DOI 10.15393/j5.art. 2026.10964
УДК 378:004.056:37.091.12

**ФИЛОНОВА Анна Сергеевна**
кандидат психологических наук, доцент, доцент кафедры рекламы и связей с общественностью в медиаиндустрии
Московский политехнический университет
(г. Москва, Российская Федерация)
*annasf76@mail.ru*

# ИНТЕГРАТИВНАЯ МОДЕЛЬ МЕДИАБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ ВУЗА

**Аннотация**: актуальность исследования обусловлена возрастанием медиарисков в условиях цифровой трансформации образования, когда студенты и преподаватели активно взаимодействуют с цифровыми платформами, социальными сетями и мультимедийным контентом. Недостаточный уровень медиакомпетентности и отсутствие системных мер защиты повышают уязвимость участников образовательного процесса перед дезинформацией, киберугрозами и манипулятивным воздействием медиа. Цель исследования заключается в теоретическом обосновании и разработке интегративной модели медиабезопасности в образовательной среде вуза. Методологическую основу составил междисциплинарный подход, сочетающий идеи медиаобразования, информационной безопасности и педагогической психологии. Использованы методы теоретического анализа отечественных и зарубежных исследований, контент-анализа нормативных документов и концептуального моделирования. Разработана авторская интегративная модель медиабезопасности, включающая четыре взаимосвязанных компонента: образовательный, технический, психологический и организационно-управленческий. Концептуально описан механизм синергетического взаимодействия компонентов модели. Представлены конкретные примеры реализации интегративного подхода в российских и зарубежных университетах. Реализация интегративной модели создает условия для формирования у студентов и преподавателей навыков безопасного медиаповедения, снижения уровня медиарисков и укрепления информационной культуры вуза. Практическая значимость состоит в возможности применения предложенной модели при разработке образовательных программ и университетской политики.

**Ключевые слова:** медиабезопасность, медиаобразование, медиаграмотность, информационная безопасность, высшее образование, интегративный подход, цифровая среда.

**Дата поступления:** 26.09.2025

**Дата публикации:** 26.03.2026

**Для цитирования:** Филонова А. С. Интегративная модель медиабезопасности в образовательной среде вуза // Непрерывное образование: XXI век. 2026. Т. 14. № 1. DOI: 10.15393/j5.art. 2026.10964

**FILONOVA Anna S.**
PhD in Psychology, Associate Professor; Associate Professor, Department of Advertising and Public Relations in the Media Industry
Moscow Polytechnic University
(Moscow, Russian Federation)
*annasf76@mail.ru*

# INTEGRATIVE MODEL OF MEDIA SECURITY IN THE UNIVERSITY EDUCATIONAL ENVIRONMENT

**Abstract:** the relevance of this study is driven by the growing media risks in the context of higher education digital transformation, where students and faculty actively interact with digital platforms, social networks, and multimedia content. Insufficient media competence and the lack of systemic protective measures increase the vulnerability of educational process participants to disinformation, cyber threats, and manipulative media influence. The aim of the research is to theoretically substantiate and develop an integrative model of media security in the university educational environment. The methodological basis is an interdisciplinary approach combining the ideas of media education, information security, and educational psychology. The study employs theoretical analysis of Russian and international research, content analysis of regulatory documents, and conceptual modeling. An original integrative media security model is proposed, comprising four interrelated components: educational, technical, psychological, and organizational-managerial. The mechanism of synergistic interaction between model components is conceptually described. Specific examples of integrative approach implementation in Russian and foreign universities are presented. Implementing the integrative model creates conditions for developing safe media behavior skills among students and faculty, reduces media risks, and strengthens the university's information culture. The practical significance lies in the applicability of the proposed model for developing university educational programs and policies.

**Keywords:** media security, media education, media literacy, information security, higher education, integrative approach, digital environment.

