Научная статья
УДК 378.2
DOI: 10.24412/2072-9014-2026-175-86-102

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ПОДГОТОВКИ БУДУЩИХ УЧИТЕЛЕЙ-ПРЕДМЕТНИКОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ В УСЛОВИЯХ ВИРТУАЛИЗАЦИИ

Виталий Александрович Лаврухин

Мурманский арктический университет,
Мурманск, Россия

lavrukhin.va@mail.ru, http://orcid.org/0009-0006-7866-8301

Аннотация. В статье актуализируется вопрос обеспечения безопасности обучающихся в ответ на цифровые вызовы современности и виртуализации социально-образовательной среды как одного из результатов цифровой трансформации школы. Описаны классификация и модель уровней обеспечения безопасности при взаимодействии пользователя с цифровым и виртуальным пространством, которые не являются тождественными. На основании изложенных материалов описаны актуальные составляющие содержания учебного курса для будущих учителей-предметников по вопросам обеспечения информационной, цифровой и кибербезопасности учащихся.

Ключевые слова: вызовы и угрозы современности; цифровая трансформация школы; виртуализация; информационная безопасность; цифровая безопасность; кибербезопасность; модель уровней обеспечения безопасности; подготовка учителей.

Для цитирования: Лаврухин В. А. Теоретические аспекты подготовки будущих учителей-предметников в области обеспечения информационной безопасности обучающихся в условиях виртуализации / В. А. Лаврухин // Вестник МГПУ. Серия «Информатика и информатизация образования». 2026. № 1 (75). С. 86–102. https://doi.org/10.24412/2072-9014-2026-175-86-102

Original article
UDC 378.2
DOI: 10.24412/2072-9014-2026-175-86-102

THEORETICAL ASPECTS OF TRAINING FUTURE SUBJECT TEACHERS IN THE FIELD OF ENSURING INFORMATION SECURITY OF STUDENTS IN THE CONTEXT OF VIRTUALIZATION

Vitalii A. Lavrukhin

Murmansk Arctic University,
Murmansk, Russia

lavrukhin.va@mail.ru, http://orcid.org/0009-0006-7866-8301

Abstract. The article updates the issue of ensuring the safety of students in response to the digital challenges of the modern world and the virtualization of the socio-educational environment as one of the results of the digital transformation of schools. It describes the classification and model of security levels when a user interacts with the digital and virtual space, which are not identical. Based on these materials, the article describes the current components of the curriculum for future subject teachers on the issues of ensuring the information, digital, and cyber security of students.

Keywords: challenges and threats of the present; digital transformation of schools; virtualization; information security; digital security; cybersecurity; security level model; teacher training.

For citation: Lavrukhin V. A. Theoretical aspects of training future subject teachers in the field of ensuring information security of students and information security of students in the context of virtualization / V. A. Lavrukhin // MCU Journal of Informatics and Informatization of Education. 2026. № 1 (75). P. 86–102. https://doi.org/10.24412/2072-9014-2026-175-86-102

Введение

Любая образовательная организация и система образования в целом, являясь одним из важнейших социальных институтов любого государства, тесно связана со всеми изменениями в различных сферах общества: экономической, культурной, политической и научно-технологической, в том числе в информационно-коммуникационной среде. Данный факт не позволяет школе существовать изолированно от социума и не принимать во внимание все изменения, которые происходят в этих сферах.

Как подчеркивается в работе В. В. Гриншкуна и Г. А. Красновой [1], большинство процессов, протекающих в современной образовательной организации, от обучения и воспитания до административно-хозяйственных и кадровых

вопросов, все больше зависят от цифровых технологий — новых достижений информационных и технологических революций. Среди них: различные автоматизированные-информационные системы результатов образовательной деятельности и профилактики безнадзорности и правонарушений; онлайн-платформы как для обучения школьников, так и для повышения уровня квалификации учителей; системы управления учебно-воспитательным процессом; иные инструменты и онлайн-сервисы для совместной работы в ходе выполнения учебных исследовательских проектов и для самостоятельной работы учащихся с информацией различных видов.

Одним из основных источников знаний для обучающихся, а также знаковой фигурой для них в вопросах безопасного поведения, в том числе информационно-безопасного, был и остается учитель. Именно он, наряду с родителями, играет ключевую роль в формировании у учеников цифровой компетентности и в целом цифровой культуры. Уже сейчас многие образовательные порталы разрабатывают и предлагают для работающих учителей различные онлайн-курсы в области цифровой безопасности, к примеру образовательный портал Prodlenka[1], российское общество «Знание»[2] и др. Обозначенный выше запрос системы образования к практикующим специалистам в области информационной, цифровой и кибербезопасности обусловлен современным уровнем развития информационного общества, основной характеристикой которого является повсеместное внедрение технологий цифровизации и виртуализации социальной среды. Их образовательный потенциал предоставляет педагогам особые инновационные возможности, обращается внимание в работе С. Г. Григорьева, М. А. Родионова и О. А. Кочетковой [2].

