (Note: Due to revisions and updates to the survey forms and methodology for the information and communications sector, no data enrichment has been applied to the statistics from 2024 onward.). URL: https://www.1212.mn/en/statcate/table-view/Industry,%20service/Telecommunication/DT_NSO_1300_012V1_y.px?subtables=NUMBER%20OF%20INTERNET%20USERS%20AND%20COMPUTERS,%20by%20region,%20aimags%20and%20the%20Capital (viewed: 02.06.2026).

[2] SANS Institute. (2016). Information Security. https://www.sans.org/security-resources/glossary-of-terms/information-security

[3] DOT Security. (2024, October 10). What are the 3 Components of Information Security? URL: https://dotsecurity.com/insights/blog-what-are-the-components-information-security (viewed: 02.06.2026).

на протяжении всего ее жизненного цикла, при этом данная информация не может быть изменена несанкционированным или незамеченным образом (Efrim, 2005). Эта гарантия данных, соответствует модели ACID* (atomicity/атомарность, consistency/согласованность, isolation/изолированность, durability/долговечность), предназначенной для передачи и обработки информации (Haerder, Reuter, 1983)[4].

В более широком смысле, гарантия целостности информационных данных — это принцип информационной безопасности, который охватывает человеческие (социальные) отношения, а также, коммерческую честность и гарантию доступа к информации (Efrim, 2005; Stoneburner, Hayden, Feringa, 2004; Boritz, 2005; Kanahaiya, Pramod, 2023; Kelley at al., 2023).

Названные элементы *«триады информационной безопасности»* (по DOT Security, 2024), стали основными направлениями в сфере информационной безопасности, которые позволяют эффективно внедрять различные «”политики” и новшества без ущерба для производительности любой организации» (Sarkar, Shukla, 2023). Триада информационной безопасности реализуется через *организованный процесс управления рисками*, который включает (по DOT Security, 2024):

— *выявление* потенциальных *угроз*, уязвимостей и воздействий на информацию и связанные с ней активы;

— принятие решений о том, *как реагировать на риск* (избеганием, снижением, принятием и т. п.) и устранение сбоев непосредственно, в процессе оценки рисков;

— при необходимости снижения риска выбор, планирование и *внедрение* соответствующих *мер контроля безопасности*.

Представленная модель триады подразумевает ежедневный мониторинг операционной деятельности и внесения необходимых корректировок для постоянного улучшения в решении возникающих проблем.

Еще одно направление информационной безопасности («infosec») — это *практические действия по защите информации* путем снижения информационных рисков (Marshall et al., 2018). Это та часть управления информационными рисками, которая включает предотвращение ненадлежащего несанкционированного доступа к данным, их незаконного использования, разглашения, прерывания доступа, уничтожения, использования в коррупционных целях, внесения сторонних изменений, проверки, записи и обесценивания (Joshi, Singh, 2017). Таким образом, это любые виды деятельности, направленные на снижение негативного воздействия.

Системы информационной безопасности, как правило, включают средства контроля для обеспечения собственной надежности, в частности, для защиты ядра и основных функций системы от преднамеренных и случайных угроз (Beckers, 2015).

Для стандартизации информационной безопасности необходимо сотрудничество исследователей и специалистов разного профиля (Розенова, Огнев, Лихачева, 2025а), что позволит оптимизировать руководящие принципы, политики и отраслевые стандарты безопасности — пароли, антивирусное программное обеспечение, программы шифрования, юридические документы об ответственности, а также повысить осведомленность в области безопасности.

К настоящему моменту уже есть разветвленные стандарты, закрепленные законами и правилами, регулирующими доступ, обработку, хранение, передачу и уничтожение данных. Однако внедрение любых стандартов и руководств имеет ограниченную эффективность, если не удастся сформировать *культуру* постоянного улучшения и соблюдения требований. Например, в «Руководящих принципах по безопасности информационных систем и сетей» Организации экономического сотрудничества и развития (ОЭСР), пересмотренных в 1992 и 2002 годах, предложены девять общепризнанных принципов: «осведомленность, ответственность, реагирование, этика, демократия, оценка рисков, разработка и внедрение правил безопасности, а также управление безопасностью». На основе этих принципов в 2004 году были предложены еще 33 дополнительных принципа проектирования безопасности информационных технологий NIST (Stoneburner, Hayden, Feringa, 2004), которые были детерминированы результатами практики.

