

DATA SCIENCE В УПРАВЛЕНИИ ОБРАЗОВАТЕЛЬНЫМ ПРОСТРАНСТВОМ

Направления деятельности педагога по формированию информационной безопасности старшекласников

Владислав Андреевич Евтехов

Аспирант

Брянский государственный университет им. И.Г. Петровского

Брянск, Россия

Vvlad.evtexR@yandex.ru

ORCID 0000-0000-0000-0000

Поступила в редакцию 07.06.2024

Принята 29.07.2024

Опубликована 30.08.2024

УДК 37.016:004.8

DOI 10.25726/k8856-4636-9365-e

EDN CQKCFC

БАК 5.8.2. Теория и методика обучения и воспитания (по областям и уровням образования) (педагогические науки)

OECD 05.03.HB. EDUCATION, SCIENTIFIC DISCIPLINES

Аннотация

Современная жизнь общества во многом предопределена масштабным влиянием телекоммуникационных и информационных технологий, без которых трудно вообразить любую сферу деятельности человека. Принимая во внимание интенсивное внедрение компьютерных ресурсов в административные процессы, необходимо подчеркнуть, что люди начинают работать с персональными устройствами с самого раннего возраста. «Всемирная паутина» привнесла кардинальные перемены во множество областей, раскрываясь в качестве технологического, экономического и социокультурного феномена. Однако, помимо очевидных преимуществ, столь стремительный прогресс обострил целый ряд проблем, среди которых наибольшую значимость приобретает безопасность киберпространства (она же информационная безопасность). Кроме того, на сегодняшний день сетевые компьютерные игры переросли в один из ключевых видов досуга для молодежной аудитории. В контексте данных обстоятельств исключительно важным представляется достижение полноформатной информационной безопасности, что подразумевает поддержание стабильной работы компьютеров и ресурсов информационного типа. Именно поэтому Российская Федерация считает обеспечение защиты информации одной из приоритетных задач госуправления в сфере национальной безопасности, что в итоге определяет предмет данной научной работы.

Ключевые слова

интерактивные технологии, военные специальности, военные профессии, цифровизация, военное образование, профориентация, кибербезопасность, информационная безопасность, информационные технологии.

Введение

В настоящее время в России и других государствах планеты не угасает ряд опасностей, исходящих от возможных военных действий, особенно если речь идет о конфликтах с использованием химических, биологических или ядерных вооружений (Ведерникова, 2022). По мнению И.А. Михальченко

и А.И. Позднякова, актуальность задачи информационной безопасности существенно возрастает в связи с феноменом информационных войн.

События последних лет, затрагивающие Украину и Сирию, формируют осознание непрерывной угрозы национальной безопасности любого государства, включая Российскую Федерацию. В этих условиях исключительно важно, помимо всего прочего, обеспечить высокий уровень информационной безопасности (Кузьмина, 2021).

Генезис научного направления «информационная безопасность и защита информации» в отечественной научной школе ассоциируется с именами таких исследователей, как В.А. Герасименко, А.А. Малюк, М.Б. Игнатьев, В.А. Минаев, П.Д. Зегжда и др. Организация безопасного образовательного процесса поднималась в трудах Б.С. Гершунского, В.П. Казначеева, Д.А. Новикова и ряда других авторов.

В настоящее время образовательные учреждения активно оснащаются компьютерной техникой. Отражение воздействия вычислительных систем на образовательные практики встречается в исследованиях А.Г. Гейна, А.П. Ершова, В.Н. Каптелинина, А.А. Кузнецова (Жихарева, 2022), И.В. Роберт. В последние годы возрастает интерес к всестороннему анализу влияния Интернета на психику и поведенческие особенности обучающихся, о чем свидетельствуют выводы А.А. Веряева (Оленников, 2020). Проблематику информатизации образовательной сферы подвергли изучению Л.В. Астахов, Л.Л. Ефимов, Ю.Г. Коротенков, В.Ф. Пилпенко, В.В. Хорошов, М.И. Бочаров.

При этом заслуживает признания факт, что использование сети Интернет в образовательном сегменте, несмотря на имеющиеся риски, расширяет возможности и обеспечивает оперативное решение множества дидактических задач. К подобному выводу приходят многие авторы, в том числе А.Г. Асмолов, Б.Б. Вендровская, М.Б. Иг

Материалы и методы исследования

Являясь частью системной защиты данных, кибербезопасность сосредоточена на комплексном контроле конфиденциальных сведений. Информационная безопасность, в свою очередь, охватывает всестороннюю защиту информации как таковой (Кузьмина, 2021).