В настоящее время накоплен достаточно обширный отечественный и зарубежный опыт эмпирических и научно-методических исследований в области виртуализации общества с различных позиций научного знания и с целью поиска единого подхода к трактовке данного понятия (см. работы С. Дудник [3], М. Кастельс [4], Т. В. Марковой и Е. С. Мартьянова [5], Д. В. Иванова [6] и др.). Важность изучения процессов виртуализации социальных институтов и характерного взаимодействия с элементами социума, преимущества и возможные риски повсеместной виртуализации и, как следствие, виртуализация социально-образовательного пространства акцентировалась в работах А. В. Гриншкуна [7], С. Д. Каракозова, Н. Ю. Королевой, Н. И. Рыжовой [8] и др.

Проблема исследования состоит в том, что, несмотря на активное внедрение цифровых инструментов в образовательный процесс и стремительное

[1] Каталог курсов повышения квалификации ОП «Prodlenka». URL: https://www.prodlenka.org/kpk-dlja-pedagogov/cifrovaja-gramotnost-pedagoga-i-osnovy-bezopa (дата обращения: 19.12.2025).

[2] URL: https://znanierussia.ru/news/znanie-zapustilo-onlajn-kurs-po-kiberbezopasnosti-dlya-pedagogov-i-roditelej (дата обращения: 19.12.2025).

расширение виртуального пространства взаимодействия обучающихся, в педагогической науке и практике отсутствует единое понимание модели обеспечения информационной безопасности, учитывающей специфику угроз, характерных именно для виртуальных технологий и разграничивающей уровни информационной, кибер- и цифровой безопасности применительно к этим инструментам. Это актуализирует проблематику профессиональной подготовки будущих учителей-предметников с точки зрения обеспечения безопасности обучающихся в виртуальном пространстве на указанных уровнях.

Цель исследования — разработать трехуровневую модель обеспечения информационной безопасности обучающихся как пользователей виртуального пространства и на ее основе предложить конкретизацию содержания соответствующего учебного курса для будущих педагогов.

Для достижения обозначенной цели необходимо решить следующие *задачи*, которые определяют и логику исследования:

– Первый этап: проанализировать научно-методические источники, цифровые инструменты взаимодействия с виртуальной социально-образовательной средой и предложить классификацию характерных для них угроз безопасности.

– Второй этап: построить модель уровней безопасности, разграничивающую информационную, кибер- и цифровую безопасность.

– Третий этап: на основе модели определить актуальные элементы содержания учебного курса по данной проблематике для будущих учителей-предметников.

Методы исследования

Для достижения поставленной цели в ходе исследования применялся комплекс теоретических и эмпирических методов.

Теоретические методы: анализ и систематизация отечественных и зарубежных научных источников по проблемам виртуализации общества, информационной безопасности, кибербезопасности и цифровой безопасности; сравнительный анализ подходов к трактовке ключевых понятий; классификация угроз безопасности применительно к конкретным цифровым инструментам взаимодействия с виртуальной социально-образовательной средой; метод моделирования — для построения трехуровневой модели обеспечения информационной безопасности пользователей виртуального пространства на уровне информационной, кибер- и цифровой безопасности..

Эмпирические методы: анализ открытых источников в интернете — тематических форумов, каталогов поисковых запросов в области цифровой безопасности; обобщение педагогического опыта реализации курсов в области цифровой безопасности в системе подготовки учителей.

Нормативную основу для данного исследования составляет Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[3], определяющая государственные приоритеты в области цифровой безопасности граждан, в том числе обучающихся.

Результаты исследования

Наиболее широкое понимание виртуализации с позиций исследования некомпьютерного вида виртуализации общества, предложенное Д. В. Ивановым, позволяет трактовать этот процесс как «любое замещение реальности ее симуляцией или образом, причем не обязательно с помощью компьютерной техники, но обязательно с применением логики виртуальной реальности» [6, с. 143]. В настоящее время условно определяются два вида виртуализации: некомпьютерная (с позиций философии, социологии, экономики, политики и т. п.) и компьютерная (с позиций информатики, криптографии, компьютерной графики, искусственного интеллекта и т. п.).

Так, Г. Бехман в своей работе рассматривает виртуализацию общества как «процесс создания альтернативного социального пространства» [9, с. 58], другие предлагают определять ее как «конвергенцию виртуальной и физической реальности с расширением спектра коммуникативных практик» (А. П. Моисеева, О. А. Мазурина, О. А. Перепелкин) [10, с. 143] или как «семиотическое замещение действительности» (Ж. Бодрийяр) [11, с. 76].

Вместе с тем в диссертационном исследовании А. А. Бодрова виртуализация общества представляет собой «процесс замещения институциональных практик симуляциями» [12, с. 48], а Ю. А. Кузнецова определяет концепцию виртуального пространства как «область постоянно развивающихся социальных взаимоотношений и взаимодействий, возникающих, продолжающихся, прекращающихся в процессе пользования продуктами информационного-цифрового-сетевого общества» [13, с. 347].

Ряд исследователей рассматривает феномен виртуализации общества с позиций компьютеризации и цифровизации. Так, М. М. Назаров определяет ее как «создание достоверных цифровых имитаций средствами современных компьютерных технологий» [14, с. 143]. Э. В. Алиев предлагает рассматривать ее в качестве компьютерных систем, которые обеспечивают визуальные и звуковые эффекты, погружающие зрителя в воображаемый мир за экраном [15, с. 33].