**Received:** September 26, 2025

**Date of publication:** March 26, 2026

**For citation:** Filonova A. S. Integrative model of media security in the university educational environment. *Nepreryvnoe obrazovanie: XXI vek [Lifelong education: the 21st century]*. 2026. Vol. 14. No. 1. DOI: 10.15393/j5.art. 2026.10964

Проблематика медиабезопасности в высшей школе становится все более значимой в связи с глобальной цифровизацией и медиатизацией общества. Современные студенты ежедневно потребляют и создают медиаконтент, используют социальные сети, получают новости преимущественно из интернет-источников. Такая медиасреда предоставляет новые образовательные возможности, но одновременно несет серьезные угрозы: распространение дезинформации и фейковых новостей, интернет-мошенничество, кибербуллинг, манипулятивное воздействие медиатекстов [1; 2]. Даже взрослые пользователи не могут быть абсолютно защищены в цифровой среде, а студенты, по мнению психологов и педагогов, как наиболее активная аудитория оказываются особенно уязвимы.

Понятие «медиабезопасность» возникло на стыке исследований информационной безопасности и медиаобразования в конце XX – начале XXI в. [3; 4].

До сих пор в научном сообществе нет единого определения термина. В широком смысле медиабезопасность рассматривается как часть информационной безопасности общества, связанная с распространением информации через средства массовой коммуникации [5]. В прикладном аспекте медиабезопасность личности охватывает как техническую защиту данных, так и защищенность от деструктивного контента и психологических угроз [6]. Таким образом, медиабезопасность интегрирует вопросы кибербезопасности и медиаграмотности.

Классики медиаисследований подчеркивали глобальный характер влияния медиа. Маршалл Маклюэн предсказывал, что глобализация коммуникаций создаст единое медиапространство – «глобальную деревню» [7]. В этом пространстве качество контента и способность аудитории к его критической интерпретации напрямую влияют на безопасность общества.

Отечественные и зарубежные исследователи последовательно развивают понимание роли медиаобразования в обеспечении безопасности. А. В. Федоров указывает, что главная задача медиаобразования – обучить критическому анализу медиатекста, формировать умение аргументированной оценки информации и самостоятельность суждений [3]. Е. Л. Вартанова и соавторы подчеркивают, что развитие критического мышления и медиакомпетентности является необходимым условием информационной безопасности [8]. Н. Б. Кириллова связывает развитие медиаграмотности с формированием критического мышления и культуры ответственного медиапотребления [9]. И. В. Жилавская рассматривает медиакультуру как условие медиабезопасности общества [4].

Зарубежные исследования медиаграмотности также акцентируют ее роль в обеспечении безопасного поведения в цифровой среде. Соня Ливингстон рассматривает медиаграмотность как способность критически оценивать и безопасно использовать цифровые медиа в условиях растущих онлайн-угроз [1]. Рене Хоббс подчеркивает, что медиаграмотность является ключевым элементом цифровой гражданственности [2]. В аналитической записке Европейского парламента медиаграмотность определяется как «набор знаний и умений, позволяющий эффективно и безопасно использовать медиа» [10].

Однако существующие исследования и практики зачастую носят фрагментарный характер: одни сосредоточены на технических средствах защиты, другие – на медиаобразовании или психологической профилактике. Подобная разрозненность снижает эффективность предпринимаемых действий и не обеспечивает целостной защиты участников образовательного процесса [11; 12]. В этих условиях необходима интегративная модель медиабезопасности, которая позволит объединить различные подходы в единую систему. Именно такой подход становится ключевым условием формирования устойчивой и безопасной медиасреды в вузе, отвечающей вызовам цифровой эпохи [13].

*Цель исследования* состояла в разработке интегративной модели обеспечения медиабезопасности в вузовском образовании на основе объединения образовательных, технических, психологических и организационно-управленческих компонентов.

*Задачи исследования:*

1. Проанализировать существующие подходы к медиабезопасности в отечественной и зарубежной литературе.

2. Выявить и описать ключевые компоненты медиабезопасной образовательной среды вуза.

3. Систематизировать лучшие практики интеграции медиаобразования и информационной безопасности.

4. Разработать авторскую модель интегративного обеспечения медиабезопасности в вузе.

*Методологические основания*. Методологическую основу составил интегративный междисциплинарный подход, сочетающий идеи медиаобразования, медиакомпетентности, информационной и кибербезопасности, а также педагогической психологии. Такой подход позволяет рассматривать медиабезопасность как систему со взаимосвязанными компонентами, обеспечивающими комплексную защиту участников образовательного процесса [1; 3; 8].