Первоначально термин «информация» берет свое начало в латинском слове *informatio* – разъяснение. Научное применение этого понятия относительно недавно стало охватывать весь спектр речевых и коммуникативных данных (Абдулгамидов, 2022). Так, Г.В. Грачев утверждает, что безопасность информации для отдельного человека предполагает должный уровень охраны его интересов в информационном поле, обеспечивая сохранность личности как социокультурного субъекта. В этом же ключе Н.И. Саттарова отмечает: реализация безопасности частного индивида означает практическую защиту его базовых интересов, включая комплекс конституционных прав и правомерное обеспечение личной безопасности. В дополнение к этому, решающее значение приобретает сохранение возможностей интеллектуального и физического развития, а также предохранение сознания от пагубных информационных воздействий (Зорина, 2022).

Расширяя данный подход применительно к образовательной среде, Т.А. Малых подчеркивает, что информационная безопасность учащихся определяется как состояние гарантированной защищенности их жизненно важных интересов. Оно выражается в способности своевременно фиксировать потенциальные угрозы и компенсировать отрицательные последствия деструктивной информации (Солдатова, 2022).

По смыслу новейшего проекта Концепции стратегии кибербезопасности РФ термин «киберпространство» охватывает деятельность в рамках всего информационного пространства, включающего сеть Интернет, а также иные телекоммуникационные сети и форматы, опосредованные деятельностью человека.

Исследователь Б.Д. Слабнин, со своей стороны, предлагает толковать кибербезопасность через совокупность условий, при которых любой элемент киберпространства может стать источником прямой угрозы (Слабнин, 2018). В то же время, по мысли А.С. Алпеева, обеспечение кибербезопасности предполагает создание комплекса защитных мер против «физических, моральных, эмоциональных, психологических воздействий, а также вероятных ошибок или иных инцидентов в киберпространстве»

(Жихарева, 2022). Параллельно этому, в русско-американском словаре указано, что «кибербезопасность» в информационной сфере характеризуется способностью киберпространства противостоять угрозам, нейтрализовать их и восстанавливаться после негативных влияний (Белов, 2022).

Таким образом, кибербезопасность выступает одной из ключевых подсистем комплексной информационной безопасности. В ее рамках не только исследуются нюансы функционирования отдельных киберобъектов и специальные аспекты правовой документации, но и внедряются механизмы правовой защиты от потенциальных источников угроз (Прудникова, 2022).

Результаты и обсуждение

Анализируя основные направления деятельности педагога по формированию информационной безопасности старшеклассников, следует более детально рассмотреть некоторые ключевые аспекты данной проблематики.

Концепция информационной безопасности детей акцентирует внимание на том, что усилия семьи, всего общества и государственных структур должны быть направлены на формирование у ребенка с ранних лет навыков самостоятельного и уверенного ориентирования в медиасреде, умения анализировать многочисленные источники информации, противостоять внешнему давлению и вырабатывать собственную оценку качества получаемых сведений (Расина, 2021).

Вместе с тем, необходимо отметить наличие ряда сложностей в данном контексте, включая физиологические изменения в головном мозге у детей, испытывающих зависимость от компьютеров, ослабление познавательных процессов, ухудшение памяти и концентрации внимания, снижение критической оценки происходящего, ограничение сферы сознания (Савин, 2023). Эти негативные факторы требуют особого внимания при разработке программ информационной безопасности для школьников.

При определении направлений работы педагога в данной сфере целесообразно опираться на положения «Концепции стратегии кибербезопасности РФ». Согласно этому документу, в ближайшей перспективе рекомендуется интегрировать в образовательную программу специальный модуль, посвященный информационной и кибербезопасности, нацеленный на формирование у детей норм безопасного поведения в цифровом пространстве (Белов, 2022).

Для достижения этой цели необходимо решение следующих задач:

1. Введение ключевых понятий в области кибербезопасности и предоставление детальных инструкций, регламентирующих правила поведения в киберпространстве.
2. Развитие у школьников практической способности действовать в информационной среде применительно к различным прикладным задачам.
3. Формирование у учащихся навыков реагирования при возникновении киберугроз посредством интерактивных игровых методик и тренажеров.
4. Создание кибербезопасной домашней обстановки при активном участии родителей, в том числе через специальные учебно-методические пособия (Расина, 2021).