Однако, несмотря на различные, описанные выше теоретико-методологические подходы к определению виртуализации общества, большинство исследователей сходятся в факте, приведенном в работе С. Д. Каракозова, Н. И. Рыжовой и Н. Ю. Королевой: «В современном мире изменяется характер

[3] URL: https://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 14.11.2025).

субъект-субъектного и субъект-объектного взаимодействия членов социума с его элементами» [8, с. 7], что, безусловно, влияет на набор компетентностей у пользователей, обусловленный овладением инструментами и сервисами, необходимыми для эффективного взаимодействия с компонентами виртуальной социальной среды.

Современный запрос социума и государства, в частности, ориентирован на развитие информационного общества с ориентиром на определенные цели, решением очерченного круга задач и выстроенную систему мер по реализации внутренней и внешней политики России. Все эти аспекты находят отражение в стратегии развития информационного общества в Российской Федерации. Подрастающее поколение, которому предстоит жить и функционировать в цифровом обществе, является одним из центральных компонентов, нуждающихся в овладении современными цифровыми инструментами и сервисами взаимодействия с составляющими социально-образовательной среды в условиях ее виртуализации.

В практику образовательных организаций внедряются учебные курсы по освоению принципов взаимодействия и использования технологий искусственного интеллекта [16], применения AR-/VR-технологий в жизни и деятельности [2; 17], в научно-методической литературе описывается педагогический опыт их внедрения. В работах К. В. Розова [18], И. А. Бекшаева [19], А. В. Гриншкуна и др. [20] обосновывается современная объективная потребность в реализации данных учебных курсов.

Приведем ряд основных, на наш взгляд, групп цифровых инструментов, используемых обучающимися в виртуальной социально-образовательной среде, среди которых присутствуют как ставшие уже традиционными и включенными в образовательные программы основного общего и среднего общего образования, так и набирающие все большую актуальность среди подрастающего поколения, но имеющие пока недостаточную проработку в методической литературе: (1) офисные пакеты; (2) системы управления базами данных; (3) веб-браузеры; (4) облачные технологии; (5) сервисы Web 2.0 и Web 3.0; (6) инструменты работы с AR- и VR-технологиями; (7) приложения для работы с нейросетью и искусственным интеллектом.

Овладение приведенным выше набором цифровых инструментов должно не только быть высокоэффективным с точки зрения пользы от их использования, но и осуществляться с соблюдением общих принципов безопасности, так как пользователь имеет гипотетическую возможность столкнуться (а зачастую и сталкивается) с воздействием различных угроз для личной и/или аппаратно-программной безопасности. Такое суждение тесно связано с мнением многих исследователей, которые в своих работах отмечают важность проведения научных исследований, позволяющих получить новые знания о киберугрозах и способах их профилактики.

Изучив различные форумы в интернете, каталог наиболее популярных запросов к различным поисковым системам в области цифровой безопасности,

а также на основе эмпирического опыта по данной проблематике мы выделили ряд основных угроз безопасности различного характера, которые представлены в таблице.

Таблица

Основные угрозы безопасности при работе с цифровыми инструментами в виртуальной социально-образовательной среде

Цифровой инструмент виртуальной социально-образовательной среды	Угрозы безопасности
Офисные пакеты	Нарушение целостности файлов
	Встраивание вредоносных COM-объектов
	Уязвимости устаревших компонентов офисных пакетов
	Запуск вредоносных DLL-библиотек и исполняемых файлов с помощью макросов VBA
	Запуск вредоносного JavaScript-кода через встроенные скрипты
	Эксплуатация уязвимостей различных форматов файлов с целью выполнения удаленного кода при открытии документа
	Фишинговые письма с вложениями
Системы управления базами данных	Подключение к внешним источникам данных без участия пользователя, через открытие документа и несанкционированный доступ к данным внутренней БД
	Нарушение целостности данных в результате программного воздействия на СУБД или ошибок пользователя
	DoS/DDoS-атаки
	Эскалация привилегий
	Неправильная настройка СУБД, устаревшее ПО или недостатки в логике работы приложений
Web-браузеры	Уязвимость нулевого дня
	Атаки на известные уязвимости устаревших браузеров, которые не были исправлены из-за отсутствия обновлений
	Межсайтовый скриптинг
	Распространение в сети эксплойтов и их пакетов
	Вредоносная реклама
	Вредоносные HTML-вложения
	Фишинговые сайты и спеар-фишинг
	Использование технологии «Злой двойник»

Цифровой инструмент виртуальной социально-образовательной среды	Угрозы безопасности
	Вредоносные расширения браузера
	Перехват сетевых сеансов пользователя
	Компрометация данных пользователя через кэш браузера и его историю
	Перехват сетевого трафика (атаки типа «человек посередине»)
Облачные технологии	Уязвимости в интерфейсах API и/или СУД
	Фишинговые атаки на облачные хранилища и сервисы
	Брутфорс-атаки
	DDoS-атаки
	Уязвимости в гипервизорах
	Недостаточное сегментирование облачной среды
	Неправильная настройка компонентов облачной инфраструктуры
	Нарушение целостности данных, хранящихся в облачных сервисах
	Игнорирование пользователем правил цифровой гигиены
	Слабая политика аутентификации со стороны облачного сервиса
	Нарушение принципов парольной защиты со стороны пользователя
Сервисы Web 2.0	Слабая защита каналов передачи данных, и, как следствие, утечка персональных и учетных данных
	XML-уязвимости, приводящие к запуску вредоносных файлов или TCP-соединений
	Распространение вредоносного контента через совместные приложения, RSS/Atom-ленты
	Вирусные программы (черви, троянские программы и т. п.)
	Спам и мошенничество
	Уязвимость клиентских приложений
	Злоупотребление возможностями сервисов для обхода систем безопасности ПО
	Нарушение целостности данных при совместном доступе
	Автоматизация различного рода атак вследствие отсутствия должной защиты от ботов