Риски и угрозы информационной безопасности в цифровой среде

Существуют десятки форм угроз, которые могут представлять риск для информационной безопасности (атаки на программное обеспечение, кража интеллектуальной собственности, кража личных данных, кража оборудования и информации, саботаж и информационный разбой). Кража интеллектуальной собственности продолжает наносить значительный ущерб во многих сферах деятельности, в том числе предпринимателям в сфере информационных технологий (IT) (Zhuravlov et al., 2020). Распространенной тенденцией стала кража жизненно важной личной информации путем проникновения в частные данные с использованием методов социальной инженерии. Повсеместное использование мобильных устройств увеличило объем таких данных и привело к резкому росту киберпреступности, основанной на краже, уничтожении или распространении личных данных, что стало серьезным вызовом для цифрового развития (Wiederhold, 2024; Розенова, Огнев, Лихачева, 2025а).

[4] Модель ACID, используемая в информатике, понимается как набор транзакционных свойств базы данных, предназначенных для обеспечения валидности данных независимо от ошибок программного обеспечения, перебоев в подаче электроэнергии и других сторонних рисков.

Современный мир наработал множество способов защиты от названных угроз и атак (Stoneburner, Hayden, Feringa, 2004; Efrim, 2005; Haerder, Reuter, 1983), но наиболее важным средством является *системная профилактика*, включающая как технологические системы защит (совершенствование программного обеспечения, увеличение IT-затрат, постоянство мобильного мониторинга и прочее), так и работу с населением (постоянство информирования и активного обучения (Розенова, Огнев, Лихачева, 2025b)

Тотальная цифровизация определила изменение способов влияния и распространения идей через цифровую среду, что создало риск превращения общества в «конформистов», чрезмерно зависимых от виртуального мира[5] (Verma, 2024; Cross, Lee, 2022; Vize, Byrd, Stepp, 2023). Например, наука еще не в полной мере оценила реальную роль Интернета в современной политике. Идеологический экстремизм, терроризм и киберугрозы продолжают негативно влиять на национальную безопасность. Возникла острая необходимость научного изучения методов защиты от этих угроз. Ярким примером является использование социальных сетей для организации массовых протестов, что требует принятия мер по управлению общественным сознанием (Чулуунбаатар, Хатанболд, 2014).

Быстрый рост Интернета стал почвой для вовлечения молодежи в деятельность экстремистских организаций и негативных сообществ. Сетевые группы в форме реального социального взаимодействия в Интернете стали активно влиять на общественные дискуссии (пикеты, демонстрации, группы массовых суицидов или аутоагресии и т. п) (Цэцэнбилэг, Хатанболд, 2024). Поэтому ограничение, контроль и выявление позитивных и негативных сторон цифрового взаимодействия стали важнейшей задачей для институтов национальной безопасности и научных организаций (Цэцэнбилэг, Хатанболд, 2024).

Цель исследования. Наш исследовательский интерес определился необходимостью выявления социальных рисков для молодежи, связанных с использованием цифровых технологий, на основе анализа осведомленности монгольской молодежи об информационно-цифровой безопасности.

В статье представлена часть результатов большого социологического исследования, проведенного в рамках совместного проекта «Социальные риски молодежи Беларуси и Монголии в условиях цифровизации» (ШУТ ХТБ-2022/01) на базе Улан-Баторского парка науки и технологий МУИС.

Выборку исследования составила многоступенчатая стратифицированная выборка из 800 молодых людей в возрасте 18—34 лет, представляющих различные регионы Монголии: Увс (Западный регион), Оворхангай (Хангайский регион), Дорноговь (Центральный регион), Дорнод (Восточный регион), а также из городов Дархан и Улан-Батор. По результатам исследования была издана коллективная монография и опубликованы статьи в соавторстве с белорусскими коллегами (Цэцэнбилэг, Хатанболд, 2024; Шкурова, Новицкий, Цэцэнбилэг, 2024).

Обработка данных проводилась с применением дескриптивной статистики, сравнительного анализа, метода K-средних (k-means), регрессионного, кластерного и факторного анализа, дисперсионного анализа (ANOVA) и индексных расчетов.

