Целищева Зухра Абдурашидовна
канд. культурологии, доцент
Молочкова Анастасия Владимировна
студентка

ФГБОУ ВО «Нижневартовский государственный университет»
г. Нижневартовск, ХМАО – Югра АО

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЦИФРОВОЙ ГРАМОТНОСТИ МОЛОДЕЖИ

Аннотация: *в статье рассматриваются теоретические основы цифровой грамотности молодежи как ключевой компетенции современного информационного общества. Анализируются подходы к определению понятия «цифровая грамотность», ее структурные компоненты и содержание. Выявляются основные риски, связанные с низким уровнем цифровой грамотности молодежи. Характеризуются методы формирования цифровых компетенций, включая технические меры защиты, образовательные программы и формирование культуры безопасного поведения в сети. Особое внимание уделяется нормативно-правовому регулированию кибербезопасности в Российской Федерации.*

Ключевые слова: *цифровая грамотность, молодежь, кибербезопасность, методы формирования, нормативно-правовое регулирование, цифровые компетенции, киберугрозы.*

С развитием цифровых технологий и ростом их влияния на повседневную жизнь вопросы цифровой грамотности приобретают все большую актуальность. Как отмечают исследователи, цифровая грамотность признана жизненно важным навыком на современном этапе эволюционного развития информационного общества [3, с. 4]. Одним из ключевых аспектов успешной социализации молодежи является формирование цифровой грамотности – совокупности знаний, умений и установок, позволяющих эффективно, безопасно и критически взаи-

модействовать с цифровой средой, использовать ее возможности для образования, коммуникации и самореализации [2, с. 20].

Понятие и структура цифровой грамотности. Впервые определение понятия «цифровая грамотность» было предложено П. Гилстером в 1997 г., который трактовал его как способность понимать и использовать информацию, полученную из цифровых источников посредством компьютеров. В современной научной литературе под цифровой грамотностью понимается базовая компетенция человека, включающая умения и навыки получения, оценки, обработки и производства информации с помощью цифровых технологий, выбор программно-технических средств для решения задач, их безопасное использование, а также эффективное взаимодействие с другими пользователями в цифровой среде с соблюдением этических норм [4, с. 42].

Цифровая грамотность включает технические, когнитивные, коммуникативные и правовые компоненты, что особенно важно для такой уязвимой и активно включенной в цифровую среду группы, как молодежь. Как показывают научные публикации, неограниченное информационное потребление и использование цифровых устройств детьми и молодежью могут сопровождаться как позитивными, так и негативными эффектами [4]. К числу основных рисков относятся: трудности с распознаванием недостоверной информации, уязвимость к манипуляциям, пренебрежение правилами кибергигиены, недостаток знаний о защите персональных данных и правовых последствиях онлайн-действий.

Низкий уровень цифровой грамотности проявляется в неумении критически оценивать информацию, уязвимости перед фишинговыми атаками, сложностях с безопасным общением в социальных сетях и недостаточных навыках защиты личных данных. Некритичное восприятие информации способствует распространению ложных сведений и вовлечению в деструктивные группы. Отсутствие навыков безопасного онлайн-общения может привести к участию в кибербуллинге или превращению в его жертву, а незнание основ защиты данных увеличивает риск мошенничества и утечки конфиденциальной информации.

Нормативно-правовое регулирование кибербезопасности. Кибербезопасность в Российской Федерации регулируется комплексом федеральных законов. В сфере общих принципов информационной безопасности действуют: Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации», определяющий базовые понятия и регулирующий распространение информации; Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры», охватывающий защиту систем в ключевых отраслях экономики. В области защиты персональных данных ключевым является Федеральный закон №152-ФЗ «О персональных данных», обязывающий получать согласие на обработку данных и требующий их хранения на серверах на территории РФ. С 2025 года ужесточена ответственность за нарушения в этой сфере: штрафы за утечки данных достигают 15 млн рублей.

Методы формирования цифровой грамотности. Формирование цифровой грамотности включает комплекс методов, направленных на защиту пользователей от различных угроз. Одним из эффективных способов повышения безопасности является двухфакторная аутентификация (2FA) – использование сторонних приложений для проверки подлинности, требующих ввода кодов, генерируемых в реальном времени. Методы сетевой безопасности включают технические, правовые и образовательные меры [1].