Цифровой инструмент виртуальной социально-образовательной среды	Угрозы безопасности
	Нарушение принципов парольной защиты со стороны пользователя
	Психологическая зависимость пользователя
Сервисы Web 3.0	Уязвимости смарт-контрактов
	Фишинговые атаки с целью компрометации seed-фраз, доступа к кошелькам и т. п.
	Clipper-атаки
	Скрытое предоставление разрешений на управление пользовательским токеном
	Атаки на блокчейны
	Уязвимость DeFi-платформ
	Мошенничество с токенами и проектами
	Уязвимости фронтенда DApps
	Несовершенство механизмов консенсуса
Инструменты работы с AR- и VR-технологиями	Компрометация сетевых учетных данных
	Внедрение вредоносного кода в AR- и VR-приложения через рекламу и фишинговые атаки
	Перехват данных, передаваемых между AR- и VR-приложениями, поставщиками услуг и сторонними серверами
	Кибершантаж с использованием записей действий с дополненной и/или виртуальной реальностью
	Утечка данных о пользователе: местоположение, голосовые параметры, взаимодействия и т. п.
	Кибершпионаж через датчики устройств
	Подмена данных и дезинформация посредством манипуляций с контентом и средств социальной инженерии
	Дипфейки
	Фальшивые указатели, экраны и интерфейсы
Приложения для работы с нейросетью и искусственным интеллектом	Утечка конфиденциальной информации, в том числе с целью улучшения алгоритмов обучения нейросети и ИИ
	Генерирование правдоподобной, но недостоверной информации
	Промпт-инъекции и отравление данных
	Генерация вредоносного кода и его модификация, киберпреступления
	«Наученная» предвзятость алгоритмов
	Зависимость от использования систем ИИ

Анализируя отмеченные в таблице основные угрозы безопасности, можно заметить, что такая угроза, как утечка персональных и учетных данных, в том или ином виде актуальна при работе практически со всеми цифровыми инструментами виртуальной социально-образовательной среды: системами управления базами данных, веб-браузерами, облачными технологиями, сервисами Web 2.0 и Web 3.0, инструментами работы с AR- и VR-технологиями, а также приложениями для работы с нейросетью и искусственным интеллектом. Безусловно, данная угроза будет обязательно приобретать различную функциональную реализацию в зависимости от использования того или иного конкретного инструмента.

Вместе с тем отметим, что успешное противостояние ущербу от реализации такой угрозы зависит от высокого уровня владения пользователем основами политики работы с персональными данными, парольной защиты, шифрования данных, технических средств защиты от взломов и т. д., которое является общеприменимым и не зависит от использования того или иного конкретного цифрового инструмента.

Таким образом, обозначенные выше угрозы можно разделить на несколько основных групп, исходя из целевой инфраструктурной мишени:

– уязвимость программного обеспечения;
– искажение пользовательских данных;
– кража персональных и учетных данных;
– атаки по типу «человек посередине»;
– киберпреступления;
– фишинговые атаки;
– вредоносный контент; социальные манипуляции.

Схематично обобщенная модель виртуальной социально-образовательной среды и уровни взаимодействия пользователя с компонентами виртуального пространства представлены нами ранее [21, с. 133]. Вместе с тем, расширяя ранее проведенное исследование, отметим, что такое взаимодействие не является «свободным» от угроз иных компонентов и других пользователей виртуальной среды, объединенных нами в группы (см. рис. 1).

Как видно из представленной схемы из рисунка 1, в процессе взаимодействия пользователя с компонентами виртуальной социально-образовательной среды современные виды угроз и рисков стремятся к негативному воздействию как на технические компоненты виртуальной среды, так и на инструменты и сервисы взаимодействия с ними пользователя, а также и на самого пользователя. Необходимо признать, что вопрос обеспечения безопасности при функционировании в виртуальном обществе не менее важен, чем ИКТ-компетентность самих пользователей, а во многих случаях еще и первостепенен (потеря репутации, денег и т. п.).