Результаты исследования осведомленности монгольской молодежи о цифровых рисках

В ходе исследования выявилось следующее: 65,3% респондентов хорошо знают о компьютерных вирусах, 61% — о дезинформации (фейковых новостях), 59,1% — об интернет-зависимости и 51,5% — о киберкражах и мошенничестве, 35,9% опрошенных слышали о возможности управления человеческим сознанием и поведением через информацию. Более подробно информация представлена в сводной таблице (табл. 1).

В силу многочисленности и емкости таблиц, отражающих исследовательские результаты, в тексте мы приводим описание уже проведенного качественно-содержательного анализа, который показал, что среди молодежи в возрасте 18—32 лет сельские жители чаще, чем городские, считают, что риски возросли с началом эпохи цифровизации. Хотя молодежь знает или слышала о цифровых рисках, практические навыки защиты остаются слабыми. Полученные результаты свидетельствуют о недостаточном уровне цифровой грамотности. Наиболее распространенной установкой молодежи является убеждение, что «со мной этого не случится», свидетельствующей о слабости рефлексивной позиции по отношению к своему и чужому опыту и легкомысленном отношении к кибербезопасности.

В отношении *последствий цифровизации*, *нарушения информационной безопасности* были определены молодыми респондентами как последствия с наиболее высоким уровнем риска. Молодые люди глубоко осознают недопустимость передачи третьим лицам своих банковских данных, паролей от интернет-сервисов и кодов доступа к социальным сетям, содержащим конфиденциальную информацию. Наблюдается высокая степень осмотрительности: молодежь стремится обеспечивать безопасность личных данных, понимая прямую связь между защитой информации и сохранением своей репутации в цифровом мире.

[5] Fletcher, E. (2022, January 25). Social media a gold mine for scammers in 2021 (Data Spotlight). Washington: Federal Trade Commission. URL: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021 (viewed: 02.06.2026).

Таблица 1 / Table 1

Осведомленность молодежи о цифровых рисках (примененные варианты ответов: 1 — знаю, 2 — слышал, 3 — не знаю)
Young People's Awareness of Digital Risks (Response options used: 1 — I know, 2 — I've heard, 3 — I don't know)

№ п/п	Показатель / Indicator	Знаю / I know (%)	Слышал / Heard (%)	Не знаю / Don't know (%)	Среднее значение / Average value
1	Компьютерные вирусы / Computer viruses	65,3	24,1	10,6	1,5
2	Интернет-зависимость / Internet addiction	59,1	28,6	12,3	1,5
3	Информационная война / Information war	38,8	32,1	29,1	1,9
4	Фейковые новости / Fake news	61,0	25,9	13,1	1,5
5	Конфиденциальные учетные данные / Confidential credentials	29,5	33,3	37,3	2,1
6	Киберкражи, мошенничество / Cyber theft, fraud	51,5	34,8	13,8	1,6
7	Управление сознанием и поведением / Cyber theft, fraud	36,5	35,9	27,6	1,9
8	Право на неприкосновенность частной жизни / Right to privacy	43,1	34,9	22,0	1,8
9	Право на защиту репутации / The right to protect one's reputation	49,3	28,5	22,3	1,7
ИТОГО		**1,7**			

Вторым по значимости аспектом влияния цифровизации молодежь назвала *последствия криминального характера*. В последние годы масштабы виктимизации (превращения в жертву) в результате киберпреступлений значительно увеличились. Особую тревогу вызывает рост психологического давления на подростков: злоумышленники «отлавливают» размещенную в Сети информацию или случайные негативные/девиантные действия молодых людей, используя их для дальнейшего шантажа и угроз (Розенова, Огнев, Лихачева, 2025а). Эти процессы становятся фундаментом для распространения преступности в цифровой среде (Sarkar, Shukla, 2023; Wiederhold, 2024)

Факторизация результатов оценки осведомленности монгольской молодежи о рисках и последствиях цифровизации

Обобщенные результаты исследования подтверждают, что в плане информационной безопасности для молодежи наиболее важными аспектами являются: «Никому не передавать свои пароли и коды (банковские, интернет-сервисы и т. д.)», «Обеспечение безопасности личных данных для защиты своей репутации» и «Использование Интернета в образовательных целях».