В современных российских школах накоплен существенный опыт преподавания информационных технологий. При этом значимым представляется развитие у учащихся таких умений, как эффективный поиск данных в многообразии источников, конвертация визуальной информации в текстовую форму, трансформация данных с учетом особенностей коммуникации, оценка информационных сообщений, выявление неточностей и выделение ключевых идей (Мансуров, 2022).

Обучение основам кибербезопасности является одной из наиболее актуальных проблем для педагогического сообщества. Важно учитывать, что значительную часть времени дети проводят в учебном заведении, где специалисты могут предоставить им как теоретические знания по информационной безопасности, так и отработку практических действий (Оленников, 2020).

На сегодняшний день отсутствует полноценная классификация угроз кибербезопасности детей, в том числе по источникам возникновения. В обобщенном виде можно выделить четыре основные

группы таких источников: государственные структуры, социальные объединения, отдельные индивиды и различные социальные группы (Савин, 2023).

Сохраняется серьезная угроза для учащихся начальных классов, исходящая от массовых информационных каналов. СМИ могут оказывать негативное воздействие на детей, особенно при регулярном повторении отрицательных сведений. Телевидение, являясь одним из видов опосредованной коммуникации, влияет на личностное формирование ребенка с самых ранних этапов жизни.

Для преодоления данной проблемы необходимы меры по укреплению нормативно-правовой базы, регулирующей функционирование СМИ с целью защиты детей от деструктивной информации, созданию специальных циклов занятий по кибербезопасности для младших школьников, а также поощрению развития у них навыков критического мышления.

Ситуация усложняется тем, что ребенок требует не просто разового ознакомления с основами кибербезопасности, а комплексной системы знаний, позволяющей ответственно действовать в долгосрочной перспективе. Существенную помощь здесь может оказать педагог, знакомящий детей как с теоретическими аспектами, так и с практическими алгоритмами поведения в цифровой среде.

Следует отметить, что проблематика компьютерной безопасности образовательной среды давно затронута в трудах отечественных ученых, таких как Б.С. Гершунский, В.П. Казначеев, Д.А. Новиков и др. Интернет-технологии открывают широкие возможности для решения дидактических задач, на что указывают работы А.Г. Асмолова, Б.Б. Вендровской, М.Б. Игнатьева, С.Н. Позднякова и др. Современные тенденции информатизации образования освещены в публикациях Л.В. Астахова, Л.Л. Ефимова, Ю.Г. Коротенкова, В.Ф. Пилпенко, В.В. Хорошова, М.И. Бочарова.

Обеспечение безопасной информационной среды для современных школьников требует комплексного подхода, охватывающего как инфраструктурные и технологические решения, так и развитие у учащихся критического мышления, медиаграмотности и навыков самозащиты от деструктивного контента. Здесь важно подчеркнуть, что ответственность за формирование устойчивых механизмов информационной безопасности должна распределяться между всеми ключевыми субъектами образовательного процесса - педагогами, родителями, администрацией школ и профильными государственными органами.

По данным опроса ВЦИОМ, проведенного в ноябре 2023 года, 78% российских родителей обеспокоены потенциальными угрозами, с которыми их дети могут столкнуться в интернете. При этом 43% опрошенных признали, что не обладают достаточными знаниями и компетенциями для эффективного контроля онлайн-активности своих детей (ВЦИОМ, 2023). Это свидетельствует о насущной необходимости усиления роли школы и педагогов в просвещении и практическом содействии семьям в вопросах детской кибербезопасности. Одним из перспективных направлений представляется интеграция тематики информационной безопасности в базовые образовательные программы по таким предметам, как информатика, обществознание, ОБЖ. Причем речь должна идти не просто о теоретическом ознакомлении с проблематикой, а о выработке у школьников конкретных умений и навыков - от базовых правил сетевой гигиены до продвинутых техник верификации интернет-источников и противодействия социальной инженерии. Особое внимание следует уделить практико-ориентированным формам обучения - ролевым играм, кейсам, симуляторам, позволяющим в интерактивном ключе отрабатывать модели безопасного поведения в цифровой среде.