В качестве теоретической базы использованы: концепция медиаобразования и медиаграмотности (А. В. Федоров, С. Ливингстон, Р. Хоббс); модели медиакомпетентности, разработанные в отечественной традиции (Н. Б. Кириллова, И. В. Жилавская, Е. Л. Вартанова) и в международных исследованиях [2]; работы в области информационной безопасности и медиарисков в высшей школе [12].

*Методы исследования.* Для решения поставленных задач использовался комплекс методов:

1. Теоретический анализ – изучение научных публикаций по проблемам медиабезопасности, медиаграмотности и медиаобразования [1–4], анализ понятийного аппарата и выявление структурных элементов медиабезопасности.

2. Сравнительно-сопоставительный анализ – сопоставление различных моделей обеспечения медиабезопасности (технический и педагогический подходы), анализ отечественного и зарубежного опыта (программы UNESCO Media and Information Literacy; инициативы Европейского парламента) [10; 14].

3. Контент-анализ нормативных документов – изучение российских и международных актов и стратегий в сфере информационной безопасности и цифровой грамотности (государственная программа «Цифровая экономика РФ», European Parliamentary Research Service).

4. Концептуальное моделирование – построение авторской модели интегративного обеспечения медиабезопасности в вузе, включающей образовательный, технический, психологический и организационный компоненты [13].

5. Экспертное оценивание – использование мнений специалистов в области медиаобразования и информационной безопасности (в форме обсуждений на конференциях и профильных семинарах), что позволило соотнести разработанную модель с практическими потребностями высшей школы.

***Дискуссионные вопросы медиабезопасности в высшем образовании.*** Прежде чем перейти к описанию авторской модели, необходимо обозначить ключевые дискуссионные вопросы, определяющие контекст исследования.

Во-первых, остается открытым вопрос о соотношении технических и образовательных мер. Одни исследователи [12] подчеркивают приоритет институциональной цифровой инфраструктуры, в то время как другие [1; 2] делают акцент на развитии медиаграмотности как основном инструменте профилактики медиарисков. Интегративный подход предполагает синтез этих направлений, однако требует эмпирической проверки степени взаимоусиления образовательных и технических решений.

Во-вторых, необходимо учитывать различия между поколениями участников образовательного процесса. Как показывают исследования [8; 16], студенты и преподаватели демонстрируют неодинаковый уровень цифровых компетенций и восприимчивости к медиарискам. Возникает задача адаптации интегративной модели к разным группам аудитории – «цифровым аборигенам» и «цифровым иммигрантам».

В-третьих, остается дискуссионным вопрос институционализации медиабезопасности: должна ли она входить в образовательные стандарты в качестве обязательной компетенции или ее развитие следует оставлять на усмотрение университетов. Международные практики [10; 14] указывают на необходимость национальных стратегий, но в российском контексте эта тема пока недостаточно развита.

Наконец, важным предметом дискуссии является влияние новых технологических тенденций – генеративного искусственного интеллекта, метаверсов, синтетических медиа, которые радикально изменяют характер медиарисков и требуют постоянного обновления как образовательных программ, так и инструментов защиты.

***Авторская интегративная модель медиабезопасности.*** Теоретический анализ показал, что обеспечение медиабезопасности не может ограничиваться отдельными действиями – техническими фильтрами, разовыми просветительскими лекциями или психологическими консультациями. Эффективность возможна лишь при условии интеграции мер. На основании анализа научных публикаций и изучения практического опыта российских и зарубежных университетов была разработана авторская интегративная модель медиабезопасности в образовательной среде вуза, включающая четыре взаимосвязанных компонента: образовательный, технический, психологический и организационно-управленческий.

Модель представляет собой систему из четырех взаимосвязанных компонентов, где каждый элемент усиливает действие других: образовательный компонент формирует осознанность, повышающую эффективность технических мер; технический компонент обеспечивает инфраструктурную защиту; психологический компонент развивает устойчивость к манипуляциям; организационно-управленческий компонент выполняет интегрирующую функцию, координируя работу остальных элементов.

**Компоненты модели и механизма их взаимодействия**

*Образовательный компонент* является ядром модели и направлен на формирование медиакомпетентности, критического мышления и навыков ответственного медиапотребления у студентов и преподавателей.