Было выявлено, что социальные риски, проявляющиеся в молодежной среде, характеризуются многогранностью и взаимозависимостью. Сферы образования, профессиональной подготовки, экономики и досуга оказались наиболее уязвимыми к социальным рискам, сопровождающим процесс цифровизации.

Для уточнения и обобщенного понимания результатов изучения последствий цифровизации мы применили процедуры факторизации данных, с помощью которых были выделены два основных фактора: *Фактор 1,* отразивший недостаточную осведомленность о последствиях цифровизации, но наличие фактологической основы о феноменологии рисков в цифровой среде, и *Фактор 2*, объединивший знания о механизмах и последствиях функционирования цифровой среды (табл. 2).

На основе выделенных факторов был рассчитан индекс осведомленности молодежи о рисках цифровизации в разрезе «город — сельская местность» (табл. 3).

Таблица 2 / Table 2

Факторные интеграции оценки молодежью последствий влияния цифровизации
Factor integration of youth assessment of the consequences of digitalization

№ п/п	Показатель	Фактор 1	Фактор 2
1	Информация в СМИ влияет на мысли и поведение человека / Information in the media affects a person's thoughts and behavior,	0,108	**0,775**
2	Каналы СМИ (газеты, радио, ТВ, сайты) могут быть как частными, так и государственными / Media channels (newspapers, radio, TV, and websites) can be both private and public	0,245	**0,729**
3	Цифровая коммуникация включает сбор и хранение данных о пользователях / Digital communication includes the collection and storage of user data,	0,332	**0,683**
4	Анонимность в Интернете зачастую неэффективна; каждого пользователя можно идентифицировать / Online anonymity is often ineffective; every user can be identified	0,120	**0,794**
5	Размещение определенной информации в Интернете может негативно сказаться на личной жизни и карьере / Sharing certain information on the internet can have a negative impact on your personal life and career,	0,240	**0,692**

№ п/п	Показатель	Фактор 1	Фактор 2
6	Интернет можно использовать в образовательных целях / The Internet can be used for educational purposes,	0,569	0,416
7	Никому нельзя передавать свои пароли и коды (банки, интернет и др,) / You should not share your passwords and codes with anyone (banks, the internet, etc,)	**0,715**	0,160
8	Необходимо обеспечивать безопасность личных данных для защиты репутации / It is necessary to ensure the security of personal data in order to protect your reputation,	**0,700**	0,246
9	Киберпреступность (мошенничество через чаты/мессенджеры) / Cybercrime (fraud via chat rooms/messengers)	**0,801**	0,259
10	Причинение психологического вреда подросткам / Causing psychological harm to teenagers	**0,857**	0,173
11	Сексуальные домогательства в отношении подростков / Sexual harassment of teenagers	**0,850**	0,133
12	Отправка или вымогательство интимных фото и видео / Sending or extorting intimate photos and videos	**0,795**	0,237

Таблица 3 / Table 3

Индекс осведомленности о рисках цифровизации (%)
Digitalization Risk Awareness Index (in percent)

№ п/п	Регион / Region	Осведомлены Informed	Средний уровень Intermediate level	Не осведомлены Not informed
1	Город / City	37,1%	32,7%	30,3%
2	Сельская местность / Countryside	29,2%	35,9%	34,9%

Качественно-количественный анализ позволил заключить следующее: *городская молодежь* в целом осознает наличие как положительных, так и отрицательных сторон цифровизации, однако обладает недостаточными знаниями о конкретных методах самозащиты. Доля абсолютно не осведомленных молодых людей в городе составляет 30,3%. *Сельская молодежь* демонстрирует более низкие показатели: доля не осведомленных о рисках составляет почти 35% (34,9%).

Мы также рассмотрели осведомленность молодежи о рисках цифровизации в соотнесении с ее образовательным уровнем. Результаты отражены в табл. 4.

Из табл. 4 видно, что 75% молодых людей без образования или с начальным уровнем образования имеют недостаточные знания о социальных последствиях цифровизации. Молодежь с неполным средним, полным средним и средним специальным образованием обладает средним уровнем знаний о негативных последствиях социальной среды. Можно сделать вывод, что молодые люди с высшим образованием (степень бакалавра) относительно лучше осведомлены в данном вопросе.