Не менее важным представляется налаживание эффективной коммуникации с родителями учеников по вопросам информационной безопасности. Помимо регулярного информирования о возникающих угрозах и способах защиты, школа могла бы инициировать проведение специальных семинаров, мастер-классов, на которых родители вместе с детьми осваивали бы базовые приемы цифровой самозащиты. Продуктивным форматом могут стать совместные детско-родительские медиапроекты (например, разработка памяток по безопасности, съемка просветительских роликов и т.п.), нацеленные на укрепление внутрисемейного диалога по данной проблематике.

Отдельного упоминания заслуживает задача формирования у старшеклассников ответственной гражданской позиции как пользователей цифровых медиа. В условиях нарастающей фрагментации и

поляризации глобального интернет-пространства принципиально важно, чтобы подрастающее поколение овладевало навыками осознанного цифрового потребления, умело противостояло манипулятивным технологиям, дезинформации и языку вражды. Культивирование сетевой этики, уважительной коммуникации, неприятия киберагрессии должно стать неотъемлемой частью школьного медиаобразования.

Значимую роль в повышении информационной безопасности учащихся призвана сыграть целенаправленная профилактика интернет-зависимости. По экспертным оценкам, в 2023 году каждый пятый российский старшеклассник был подвержен той или иной форме нездоровой увлеченности интернетом, причем в группу риска входили преимущественно подростки из неблагополучных семей и имеющие проблемы с успеваемостью (Солдатова и др., 2023). Предупреждение развития аддиктивных форм онлайн-поведения требует тесной кооперации педагогов, психологов, социальных работников. Ключевыми направлениями профилактики могут стать: регулярная психодиагностика, индивидуальное консультирование, тренинги личностного роста, вовлечение подростков в офлайн-активности (спорт, творчество, волонтерство).

Естественно, реализация комплексной стратегии обеспечения информационной безопасности школьников невозможна без опоры на прочную нормативно-правовую базу и институциональную поддержку. В последние годы в России предприняты важные шаги в этом направлении - в частности, приняты законы "О защите детей от информации, причиняющей вред их здоровью и развитию", "О безопасности критической информационной инфраструктуры РФ", утверждена Концепция информационной безопасности детей. Вместе с тем, многие эксперты указывают на необходимость дальнейшего совершенствования правовых механизмов, особенно в части регулирования ответственности интернет-платформ, борьбы с негативным контентом, усиления медиаграмотности населения (Солдатова, 2022).

Заключение

Анализ существующей сейчас психолого-педагогической литературы позволяет установить наиболее важные факторы развития личности учащихся старших классов школы (Солдатова, 2022).

Во-первых, важна реализация системы «ребенок – учитель», которая оказывает свое влияние на отношения между детьми и родителями, между школьниками, на отношение ребенка к самому себе. Следует отметить при этом, что для школьников младших классов является значимым авторитет педагога. Во-вторых, сейчас главный вид деятельности учащихся начальных классов школы – это учебная деятельность. Поэтому формирование кибербезопасности необходимо организовать в рамках обучения (Юдаева, 2022). В-третьих, у детей постепенно формируются основы нравственного поведения. Является целесообразным сформировать основы кибербезопасности, применяя для этой цели категории моральных норм и ценностей. В числе прочего важно активизировать внутренние силы детей по самосовершенствованию. У учащихся старших классов школы обеспечивается достаточная мыслительная пластичность. На практике всегда возможно ее качественное изменение в процессе значимой для учащегося учебно-познавательной деятельности. При этом ее структура должна давать возможность органично включать в нее управляемый педагогический процесс развития у учащихся школы знаний по кибербезопасности. Кроме того, необходимо понимать, какой ущерб является вероятным, и обеспечить от него надежную защиту. Помимо этого, важно обеспечение профилактики разрушения самооценки детей, а также профилактика дезориентации в окружающем, утраты самоидентичности. Необходимо предотвращать появление психической зависимости от иных субъектов и т.д. (Слабнин, 2018). В-пятых, весьма важно и то, чтобы учитель был абсолютно уверен, что он представляет собой субъект защиты личности ребенка в ходе его обучения, опережая при этом действия, проявляемые со стороны общества, а также государства (Чучалова, 2021).

Подводя итоги вышеизложенному, важно отметить, что управление информационной безопасностью в системе общего образования не только ограждает от информационных угроз участников образовательного процесса, но и закладывает прочный фундамент в построении информационного общества.