Его содержание включает специализированные модули «Медиабезопасность» и «Медиаграмотность» (36–72 часа), интеграцию тематики в профильные дисциплины, а также активные формы обучения – проектные задания по разоблачению фейковых новостей, медиатренинги, анализ кейсов манипулятивного контента. Особое внимание уделяется развитию навыков критического анализа медиатекста: выявлению признаков недостоверной информации, оценке источников и распознаванию манипулятивных приемов.

*Технический компонент* предполагает создание безопасной цифровой инфраструктуры вуза посредством фильтрации интернет-трафика (блокировка вредоносных ресурсов), защиты персональных данных в соответствии с Федеральным законом № 152-ФЗ и регламентом GDPR, использования антивирусного ПО и систем обнаружения вторжений, а также мониторинга сетевой активности. Организационную основу составляют нормативные документы: правила пользования цифровыми сервисами, политика использования социальных сетей и регламент реагирования на инциденты.

Однако зарубежные и российские исследователи подчеркивают, что технические меры без образовательного сопровождения оказываются малоэффективными: молодежь легко находит способы обхода ограничений, если не понимает их цели [11]. Следовательно, образовательный и технический блоки модели должны действовать синхронно.

*Психологический компонент* направлен на развитие устойчивости участников образовательного процесса к манипулятивным воздействиям. Во многих российских вузах в структуре психологических служб наряду с решением традиционных задач (адаптация первокурсников, профилактика стресса, консультирование по личностным проблемам) все большее внимание уделяется вопросам цифрового благополучия: специалисты проводят индивидуальные консультации и групповые тренинги по профилактике интернет-зависимости и кибербуллинга, помогают пострадавшим от онлайн-мошенничества и информационных травм. Исследования показывают, что сочетание образовательных мер с психологической поддержкой существенно повышает устойчивость личности к медиарискам [6]. В вузовской среде психологический компонент особенно важен, поскольку молодые люди в возрасте 17–23 лет наиболее подвержены влиянию агрессивных медиастратегий и эмоционально насыщенного контента.

*Организационно-управленческий компонент* обеспечивает институциональную основу функционирования всей системы медиабезопасности. Он включает разработку нормативной базы (политика использования цифровых сервисов, кодекс цифровой этики, протоколы реагирования на инциденты), систематическое повышение квалификации преподавателей и персонала, создание координационных структур (советов или рабочих групп по медиабезопасности), а также партнерство с государственными органами, экспертными организациями и другими вузами. Важным элементом является включение показателей медиабезопасности в систему мониторинга качества образования.

*Механизм синергетического взаимодействия компонентов.* Принципиальной особенностью предложенной модели является не просто выделение четырех компонентов, а описание механизма их синергетического взаимодействия.

Образовательная работа повышает осознанность пользователей и снижает сопротивление техническим мерам защиты; психологическая подготовка усиливает эффект образовательных программ, формируя эмоциональную устойчивость к манипуляциям; технические системы мониторинга предоставляют данные для актуализации образовательного контента и позволяют психологической службе оперативно реагировать на инциденты. Организационно-управленческий компонент выполняет интегрирующую функцию, обеспечивая координацию подразделений, распределение ресурсов и единые стандарты взаимодействия. Таким образом, предложенная модель направлена на формирование целостной системы (экосистемы) медиабезопасности вуза, в которой согласованная реализация образовательных, технических, психологических и организационно-управленческих мер рассматривается как условие повышения устойчивости образовательной среды к медиарискам. Отдельные исследования и рамочные модели в смежных областях подтверждают целесообразность интеграции мер и управленческой координации (управленческо-синергетические основания согласованности мер см. [16]; возможности и ограничения программ медиаграмотности – [15]), однако предложенная модель носит концептуальный характер и требует эмпирической проверки в конкретных институциональных условиях [12; 13; 15; 16]. В [13] описан комплексный фреймворк обеспечения безопасности систем e-learning. Мы ссылаемся на него как на пример интегративной логики в смежной области, при этом подчеркиваем, что объект и набор компонентов в [13] отличаются от нашей 4-компонентной модели медиабезопасности образовательной среды вуза.