Для обеспечения конфиденциальности крайне важно использовать уникальные, надежные пароли для каждого сервиса и своевременно их менять. Регулярное обновление программного обеспечения помогает закрыть уязвимости, которые могут быть использованы для взлома. При использовании социальных сетей необходимо осознавать, что даже установленные настройки конфиденциальности не гарантируют полной безопасности, что делает актуальным осторожное выстраивание цифровой репутации. Контроль над личной информацией является важным шагом к повышению безопасности в сети.

Важным аспектом формирования цифровой грамотности является внедрение в учебные программы курсов и лекций, направленных на обучение безопасному поведению в интернете. Учебные программы охватывают такие аспекты,

как безопасность Wi-Fi и мобильных устройств, риски использования анонимизаторов и прокси-серверов, методы предотвращения утечек информации. Курсы включают различные форматы материалов: от видеоуроков до тестов для проверки усвоения знаний. Образовательные программы предусматривают проведение практических тренингов, сфокусированных на выработке навыков противодействия фишинговым атакам и понимании актуальных киберугроз. Интеграция интерактивных форматов (тестовые задания, викторины) стимулирует более эффективное усвоение информации и вовлекает обучающихся в активное взаимодействие с учебным контентом [5].

Формирование цифровой грамотности требует комплексного подхода, включающего разработку и внедрение системных образовательных программ на всех уровнях обучения, использование современных методов обучения, а также постоянный мониторинг и анализ уровня цифровых компетенций для выявления пробелов и корректировки образовательных стратегий. Важным элементом является повышение цифровой грамотности родителей и педагогов, обучение их распознаванию признаков низкой цифровой компетентности у молодежи, безопасному поведению в социальных сетях и ответственному использованию личной информации.

Безопасность в интернете представляет собой не только совокупность технических мер, но и культуру безопасного поведения, которая должна быть сформирована у каждого пользователя. Соблюдение конфиденциальности требует комплексного подхода, включающего использование технологий, осознанное поведение пользователей и активное сотрудничество с интернет-платформами. Развитие осведомленности о методах защиты позволяет своевременно реагировать на возможные угрозы и защищать как персональные данные, так и цифровую репутацию. Обучение безопасному поведению становится основой для формирования системы онлайн-безопасности и защиты личных данных, что является одной из приоритетных задач в условиях активного роста киберугроз и цифровой трансформации общества.

Список литературы

1. Актуальные вопросы обеспечения комплексной безопасности: материалы национальной научно-практической конференции / под ред. А.Д. Тарасова. – Оренбург: Оренбургский ГАУ, 2024. – 1343 с. – URL: https://elibrary.ru/item.asp?id=69211663 (дата обращения: 13.04.2026).

2. Алексеева Е.А. Сущность и содержание понятия цифровая грамотность в современных педагогических исследованиях / Е.А. Алексеева, Г.И. Алексеева // Научно-методический электронный журнал «Концепт». – 2025. – №11. – С. 20-32. – URL: https://cyberleninka.ru/article/n/suschnost-i-soderzhanie-ponyatiya-tsifrovaya-gramotnost-v-sovremennyh-pedagogicheskih-issledovaniyah (дата обращения: 13.04.2026). DOI 10.24412/2304-120X-2025-11212. EDN EEVJNE

3. Бороненко Т.А. Концептуальная модель понятия цифровой грамотности / Т.А. Бороненко, А.В. Кайсина, В.С. Федотова // Проблемы и непрерывное образование. – 2020. – №4(46). – URL: https://cyberleninka.ru/article/n/kontseptualnaya-model-ponyatiya-tsifrovoy-gramotnosti (дата обращения: 13.04.2026).

4. Система информационной безопасности и цифровой грамотности в России и регионах: истоки, состояние, перспективы // Zenodo. – 2025. – URL: https://www.viepp.ru/nauchnaya-statya-sistema-informacionnoj-bezopasnosti-i-cifrovoj-gramotnosti-v-rossii-i-regionax-istoki-sostoyanie-perspektivy/ (дата обращения: 13.04.2026).

5. Киберугрозы в образовательных учреждениях: защита данных студентов и преподавателей / Н. Эркаева, А. Нурыллаев, М. Ораздурдыева, А. Оденепесова // Наука и мировоззрение. – 2025. – №38. – URL: https://cyberleninka.ru/article/n/kiberugrozy-v-obrazovatelnyh-uchrezhdeniyah-zaschita-dannyh-studentov-i-prepodavateley (дата обращения: 13.04.2026).