В рамках исследования при анализе корреляции вышеупомянутых показателей было выявлено, что среди молодежи в возрасте 18—32 лет частота написания писем в редакции газет, журналов, телевидения и радио, а также звонки или SMS-сообщения в прямые эфиры радио- и телепередач находятся на сопоставимом уровне. При расчетах мы опирались на корреляцию и ковариацию, исходя из допущения, что группы переменных с высокой степенью корреляции представляют схожие факторы.

Качественный анализ результатов исследования выявил общие тенденции: опрошенные молодые люди выражают свое мнение в ходе программ с открытыми дискуссиями; пишут письма на FM-радио или передают свои комментарии по телефону; следят за страницами определенных инфлюенсеров, оставляя комментарии и делясь публикациями; обращаются с жалобами и предложениями по конкретным вопросам в правительственный информационный центр для граждан «11—11».

Таблица 4 / Table 4

Индекс осведомленности молодежи о рисках цифровизации в детерминации уровня образования
Index of youth awareness of the risks of digitalization in determining the level of educatio

№ п/п	Уровень образования / Level of education	Осведомлены / Informed	Средний уровень / Intermediate level	Не осведомлены / Not informed
1	Без образования / No education	25,0%	0,0%	75,0%
2	Начальное / Initial	20,0%	20,0%	60,0%
3	Неполное среднее / Incomplete secondary	30,0%	50,0%	20,0%
4	Полное среднее / Complete secondary education	30,3%	38,9%	30,8%
5	Среднее специальное / Secondary specialized	28,3%	38,3%	33,3%
6	Высшее (бакалавр) / Higher (bachelor's degree)	37,5%	30,2%	32,2%
7	Высшее (магистр) / Higher (Master's)	29,3%	39,0%	31,7%

Для активных пользователей Интернета характерно выражение своей позиции, комментирование и обмен мнениями в формате постов в социальных сетях. Результаты исследования также подтвердили, что, несмотря на осведомленность о настройках приватности и необходимости обеспечения информационной безопасности в цифровой среде, навыки их практического применения среди молодежи остаются на недостаточном уровне.

Практика использования социальных сетей среди молодежи

В вопросе использования социальных сетей молодежь отдает приоритет доступу через мобильные устройства с использованием передачи данных. Основными платформами для получения желаемой информации выступают социальные сети. Согласно результатам, 76,5% молодых людей имеют один аккаунт в одной из социальных сетей, при этом доля активных пользователей, проводящих в социальных сетях более 2 часов в день, достаточно высока и составляет 43,4%. Респонденты отмечают, что зачастую заходят в социальные сети привычно, без конкретной цели, как только открывают мобильный телефон. Около 29,9% опрошенных являются активными создателями контента: они ведут собственные «страницы» (page), ежедневно делятся публикациями и «сторис».

Что касается защиты персональных данных, 36,8% молодых людей в возрасте 18—32 лет слышали о настройках конфиденциальности и знают о них, однако на практике в повседневной деятельности большинство их не используют. Несмотря на массовое использование социальных сетей, меры по обеспечению безопасности личной информации остаются слабыми, а уровень практических знаний о последствиях цифровизации — недостаточным.

Исследование показало, что молодежь склонна отождествлять понятие «социальные сети» непосредственно с платформами, которые используются для обмена в Интернете. Это свидетельствует не только о повсеместном доступе к Интернету, но и о росте числа молодых людей, проявляющих высокую активность в Сети (более 2 часов ежедневно). Положительной тенденцией является стремление молодежи перепроверять полученную информацию в Интернете для ее верификации. Однако респонденты по-прежнему склонны обращаться к прямым эфирам радио и телевидения при возникновении проблемных ситуаций. Также наблюдается феномен «иллюзии знания», когда информация, полученная из социальных сетей, от друзей или из телепередач, ошибочно принимается за достоверное научное или объективное знание.

Полученные в исследовании результаты указывают на высокий уровень рисков, связанных с Интернетом и социальными сетями. Стремление к быстрому и легкому получению информации, с одной стороны, ведет к позитивным результатам, но с другой стороны чревато искажением фактов, контактами с недоброжелателями, финансовыми потерями, а также риском стать жертвой психологического, физического или сексуального насилия.