*Практический опыт реализации интегративного подхода.* Анализ деятельности российских и зарубежных университетов подтверждает эффективность комплексных программ медиабезопасности, объединяющих все четыре компонента модели. В сфере образовательного компонента показателен опыт Московского государственного университета им. М. В. Ломоносова, где на факультете журналистики реализуется спецсеминар по медиаграмотности, направленный на формирование навыков верификации информации, распознавания приемов скрытого воздействия на массовое сознание и развитие критического мышления [17]. На международном уровне программа Civic Online Reasoning Стэнфордского университета, интегрированная в образовательные программы различных факультетов, демонстрирует значительное повышение способности студентов выявлять манипулятивный контент[1]. Технический и организационно-управленческий компоненты успешно интегрированы в Уральском федеральном университете, где в 2024 г. совместно с Уральским центром систем безопасности открыта лаборатория кибербезопасности TRINITY, объединяющая тестирование средств защиты информации, обучение студентов на реальных кейсах компаний и партнерство вуза с IT-бизнесом[2]. Психологиче-

[1] Stanford History Education Group. Civic Online Reasoning. URL: https://cor.stanford.edu/ (дата обращения 20.08.2025).

[2] В УрФУ открыли лабораторию кибербезопасности // 66.RU. 2024. 4 сентября. URL: https://66.ru/news/society/268547/ (дата обращения 20.08.2025).

ский компонент активно развивается во многих российских вузах: наряду с традиционными задачами психологические службы все больше внимания уделяют вопросам цифрового благополучия. В частности, в Томском государственном университете в рамках программы «Приоритет 2030» реализуется проект «Человек в цифровом пространстве: самоощущение и профилактика стресса», направленный на исследование феномена «незавершенной адаптации» при переключении между онлайн- и офлайн-форматами обучения и разработку рекомендаций по преодолению цифрового стресса[1]. Опыт системы университетов Калифорнии (UC System, США) демонстрирует эффективность единой институциональной политики кибербезопасности, включающей обязательное ежегодное обучение сотрудников, стандартизированные протоколы реагирования на инциденты и централизованный мониторинг угроз[2]. Таким образом, анализ кейсов и практик реализации отдельных мер в российских и зарубежных университетах показывает перспективность их согласования в рамках единой политики медиабезопасности. Имеются практические рекомендации и положительные примеры взаимодействия отдельных компонентов, указывающие на возможность синергетического эффекта и повышения устойчивости защиты участников образовательного процесса от медиарисков.

Оценка эффективности интегративных программ может проводиться по совокупности показателей: (1) образовательные – результаты входного / итогового тестирования по медиаграмотности и доля обученных; (2) технические – динамика числа инцидентов (фишинг, утечки, заражения), время реагирования; (3) психологические – обращения по поводу кибербуллинга / цифрового стресса и результаты опросников цифрового благополучия; (4) управленческие – наличие регламентов, охват инструктажами, результаты аудита соблюдения политик.

*Сравнение с существующими подходами.* Разработанная интегративная модель базируется на подходе, который существенно отличается от известных стратегий обеспечения медиабезопасности в высшем образовании. *Технократический подход* сосредоточен на технической защите инфраструктуры и обладает преимуществами быстрого внедрения и измеримости результатов, однако не учитывает человеческий фактор, что обусловливает низкую устойчивость и слабую адаптивность к новым угрозам. *Просветительский подход* направлен на развитие медиаграмотности и формирование устойчивых компетенций, но не обеспечивает технической защиты. *Интегративный подход,* положенный в основу предложенной модели, объединяет оба направления в комплексную систему, обеспечивая синергию образовательных, технических, психологических и организационных мер, что обусловливает высокую устойчивость и адаптивность.

Зарубежные авторы подчеркивают важность комплексных программ, охватывающих разные уровни образования [1; 2]. В отечественной науке И. В. Жи-

[1] Проект ТГУ поможет преодолевать стресс в цифровой среде // РИА Томск. 2022. 26 сентября. URL: https://www.riatomsk.ru/article/20220926/tgu-stress-cifrovaya-sreda/ (дата обращения 20.08.2025).
[2] University of California. Information Security Office. URL: https://security.ucop.edu/ (дата обращения 20.08.2025).

лавская рассматривает медиакультуру как условие медиабезопасности общества [4], а Н. Б. Кириллова связывает развитие медиаграмотности с формированием критического мышления и культуры ответственного медиапотребления [9].