В современных исследованиях рассматриваются методы и средства противостояния различным угрозам в интернете, активно используются понятия информационной безопасности, кибербезопасности, цифровой

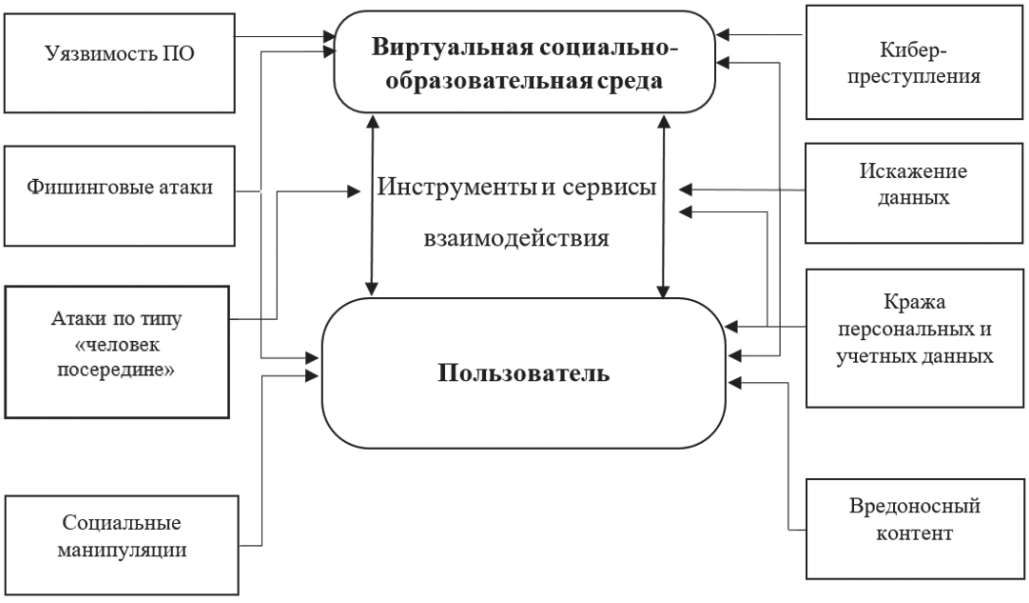

Рис. 1. Пул основных групп угроз и рисков современного взаимодействия пользователя с виртуальной социально-образовательной средой

безопасности. Основные подходы к их трактовкам рассматривались нами ранее [22]. В работе мы выявили, что, несмотря на схожесть обозначенных выше понятий, они имеют существенные различия и в основном определяют защиту различных компонентов виртуального пространства, что также нашло отражение в ранее опубликованных исследованиях [23; 24].

Таким образом, основной параметр защиты при обеспечении:

- *кибербезопасности* — киберпространство, то есть в нашей терминологии — компоненты, инструменты и сервисы виртуальной социально-образовательной среды;
- *информационной безопасности* — общие данные при различных видах угроз;
- *цифровой безопасности* — личность самого пользователя.

Обратим внимание, что инструменты обеспечения безопасности являются основным барьером от воздействия угроз и рисков, и «условно безопасное» взаимодействие пользователей с виртуальной социально-образовательной средой становится возможным при реализации трехуровневой модели безопасности пользователя (рис. 2).

Графическая визуализация представленной модели показывает, что внешние угрозы и риски безопасному взаимодействию пользователя с виртуальной социально-образовательной средой не оказывают негативного влияния ни на инфраструктуру виртуального взаимодействия, ни на самого пользователя, если будут обеспечены:

а) организационные условия кибер-, информационной и цифровой безопасности;