Выводы

Проведенное исследование и анализ его результатов свидетельствуют о том, что последствия цифровизации в Монголии носят двойственный характер. Результаты подтверждают прямое влияние интернета на поведение и социальные установки человека. Оценка уровня осведомленности о рисках цифровой среды и их последствиях выявила критический разрыв: пользователи осознают наличие потенциальных угроз, однако не обладают достаточными практическими знаниями для применения защитных мер. Данное обстоятельство указывает на высокую вероятность эскалации масштабных рисков в долгосрочной перспективе.

Современное общество и его реалии продолжают доказывать, что важнейшим аспектом является формирование в себе морали, обладающей нормами мышления, которая по своей сути опирается на поведение, нравственность, личностное развитие и коммуникацию человека (Жиллнер, 2001), объединяя в себе четыре этих элемента.

В рамках представленного исследования была предпринята попытка детально проанализировать информационно-социальные риски набирающей обороты цифровизации с целью прогнозирования и предотвращения их потенциальных негативных последствий в повседневной жизни молодежи. Результаты продемонстрировали, что понимание и представление о социальных рисках, возникающих вследствие цифровизации, среди молодых людей остаются на недостаточном уровне. Традиционно социальные риски воспринимаются населением через призму экономических или природных факторов, в отношении которых потребность в превентивных мерах осознается более четко.

С другой стороны, минимизация социальных рисков, связанных с цифровизацией, требует смещения акцента с простых ограничений времени в сети, родительского контроля или чрезмерного законодательного регулирования в сторону формирования индивидуального сознания. Ключевым фактором становится воспитание культуры разумного и этичного поведения в цифровом пространстве, а также повышение личной моральной ответственности каждого пользователя. Для демократического общества ограничение фундаментальных конституционных прав граждан на поиск и распространение информации не является приемлемым методом.

Напротив, в условиях современного цифрового мира критически важным становится научное обоснование и практическая реализация этического образования путем выявления социальных факторов, влияющих на моральный облик личности во всех сферах общественной жизни.

На основании вышеизложенного можно сделать вывод, что основным путем повышения нравственного уровня современного монгольского общества является улучшение качества и результативности этического образования. На первый план выходит задача формирования гражданина, обладающего высокой цифровой этикой, что должно рассматриваться как фундамент социального развития и ключевой фактор человеческого прогресса.