В отличие от разрозненных моделей, ориентированных либо на техническую защиту [12], либо на воспитание медиаграмотности [1; 2], представленная модель объединяет все уровни и формирует целостную стратегию. Она соответствует подходу А. В. Федорова, который подчеркивал необходимость соединения критического анализа медиатекстов с защитой личности от деструктивных информационных воздействий [3].

*Практическая значимость модели.* Применение интегративной модели позволяет вузам решать комплекс взаимосвязанных задач: снижать медиариски (дезинформация, кибербуллинг, фишинг), формировать медиакомпетентность студентов и преподавателей, укреплять информационную культуру университета и обеспечивать соответствие государственным и международным требованиям по цифровой безопасности [10; 14].

*Рекомендации по внедрению модели.* Практическое применение интегративной модели медиабезопасности предполагает поэтапную реализацию, учитывающую специфику конкретного вуза и его ресурсные возможности. На диагностическом этапе (1–2 месяца) проводится аудит текущего состояния медиабезопасности по всем четырем компонентам, выявляются сильные стороны и зоны развития, определяются приоритетные направления работы.

Организационная подготовка (2–3 месяца) включает создание координационной структуры (совета или рабочей группы по медиабезопасности), разработку комплексного плана мероприятий и обеспечение необходимых ресурсов. На этапе внедрения (6–12 месяцев) осуществляются включение модулей медиаграмотности в учебные планы, организация программ повышения квалификации преподавателей, разработка внутренних регламентов и интеграция психологической службы в систему медиабезопасности.

Мониторинг и развитие представляет собой непрерывный процесс, предполагающий регулярную оценку эффективности принимаемых мер, актуализацию программ с учетом новых медиаугроз и обмен опытом с другими образовательными организациями.

В исследовании теоретически обоснована и разработана интегративная модель медиабезопасности в образовательной среде вуза. Показано, что односторонние решения – исключительно технические фильтры или отдельные просветительские инициативы – не обеспечивают устойчивой защиты студентов и преподавателей от медиарисков. Эффективность возможна только при объединении образовательных, технических, психологических и организационно-управленческих мер в единую систему.

Предложенная модель медиабезопасности включает четыре взаимосвязанных компонента: образовательный (формирование медиаграмотности и критического мышления), технический (создание безопасной цифровой инфраструктуры), психологический (развитие устойчивости к манипуляциям и поддержка участников образовательного процесса) и организационно-управленческий

(кадровая подготовка, регламенты и институциональная политика). Анализ практического опыта подтвердил эффективность интегративного подхода.

*Теоретическая новизна исследования* заключается в следующем: медиабезопасность рассмотрена не как прикладная техническая или частная педагогическая задача, а как комплексная педагогическая категория, синтезирующая достижения медиаобразования, теории информационной безопасности, педагогической психологии и менеджмента в образовании.

*Методологическая новизна*: разработан и применен интегративный междисциплинарный подход, который, в отличие от существующих изолированных подходов (технократического, просветительского), обеспечивает системное видение проблемы за счет установления синергетических связей между компонентами модели.

*Концептуальная новизна:* не сводится к утверждению о первичности идеи синергии как таковой (системно-синергетические основания управления медиабезопасностью представлены в [16]), а заключается в разработке для вуза компонентной структуры (4 компонента) и конкретных межкомпонентных связей, описывающих, какие именно действия / данные / решения в одном компоненте запускают изменения в другом. В части образовательного компонента учтены выводы о возможностях и ограничениях программ по повышению медиаграмотности в [15].

*Практико-ориентированная новизна:* определены конкретные механизмы имплементации модели в образовательный процесс университета (модули в учебные планы, регламенты, создание координационных советов, алгоритм внедрения), что переводит модель из области теоретического обсуждения в плоскость практического применения. Представленные механизмы соотносятся с практиками ведущих российских и зарубежных университетов и иллюстрируются примерами внедрения отдельных элементов интегративного подхода.

*Практическая значимость исследования* выражается в возможности применения разработанной модели при проектировании образовательных программ, создании внутренних регламентов и политики университетов. Рекомендации могут быть использованы администрацией вузов, преподавателями и специалистами в области образовательных технологий для снижения медиарисков и развития медиакомпетентности обучающихся.