Список литературы

1. Абдулгамидов И.Н. Новая роль Интернета в обществе и определение интернет-зависимости // Наука через призму времени. 2022. № 6. С. 115-117.
2. Белов А.С., Добрышин М.М., Шугуров Д.Е. Модернизация системы информационной безопасности // Защита информации. Инсайд. 2022. № 4. С. 76-80.
3. Ведерникова О.Н. Международно-правовые основы противодействия преступлениям против детей в сети Интернет // Международное уголовное право и международная юстиция. 2022. № 2. С. 28-32.
4. Жихарева Л.В. Кибербуллинг как форма девиантного поведения личности в интернет-пространстве // Научный результат. Педагогика и психология образования. 2022. Т.8. № 4. С. 115-126.
5. Зорина Н.С. Кибербуллинг среди подростков: понятие, виды и профилактика // Административное право и процесс. 2022. № 7. С. 19-23.
6. Кузьмина О.В. Информационно-технологическая безопасность обучающихся // ВІ-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: мат. IX Межд. науч.-практ. конф. Екатеринбург, 2021. С. 134-136.
7. Мансуров Г.З. Право цифровой безопасности: учеб. М.: Директ-Медиа, 2022. 148 с.
8. Оленников С.С. Современные проблемы компьютерной и Интернет-зависимости школьников // Инновационный путь развития как ответ на вызовы нового времени: мат. Межд. науч.-практ. конф. Уфа, 2020. С. 181-183.
9. Прудникова Л.Б., Шеншин В.М., Глейberman Н.С. Информация и информационная безопасность как атрибуты гражданского общества (краткий обзор взаимосвязи) // Государственная власть и местное самоуправление. 2022. № 7. С. 7-9.
10. Расина Э.О. Психологические детерминанты, оказывающие влияние на конструирование виртуального образа личности // Вестник Кемеровского государственного университета. 2021. Т. 23. № 3 (87). С. 705-716.
11. Расина Э.О. Психологические характеристики виртуального образа личности // Мир педагогики и психологии. 2021. № 6(59). С. 83-89.
12. Савин М.В., Кондратенко М.А. Методика выявления и оценки недопустимых событий на основе модели зрелости управления информационной безопасностью // Защита информации. Инсайд. 2023. № 1. С. 24-31.
13. Слабнин Б.Д., Абушкин Б.М. Влияние интернет-зависимости на личность подростка // Актуальные проблемы столичного мегаполиса в контексте практической подготовки студентов: мат. Круглого стола в рамках I Межд. науч.-практ. студен. конф. Ч. 2. (7 фев. 2018 г., Москва). М., 2018. С. 327-334.
14. Солдатова Г.У., Чигарькова С.В., Кошечкина А.Г., Никонова Е.Ю. Повседневная деятельность подростков в смешанной реальности: пользовательская активность и многозадачность // Сибирский психологический журнал. 2022. № 83. С. 20-45.
15. Тонких А.П., Прядехо А.А. Использование информационных и коммуникационных технологий в процессе подготовки будущего учителя начальных классов // Современное педагогическое образование. 2019. № 3. С. 221-224.
16. Федеральный закон N 436-ФЗ от 29 декабря 2010 г. (ред. от 28.04.2023) «О защите детей от информации, причиняющей вред их здоровью и развитию». https://www.consultant.ru/document/cons_doc_LAW_108808
17. Чучкалова И.Ю. Информационная безопасность в условиях трансформации общества // ВІ-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: мат. IX Межд. науч.-практ. конф. (2 дек. 2021 г., Екатеринбург). Екатеринбург, 2021. С. 120-122.
18. Юдеева Т.В. Мотивация деструктивного коммуникативного поведения подростков в социальных сетях // Международный научно-исследовательский журнал. 2022. № 2-2(116). С. 178-182.

Areas of activity of the teacher for the formation of information security of high school students

Vladislav A. Evtekhov

Graduate student

I.G. Petrovsky Bryansk State University

Bryansk, Russia

Vvlad.evtexR@yandex.ru

ORCID 0000-0000-0000-0000

Received 07.06.2024

Accepted 29.07.2024

Published 30.08.2024

UDC 37.016:004.8

DOI 10.25726/k8856-4636-9365-e

EDN CQKCFC

VAK 5.8.2. Theory and methodology of teaching and upbringing (by fields and levels of education) (pedagogical sciences)