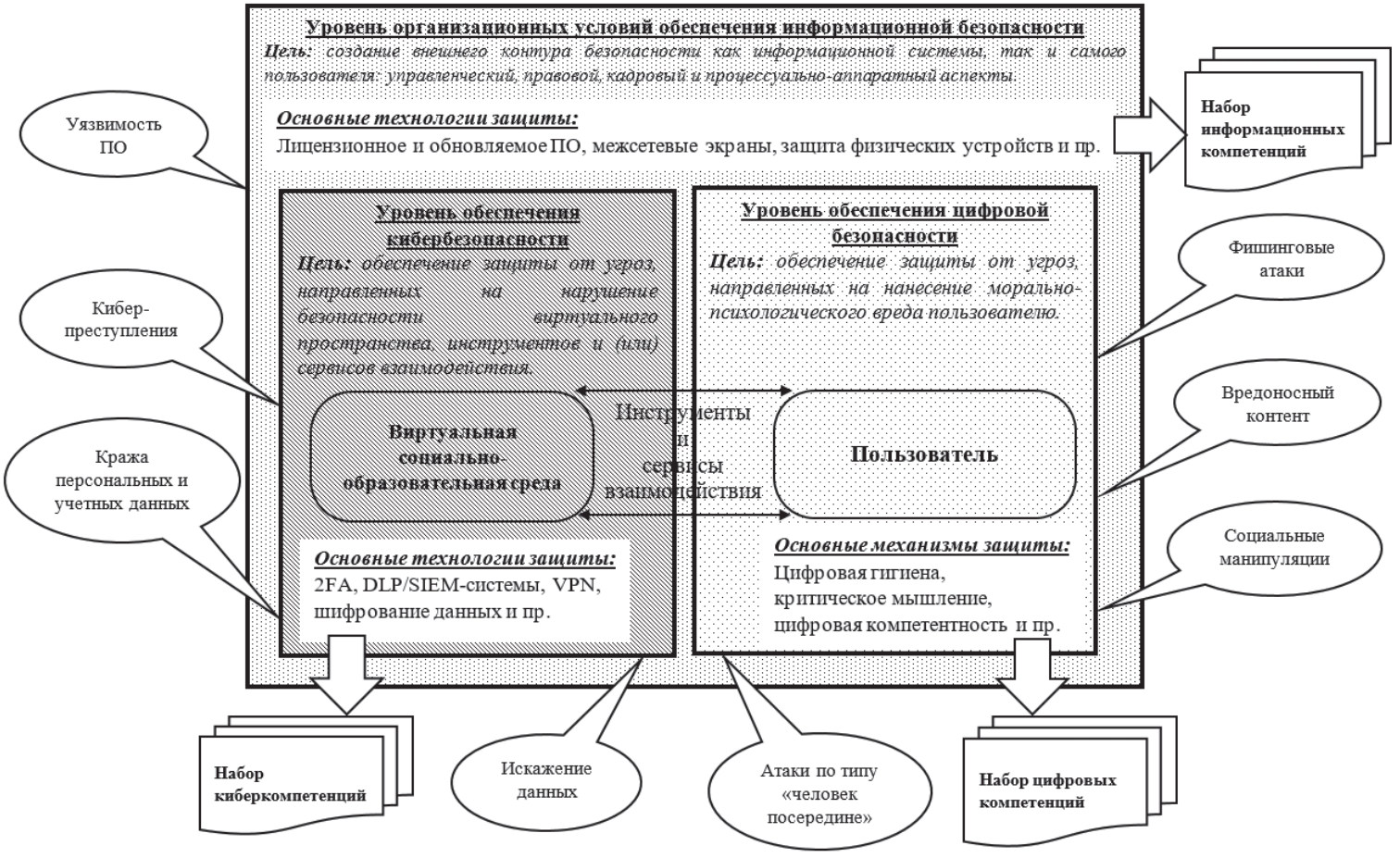

Рис. 2. Модель обеспечения безопасности обучающихся при взаимодействии с виртуальной социально-образовательной средой

б) эффективное применение технологий обеспечения кибербезопасности;

в) эффективное овладение механизмами цифровой безопасности со стороны обучающихся.

Обратим внимание, что каждый из выделенных уровней безопасности обеспечивается своим набором технологий и механизмов защиты, которые становятся своеобразным щитом между угрозами и пользователями/компонентами виртуальной социально-образовательной среды/инструментами взаимодействия/сервисами взаимодействия.

Безусловно, уровень обеспечения безопасности зависит не только и не столько от наличия тех или иных инструментов обеспечения кибер- или цифровой безопасности в распоряжении пользователя, сколько от их правильной настройки и грамотного использования.

Например, в 2024 г. на всей территории России был запущен процесс целенаправленного замедления скорости доступа к видеохостингу YouTube, что подтолкнуло российских пользователей, в том числе и обучающихся средних школ, к установке на свои смартфоны/ноутбуки VPN-приложений ради обхода ограничений и, как они считают, сохранения конфиденциальности своих личных данных в интернете. Вместе с тем в погоне за сиюминутной выгодой пользователи были подвержены еще большему риску и утечке данных, что стало возможным вследствие несформированного набора необходимых цифровых и киберкомпетенций.

Исходя из понимания того, что современные учащиеся активно взаимодействуют с виртуальной образовательной средой и обществом, а технологии такого взаимодействия стремительно развиваются, как и угрозы безопасности, можно сделать вывод о том, что освоение таких технологий и главным образом нейтрализация нарастающей угрозы является одним из основных вопросов современного содержания подготовки в этой области будущих учителей-предметников.

На наш взгляд, с учетом сегодняшних реалий и технолого-операциональных технологий взаимодействия с внешней и внутренней средой обучающихся, учителей-предметников и образовательной организации в целом, особенно остро стоит вопрос о необходимости внедрения в профессиональную подготовку будущих учителей не только информатики, но и других предметов, учебного курса, который позволил бы организовать безопасную информационную среду образовательной организации.

Заключение

Не претендуя на полноту анализа, скажем, что в научно-методических работах предлагаются и обосновываются различные подходы к решению проблемы обучения будущих учителей в области обеспечения информационной безопасности обучающихся при взаимодействии с виртуальной социально-образовательной средой: путем расширения содержания отдельных дисциплин

и/или путем введения спецкурсов, включенных в программы профессиональной и предметной подготовки будущих учителей. Мы предложили примерное содержание курса «Цифровая гигиена и кибербезопасность» для студентов, обучающихся по различным профилям направления «Педагогическое образование» (кроме профиля «Информатика»), включающего такие модули, как:

1) киберпространство и современные киберугрозы;
2) программные способы защиты информации;
3) цифровая гигиена и принципы безопасного поведения в киберпространстве;
4) безопасное использование авторского контента;
5) нормативно-правовое обеспечение информационной безопасности учащихся;
6) информационная культура и цифровая этика;
7) безопасность использования систем искусственного интеллекта.

В содержание данных модулей нами включены различные аспекты обеспечения кибер-, информационной и цифровой безопасности обучающихся при работе в виртуальном пространстве, а в качестве структурных компонентов каждого модуля представлены как теоретические аспекты обеспечения безопасности, так и тематические практические работы. Апробация предлагаемого содержания планируется в рамках дисциплины «Технологии цифрового образования», читаемой будущим учителям, обучающимся по различным профилям направления «Педагогическое образование» в Мурманском арктическом университете.

Функционирование обучающихся в виртуальных образовательном и социальном пространствах ставит перед педагогами и специалистами проблемы создания такой информационной среды образовательной организации, в которой в должной мере будут обеспечены как ИКТ-насыщенность и верифицированность ее контента, так и их информационная безопасность при использовании цифровых инструментов взаимодействия с элементами этой среды.