Список источников / References

1. Веселов, Ю.В., Карапетян, С.Р., Белова, М.В., Скворцов, Н.Г., Чернов, Г.И., Дудина, В.И. (2023). *Доверие в цифровом мире*: *Монография* (Ю.В. Веселов, общ. ред.). Москва: Ай Пи Ар Медиа.
   Veselov, Yu.V., Karapetyan, S.R., Belova, M.V., Skvortsov, N.G., Chernov, G.I., Dudina, V.I. (2023). Trust in the digital world: A monograph (Yu.V. Veselov, ed.). Moscow: IPR Media. (In Russ.).
2. Розенова, М.И., Огнев, А.С., Лихачева, Э.В. (2025b). Стратегии профилактики деструктивно-манипулятивного цифрового мошенничества. В: *Материалы IV научного форума с международным участием: Экстремальная психология в экстремальном мире* (с. 48—54). М.: Спутник+. URL: https://www.elibrary.ru/item.asp?id=89202974 (дата обращения: 02.06.2026).
   Rozenova, M.I., Ognev A.S., Likhacheva E.V. (2025b). Strategies for preventing destructive and manipulative digital fraud. In: *Proceedings of the IV scientific forum with international participation: Extreme psychology in an extreme world* (pp. 48—54). Moscow: Sputnik+. (In Russ.). URL: https://www.elibrary.ru/item.asp?id=89202974 (viewed: 02.06.2026).
3. Жиллнер, Э. (2001). *Соел ба түүний үүдэл: рационализм ба иррационалист хэлбэрийн түүхэн үүрэг, роль* (Э.Н. Хян., Х.О. Орч, ред.). Улаанбаатар: Бемби сан.
   Gillner, E. (2001). *Culture and its roots: The historical role of racism and irrationalist forms* (Eh.N Xian, Kh.O. Orch, eds). Ulaanbaatar: Bembi San.
4. Розенова, М.И., Огнев, А.С., Лихачева, Э.В. (2025a). Психологические механизмы деструктивного манипулирования и стратегии профилактики цифрового мошенничества. *Современная зарубежная психология, 14*(2), 26—37. https://doi.org/10.17759/jmfp.2025140203
   Rozenova, M.I., Ognev, A.S., Likhacheva, E.V. (2025a). Psychological mechanisms of destructive manipulation and strategies for preventing digital fraud. *Journal of Modern Foreign Psychology, 14*(2), 26—37. (In Russ.). https://doi.org/10.17759/jmfp.2025140203
5. Цэцэнбилэг, Ц., Хатанболд, О. (Ред.). (2024). *Цахимжилтын нөхцөл дэх Монгол, Беларусийн: Залуучуудын нийгмийн эрсдэл*. Улаанбаатар: Тод бичиг.
   Tsetsenbileg, Ts., Hatbold, Oh. (Eds). (2024). *Social risks of youth in Mongolia and Belarus in the context of digitization*. Ulaanbaatar: Tod Bichig.
6. Чулуунбаатар, Г., Хатанболд, О. (2014). Төлөөллийн ардчилал: Онол, үзэл баримтлалын зарим асуудал). *Философи, эрхийн судлал, 29*(1-32), 142—163.
   Chulunbaatar, G., Hatbold, O. (2014). Tilly democracy: On, some issues of Izzul doctrine. *Philosophy and Legal Studies , 29*(1-32), 142—163.
7. Шкурова, Е.В., Новицкий, Е.Н., Цэцэнбилэг, Ц. (2024). Особенности цифровых практик молодежи в Беларуси и Монголии. *Журнал Белорусского государственного университета. Социология, 2*, 58—67. URL: https://journals.bsu.by/index.php/sociology/ru/article/view/6313 (дата обращения: 02.06.2026).
   Shkurova, A.V., Navitsky, Ya.N., Tsetsenbileg, Ts. (2024). Features of digital practices of youth in Belarus and Mongolia. *Journal of the Belarusian State University. Sociology, 2*, 58—67. (In Russ.). URL: https://journals.bsu.by/index.php/sociology/ru/article/view/6313 (viewed: 02.06.2026).
8. Beckers, K. (2015). Pattern and Security Requirements: Engineering-Based Establishment of Security Standards. *Springer.*
9. Boritz, J.E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems, 6*(4), 260—279. https://doi.org/10.1016/j.accinf.2005.07.001
10. Carroll, M., Chan, A., Ashton, H., Krueger, D. (2023). Characterizing manipulation from AI systems. In: *EAAMO '23: Equity and Access in Algorithms, Mechanisms, and Optimization* (article 6). New York: Association for Computing Machinery. https://doi.org/10.1145/3617694.3623226
11. Cross, C., Lee, M. (2022). Exploring fear of crime for those targeted by romance fraud. *Victims & Offenders, 17*(5), 735—755. https://doi.org/10.1080/15564886.2021.2018080
12. Joshi, C., Singh, U.K. (2017). Information security risks management framework — A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128—137. https://doi.org/10.1016/j.jisa.2017.06.006