OECD 05.03.HB. EDUCATION, SCIENTIFIC DISCIPLINES

Abstract

At the present stage of society's development, various telecommunications and information technologies have a great impact on people's lives, without which it is impossible to imagine one of the spheres of life. It should be noted that computer technologies are now often used in some areas of management. Nowadays, many people have been learning PCs since childhood. The World Wide Web has made a real revolution in many areas of human life, being a technological, economic and cultural phenomenon. But along with the positive contributions to a person's daily life, this «leap of progress» has brought with it many problems, of which the most acute is the problem of cybersecurity (information security). Also, at the moment, computer games on the Internet are almost the main form of entertainment for young people. In these circumstances, among other things, it is very important to ensure the achievement of information security. Among other things, it is important to ensure the smooth operation of the PC and the use of information resources. Therefore, one of the main objectives of the state policy of the Russian Federation in the field of national security is information security, which has determined the problems of this article.

Keywords

interactive technologies, military specialties, military professions, digitalization, military education, career guidance, cybersecurity, information security, information technology.

References

1. Abdulgamidov I.N. The new role of the Internet in society and the definition of Internet addiction // Science through the prism of time. 2022. № 6. pp. 115-117.
2. Belov A.S., Dobryshin M.M., Shugurov D.E. Modernization of the information security system. Inside. 2022. № 4. pp. 76-80
3. Vedernikova O.N. International legal framework for countering crimes against children on the Internet // International criminal law and international justice. 2022. № 2. pp. 28-32.
4. Zhikhareva L.V. Cyberbullying as a form of deviant personality behavior in the Internet space // Scientific result. Pedagogy and psychology of education. 2022. Vol.8. № 4. pp. 115-126.
5. Zorina N.S. Cyberbullying among adolescents: concept, types and prevention // Administrative law and process. 2022. № 7. pp. 19-23.

6. Kuzmina O.V. Information technology security of students // BI-technologies and corporate information systems in optimizing the business processes of the digital economy: mat. IX of the Inter. scien. and prac. conf. Yekaterinburg, 2021. pp. 134-136.
7. Mansurov G.Z. The law of digital security: a textbook. M.: Direct-Media, 2022. 148 p.
8. Olennikov S.S. Modern problems of computer and Internet addiction in schoolchildren // Innovative development path as a response to the challenges of modern times: mat. of the Inter. scien. and prac. conf. Ufa, 2020. pp. 181-183.
9. Prudnikova L.B., Shenshin V.M., Gleiberman N.S. Information and information security as attributes of civil society (a brief overview of the relationship) // State power and local self-government. 2022. № 7. pp. 7-9.
10. Racina E.O. Psychological determinants influencing the construction of a virtual personality image // Bulletin of Kemerovo State University. 2021. Vol. 23. № 3 (87). pp. 705-716.
11. Rasina E.O. Psychological characteristics of a virtual personality image // The world of pedagogy and psychology. 2021. № 6(59). pp. 83-89.
12. Savin M.V., Kondratenko M.A. Methodology for identifying and evaluating unacceptable events based on the maturity model of information security management // Information protection. Inside. 2023. № 1. pp. 24-31.
13. Slabnin B.D., Abushkin B.M. The influence of Internet addiction on the personality of a teenager // Actual problems of the metropolitan metropolis in the context of practical training of students: mat. of the Round table of the First Inter. scien. and prac. students' conf. Vol. 2. (February 7, 2018, Moscow). M., 2018. pp. 327-334.
14. Soldatova G.U., Chigarkova S.V., Koshevaya A.G., Nikonova E.Y. Daily activities of adolescents in mixed reality: user activity and multitasking // Siberian psychological journal. 2022. № 83. pp. 20-45.
15. Tonkikh A.P., Pryadekho A.A. The use of information and communication technologies in the process of training future primary school teachers // Modern pedagogical education. 2019. № 3. pp. 221-224.
16. Federal Law No. 436-FZ of December 29, 2010 (as amended on 04/28/2023) «On the protection of children from information harmful to their health and development». https://www.consultant.ru/document/cons_doc_LAW_108808
17. Chuchkalova I.Y. Information security in the context of society transformation // BI-technologies and corporate information systems in optimizing business processes of the digital economy: mat. IX Inter. scien. and prac. conf. (December 2, 2021, Yekaterinburg). Yekaterinburg, 2021. pp. 120-122.
18. Yudeeva T.V. Motivation of destructive communicative behavior of adolescents in social networks // International scientific research journal. 2022. № 2-2(116). pp. 178-182.