Перспективы дальнейших исследований связаны с эмпирической проверкой эффективности интегративной модели в различных институциональных контекстах. Представляется целесообразным проведение педагогических экспериментов, позволяющих оценить влияние комплексных программ медиабезопасности на уровень медиаграмотности студентов, частоту инцидентов дезинформации и кибербуллинга. Важным направлением является сравнительный анализ подходов к медиабезопасности в разных странах, что позволит выявить универсальные элементы модели и адаптировать ее к специфике национальных образовательных систем. Дополнительное внимание должно быть уделено влиянию новых технологий – генеративного искусственного интеллекта, метаверсов, синтетических медиа, что требует постоянного обновления модели.

Внедрение интегративной модели медиабезопасности в практику высшей школы будет способствовать не только защите студентов и преподавателей от медиаугроз, но и формированию критически мыслящей, информационно грамотной личности, готовой к ответственному участию в цифровом обществе.

**Список литературы**


1. Livingstone S. Developing social media literacy: How children learn to interpret risky opportunities on social network sites // Communications. 2014. Vol. 39. No. 3. P. 283–303. DOI: 10.1515/commun-2014-0113
2. Hobbs R. Create to learn: Introduction to digital literacy. New York, 2017. 288 p.
3. Федоров А. В. Медиаобразование: история, теория и методика. Москва, 2015. 450 с.
4. Жилавская И. В. О современной концепции медиаобразования // Социально-гуманитарные знания. 2012. № 6. С. 181–193.
5. Богатырев К. М. Угрозы медиабезопасности в цифровой среде: систематизация и анализ // Актуальные проблемы российского права. 2022. Т. 17. № 7. С. 136–142. DOI: 10.17803/1994-1471.2022.140.7.136-142
6. Ulven J. B., Wangen G. A systematic review of cybersecurity risks in higher education // Future Internet. 2021. Vol. 13. No. 2. P. 39. DOI: 10.3390/fi13020039
7. McLuhan M. Understanding media: The extensions of man. London, 2003. 392 p.
8. Вартанова Е. Л., Вихрова Е. В., Самородова М. А. Медиаграмотность как условие преодоления цифрового неравенства [Электронный ресурс] // Медиаскоп. 2021. Вып. 1. Электрон. дан. URL: https://www.mediascope.ru/2679 (дата обращения 20.08.2025).
9. Кириллова Н. Б. Медиакультура: от модерна к постмодерну. 2-е изд., перераб. и доп. Москва, 2005. 448 с.
10. European Parliamentary Research Service. Media literacy: Fostering a key civic skill. Brussels, 2025. 45 p.
11. Мальцева Н. Н., Новак М. В. Медиаграмотность, безопасность и социализация личности в цифровом пространстве: обзор отечественной и зарубежной аналитики // Научный результат. Социальные и гуманитарные исследования. 2023. Т. 9. № 1. С. 207–212. DOI: 10.18413/2408-932X-2023-9-1-0-17
12. Information security at higher education institutions: A systematic literature review / D. Imbaquingo-Esparza, J. Díaz, M. Ron Egas [et al.] // Information and Communication Technologies – TICEC 2022 / J. Herrera-Tapia, G. Rodríguez-Morales, C. F. Fonseca [et al.]. Cham, 2022. P. 294–309. DOI: 10.1007/978-3-031-18272-3_20
13. AlKalbani H. R., Al-Busaidi K. A. An integrated framework for the security of e-learning systems in higher education institutions // Education and Information Technologies. 2025. Advance online publication. DOI: 10.1007/s10639-025-13634-1
14. UNESCO. Media and information literacy curriculum for educators and learners. Paris, 2021. 200 p. [Электронный ресурс] Электрон. дан. URL: https://unesdoc.unesco.org/ark:/48223/pf0000377062 (дата обращения 15.08.2025).
15. Bulger M., Davison P. The promises, challenges, and futures of media literacy // Journal of Media Literacy Education. 2018. Vol. 10. No. 1. P. 1–21. DOI: 10.23860/JMLE-2018-10-1-1
16. Пищова А. В. Управление медиабезопасностью субъектов образовательного процесса: системно-синергетический подход // Университетский педагогический журнал. 2022. № 2. С. 11–17.
17. Владимирова М. Б. Формирование навыков медиаграмотности у студентов факультета журналистики МГУ // Журналистика в 2016 году: творчество, профессия, индустрия: сборник материалов международной научно-практической конференции. Москва, 2017. Т. 1. С. 449–450.