13. Kanahaiya, L.A., Pramod, K. (2023). Online Fraud. In: C.M. Gupta (Ed.), *Financial Crimes: A Guide to Financial Exploitation in a Digital Age* (pp. 97—108). Cham: Springer. https://doi.org/10.1007/978-3-031-29090-9_7
14. Kelley, N.J., Hurley-Wallace, A.L., Warner, K.L., Hanoch, Y. (2023). Analytical reasoning reduces internet fraud susceptibility. *Computers in Human Behavior, 142*, Article 107648. https://doi.org/10.1016/j.chb.2022.107648
15. Marshall, C., Byron, M., Crossler, R.E., Correia, J. (2018). InfoSec process action model (IPAM): Systematically addressing individual security behavior. *Database for Advances in Information Systems, 49*(SI), 49—66. https://doi.org/10.1145/3210530.32105
16. Park, P.S., Goldstein, S., O'Gara, A., Chen, M., Hendrycks, D. (2024). AI deception: A survey of examples, risks, and potential solutions. *Patterns, 10*(5), Article 100988. https://doi.org/10.1016/j.patter.2024.100988
17. Zhuravlov, L.P., Pomytkina, L.V., Lytvynchuk, A.I., Mozharovska, T.V., Zhuravlov, V.F. (2020). Psychological security in the conditions of using information and communication technologies. In: *Proceedings of the 1st Symposium on Advances in Educational Technology (AET 2020)* (pp. 216—223). https://doi.org/10.5220/0010930200003364
18. Sarkar, G., Shukla, S.K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 2*, Article 100034. https://doi.org/10.1016/j.jeconc.2023.100034
19. Stoneburner, G., Hayden, C., Feringa, A. (2004). *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.* Gaithersburg: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-27rA
20. Verma, A. (2024). The impact of call spoofing on trust and communication: A user perception study. *International Journal of Safety and Security Engineering, 14* (2), 487—498. https://doi.org/10.18280/ijsse.140216
21. Vize, C.E., Byrd, A.L., Stepp, S.D. (2023). The relative importance of psychopathy features as predictors of externalizing behaviors in youth: A multimethod examination. *Journal of Psychopathology and Behavioral Assessment, 45*(1), 1—17. https://doi.org/10.1007/s10862-022-10017-5
22. Wiederhold, B.K. (2024). Digital desires, real losses: the complex world of online romance fraud. *Cyberpsychology, Behavior, and Social Networking, 27*(5), 300—302. https://doi.org/10.1089/cyber.2024.29311.editorial

Информация об авторах

Цэцэнбилэг Цэвээн кандидат социологических наук, доцент, ведущий научный сотрудник отдела социологии, Институт философии Монгольской академии наук, Улан-Батор, Монголия; доцент, Институт иностранных языков, Российский университет дружбы народов имени Патриса Лумумбы, Москва, Российская Федерация, ORCID: https://orcid.org/0000-0001-5987-9310, e-mail: tsetsenbilegts@gmail.com.

Хатанболд Ойдов Сартуул, доктор политических наук (Ph.D.), член-корреспондент Монгольской академии наук, ведущий научный сотрудник, Институт философии Монгольской академии наук, заместитель председателя Подкомиссии по общественным наукам МАС, Улан-Батор, Монголия, ORCID: https://orcid.org/0000-0001-7867-6850, e-mail: khatanboldo@gmail.com

Information about the authors

Tsetsenbileg Tseveen, Candidat of Science (Sociology), Associate Professor, Leading Researcher at the Department of Sociology of the Institute of Philosophy of the Mongolian Academy of Sciences (Ulaanbaatar, Mongolia); Associate Professor at the Institute of Foreign Languages of the P. Lumumba Peoples' Friendship University of Russia (Russia), ORCID: https://orcid.org/0000-0001-5987-9310, e-mail: tsetsenbilegts@gmail.com

Khatanbold Oidov Sartuul, Doctor of Political Sciences (Ph.D.), Corresponding Member of the Mongolian Academy of Sciences, Senior Researcher, Institute of Philosophy of the Mongolian Academy of Sciences, Deputy Chairman of the Subcommittee on Social Sciences of the IAU, Ulaanbaatar, Mongolia, ORCID: https://orcid.org/0000-0001-7867-6850, e-mail: khatanboldo@gmail.com

Вклад авторов

Авторы внесли равный вклад в разработку проблемы и написание статьи и приняли участие в обсуждении результатов, согласовали окончательный текст рукописи.

Contribution of the authors

All the authors made an equal contribution to the development of the problem and the writing of the article, and participated in the discussion of the results, agreed on the final text of the manuscript.

Конфликт интересов
Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest
The authors declare no conflict of interest.

Декларация об этике
Письменное информированное согласие на участие в этом исследовании было предоставлено респондентами и законными представителями респондентов.

Ethics statement
Written informed consent for participation in this study was obtained from the participants and the legal representatives of the respondents.

Поступила в редакцию 17.04.2026
Поступила после рецензирования 17.04.2026
Принята к публикации 29.05.2026
Опубликована 30.06.2026

Received 2026.04.17.
Revised 2026.04.17.
Accepted 2026.05.29.
Published 2026.06.30.