Список источников

1. Гриншкун В. В. Новое образование для новых информационных и технологических революций / В. В. Гриншкун, Г. А. Краснова // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2017. Т. 14. № 2. С. 131–139.

2. Григорьев С. Г. Образовательные возможности технологий дополненной и виртуальной реальности / С. Г. Григорьев, М. А. Родионов, О. А. Кочеткова // Информатика и образование. 2021. № 10 (329). С. 43–56.

3. Дудник С. И. Отчуждение в цифровом обществе / С. И. Дудник // Вопросы философии. 2020. № 3. С. 17–20.

4. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. М.: ВШЭ, 2000. 606 с.

5. Маркова Т. В. Виртуальная реальность как социальный феномен / Т. В. Маркова, Е. С. Мартьянов // Интерактивная наука. 2018. № 5 (27). С. 64–66.

6. Иванов Д. В. Виртуализация общества. Версия 2.0 / Д. В. Иванов. СПб.: Петербургское востоковедение, 2002. 213 с.

7. Гриншкун А. В. Использование дополненной виртуальности как иммерсивной образовательной технологии в рамках профильного обучения школьников / А. В. Гриншкун // Профильная школа. 2020. Т. 8. № 4. С. 27–31.

8. Каракозов С. Д. Виртуальная реальность: генезис понятия и тенденции использования в образовании / С. Д. Каракозов, Н. И. Рыжова, Н. Ю. Королева // Информатика и образование. 2020. № 10 (319). С. 6–16.

9. Бехманн Г. Современное общество: общество риска, информационное общество, общество знаний / Г. Бехманн. М.: Логос, 2010. 247 с.

10. Моисеева А. П. Виртуализация как социальная трансформация и коммуникация / А. П. Моисеева, О. А. Мазурина, О. А. Перепелкин // Известия Томского политехнического университета. 2010. Т. 316. № 6. С. 141–146.

11. Бодрийяр Ж. В тени молчаливого большинства, или Конец социального / Ж. Бодрийяр. Екатеринбург: Изд-во Уральского университета, 2000. 95 с.

12. Бодров А. А. Виртуальная реальность как когнитивный и социокультурный феномен: дис. … д-ра филос. наук: 09.00.01. Самара, 2007. 293 с.

13. Кузнецова Ю. А. Виртуализация общества: «киберпротезирование» социальных форм взаимодействия / Ю. А. Кузнецова // Вестник Санкт-Петербургского университета. Социология. 2021. Т. 14. Вып. 4. С. 344–359.

14. Назаров М. М. Массовая коммуникация и общество: Введение в теорию и исследования / М. М. Назаров. М.: Либроком, 2010. 354 с.

15. Алиев Э. В. Проблемы использования цифровых технологий в киноиндустрии / Э. В. Алиев // European Journal of Arts. 2023. № 1. С. 33–37.

16. Искусственный интеллект в образовательном контенте: актуальный тренд и практические аспекты эволюции учебного процесса / А. А. Калинин [и др.] // Наука и школа. 2024. № 5. С. 98–113.

17. Королева Н. Ю. Обучение будущих учителей использованию технологий дополненной реальности: подходы и опыт реализации / Н. Ю. Королева // Информатика и образование. 2024. Т. 39. № 5. С. 40–49.

18. Розов К. В. О необходимости изменения содержания профессиональной подготовки будущего учителя информатики в области искусственного интеллекта / К. В. Розов // Информатика и образование. 2020. № 4 (313). С. 12–26.

19. Бекшаев И. А. Теоретические предпосылки формирования профессиональных компетенций будущих педагогов средствами технологий виртуальной реальности / И. А. Бекшаев // Проблемы современного педагогического образования. 2025. № 87-1. С. 25–28.

20. Using methods and means of the augmented reality technology when training future teachers of the digital school / A. V. Grinshkun [et al.] // European Journal of Contemporary Education. 2021. No. 10 (2). P. 358–374.

21. Королева Н. Ю. Модель содержания обучения взаимодействию в виртуальной социально-образовательной среде пользователей различных категорий / Н. Ю. Королева, В. А. Лаврухин // Преподаватель XXI век. 2016. № 4-1. С. 128–140.

22. Лаврухин В. А. Информационная безопасность и кибербезопасность в условиях вызовов современности: актуальность, сходства и различия / В. А. Лаврухин // Человек и образование. 2024. № 1 (78). С. 123–131.

23. Рыжова Н. И. Противодействие современным информационным угрозам как актуальная задача педагогической профилактики в условиях цифровой трансформации

образования / Н. И. Рыжова, Н. Ю. Королева // ОБЖ: Основы безопасности жизни. 2024. № 3. С. 33–41.

24. Рыжова Н. И. Содержание обучения учителей основам обеспечения кибербезопасности школьников в условиях цифровизации / Н. И. Рыжова, Н. Ю. Королева, В. А. Лаврухин // Педагогическая информатика. 2023. № 2. С. 5–16.

References

1. Grinshkun V. V. New education for new information and technological revolutions / V. V. Grinshkun, G. A. Krasnova // RUDN journal of informatization in education. 2017. Vol. 14. No. 2. P. 131–139.