## References


1. Livingstone S. Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications*. 2014. Vol. 39. No. 3. P. 283–303. DOI: 10.1515/commun-2014-0113

2. Hobbs R. Create to learn: Introduction to digital literacy. Hoboken; New York, 2017. 288 p.

3. Fedorov A. V. Media education: History, theory and methodology. Moscow, 2015. 450 p. (In Russ.)

4. Zhilavskaya I. V. On the modern concept of media education. *Sotsial'no-gumanitarnye znaniya [Social and Humanitarian Knowledge]*. 2012. No. 6. P. 181–193. (In Russ.)

5. Bogatyrev K. M. Threats to media security in the digital environment: Systematization and analysis. *Aktual'nye problemy rossiyskogo prava [Actual Problems of Russian Law]*. 2022. Vol. 17. No. 7. P. 136–142. DOI: 10.17803/1994-1471.2022.140.7.136-142 (In Russ.)

6. Ulven J. B., Wangen G. A systematic review of cybersecurity risks in higher education. *Future Internet.* 2021. Vol. 13. No. 2. P. 39. DOI: 10.3390/fi13020039

7. McLuhan M. Understanding media: The extensions of man. London, 2003. 392 p.

8. Vartanova E. L., Vikhrova E. V., Samorodova M. A. Media literacy as a condition for overcoming digital inequality [Electronic resource]. *Mediaskop [Mediascope]*. 2021. No. 1. Electron. dan. URL: https://www.mediascope.ru/2679 (date of access: 20.08.2025). (In Russ.)

9. Kirillova N. B. Media culture: From modernity to postmodernity. Moscow, 2005. 448 p. (In Russ.)

10. European Parliamentary Research Service. Media literacy: Fostering a key civic skill. Brussels, 2025. 45 p.

11. Mal'tseva N. N., Novak M. V. Media literacy, security, and personal socialization in the digital space: A review of domestic and foreign analytics. *Nauchnyy rezul'tat. Sotsial'nye i gumanitarnye issledovaniya [Research Result. Social Studies and Humanities]*. 2023. Vol. 9. No. 1. P. 207–212. DOI: 10.18413/2408-932X-2023-9-1-0-17 (In Russ.)

12. Imbaquingo-Esparza D., Díaz J., Ron Egas M [et al.]. Information security at higher education institutions: A systematic literature review. *Information and Communication Technologies – TICEC 2022* / J. Herrera-Tapia, G. Rodríguez-Morales, C. F. Fonseca [et al.]. S. Berrezueta-Guzmán (Eds.). Cham, 2022. P. 294–309. DOI: 10.1007/978-3-031-18272-3_20

13. AlKalbani H. R., Al-Busaidi K. A. An integrated framework for the security of e-learning systems in higher education institutions. *Education and Information Technologies*. 2025. Advance online publication. DOI: 10.1007/s10639-025-13634-1

14. UNESCO. Media and information literacy curriculum for educators and learners. Paris, 2021. 200 p. [Electronic resource]. Electron. dan. URL: https://unesdoc.unesco.org/ark:/48223/pf0000377062 (date of access: 15.08.2025).

15. Bulger M., Davison P. The promises, challenges, and futures of media literacy. *Journal of Media Literacy Education.* 2018. Vol. 10. No. 1. P. 1–21. DOI: 10.23860/JMLE-2018-10-1-1

16. Pishchova A. V. Media security management of educational process participants: A system-synergetic approach. *Universitetskiy pedagogicheskiy zhurnal [University Pedagogical Journal]*. 2022. No. 2. P. 11–17. (In Russ.)

17. Vladimirova M. B. Formation of media literacy skills among students of the Faculty of Journalism of Moscow State University. *Zhurnalistika v 2016 godu: tvorchestvo, professiya, industriya: sbornik materialov mezhdunarodnoy nauchno-prakticheskoy konferentsii [Journalism in 2016: Creativity, Profession, Industry: Proceedings of the International Scientific and Practical Conference]*. Moscow, 2017. Vol. 1. P. 449–450. (In Russ.)