2. Grigoriev S. G. Educational opportunities of augmented and virtual reality technologies / S. G. Grigoriev, M. A. Rodionov, O. A. Kochetkova // Informatics and Education. 2021. No. 10 (329). P. 43–56.

3. Dudnik S. I. Alienation in the digital society / S. I. Dudnik // Questions of Philosophy. 2020. No. 3. P. 17–20.

4. Castels M. The Information Age: economics, society and culture / M. Castels. M.: Higher School of Economics, 2000. 606 p.

5. Markova T. V. Virtual reality as a social phenomenon / T. V. Markova, E. S. Martianov // Interactive science. 2018. No. 5 (27). P. 64–66.

6. Ivanov D. V. Virtualization of society. Version 2.0 / D. V. Ivanov. St. Petersburg: Petersburg Oriental Studies, 2002. 213 p.

7. Grinshkun A. V. The use of augmented virtuality as an immersive educational technology in the framework of specialized education for schoolchildren / A. V. Grinshkun // Specialized school. 2020. Vol. 8 No. 4. P. 27–31.

8. Karakozov S. D. Virtual reality: the genesis of the concept and trends of use in education / S. D. Karakozov, N. I. Ryzhova, N. Yu. Koroleva // Informatics and Education. 2020. No. 10 (319). P. 6–16.

9. Behmann G. Modern society: society of risk, information society, society of knowledge / G. Behmann. M.: Logos, 2010. 247 p.

10. Moiseeva A. P. Virtualization as social transformation and communication / A. P. Moiseeva, O. A. Mazurina, O. A. Perepelkin // Proceedings of Tomsk Polytechnic University. 2010. Vol. 316. No. 6. P. 141–146.

11. Baudrillard J. In the Shadow of the Silent Majority, or the End of the Social / J. Baudrillard. Yekaterinburg: Publishing House of the Ural University, 2000. 95 p.

12. Bodrov A. A. Virtual reality as a cognitive and sociocultural phenomenon: dissertation by Dr. of Philos. Sciences : 09.00.01. Samara, 2007. 293 p.

13. Kuznetsova Yu. A. Virtualization of society: “cyber prosthetics” of social forms of interaction / Yu. A. Kuznetsova // Bulletin of St. Petersburg University. Sociology. 2021. Vol. 14. Is. 4. P. 344–359.

14. Nazarov M. M. Mass communication and society: An introduction to theory and research / M. M. Nazarov. M.: Librocom, 2010. 354 p.

15. Aliev E. V. Problems of using digital technologies in the film industry / E. V. Aliev // European Journal of Arts. 2023. No. 1. P. 33–37.

16. Artificial intelligence in educational content: an actual trend and practical aspects of the evolution of the educational process / A. A. Kalinin [et al.] // Science and School. 2024. No. 5. P. 98–113.

17. Koroleva N. Yu. Training future teachers to use augmented reality technologies: approaches and implementation experience / N. Yu. Koroleva // Informatics and Education. 2024. Vol. 39. No. 5. P. 40–49.

18. Rozov K. V. On the need to change the content of professional training of future computer science teachers in the field of artificial intelligence / K. V. Rozov // Informatics and education. 2020. No. 4 (313). P.12–26.

19. Bekshaev I. A. Theoretical prerequisites for the formation of professional competencies of future teachers by means of virtual reality technologies / I. A. Bekshaev // Problems of modern pedagogical education. 2025. No. 87-1. P. 25–28.

20. Using methods and means of the augmented reality technology when training future teachers of the digital school / A. V. Grinshkun [et al.] // European Journal of Contemporary Education. 2021. No. 10 (2). P. 358–374.

21. Koroleva N. Yu. A model of the content of teaching interaction in a virtual socio-educational environment of users of various categories / N. Yu. Koroleva, V. A. Lavrukhin // Teacher of the XXI century. 2016. No. 4-1. P. 128–140.

22. Lavrukhin V. A. Information security and cybersecurity in the context of modern challenges: relevance, similarities and differences / V. A. Lavrukhin // Man and education. 2024. No. 1 (78). P. 123–131.

23. Ryzhova N. I. Countering modern information threats as an urgent task of pedagogical prevention in the context of digital transformation of education / N. I. Ryzhova, N. Yu. Koroleva // OBZH: Fundamentals of life safety. 2024. No. 3. P.33–41.

24. Ryzhova N. I. The content of teaching teachers the basics of ensuring cybersecurity of schoolchildren in the context of digitalization / N. I. Ryzhova, N. Yu. Koroleva, V. A. Lavrukhin // Pedagogical Informatics. 2023. No. 2. P. 5–16.

Статья поступила в редакцию: 20.12.2025;
одобрена после рецензирования: 04.02.2026;
принята к публикации: 04.02.2026.

The article was submitted: 20.12.2025;
approved after reviewing: 04.02.2026;
accepted for publication: 04.02.2026.

Информация об авторе / Information about the author

Виталий Александрович Лаврухин — аспирант, кафедра информационных технологий, Институт интеллектуальных систем и цифровых технологий, Мурманский арктический университет, Мурманск, Россия.

Vitalii A. Lavrukhin — Postgraduate Student, Department of Information Technologies, Institute of Intelligent Systems and Digital Technologies, Murmansk Arctic University, Murmansk, Russia.

lavrukhin.va@mail.ru, http://orcid.org/0009-0006-7866-8301