



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

Кафедра подготовки педагогов профессионального
обучения и предметных методик

НАУЧНЫЙ ДОКЛАД
об основных результатах научно-квалификационной работы (диссертации)
тема «Воспитание культуры кибербезопасности у курсантов военных вузов»

Направление подготовки 44.06.01 Образование и педагогические науки
код, направление

Направленность программы
«Теория и методика профессионального образования»

Аспирант _____
(подпись)

В.М. Цаплин

Научный руководитель _____
(подпись)

Н.В. Уварина

Челябинск
2025

ОБЩАЯ ХАРАКТЕРИСТИКА ИССЛЕДОВАНИЯ

Актуальность исследования. Обеспечение комплексной безопасности граждан и защита национальных интересов составляют стратегический приоритет государственной политики. В условиях современной геополитической динамики понятие безопасности трансформируется, выходя далеко за пределы традиционных представлений о физической защищенности. Сегодня оно охватывает создание условий для устойчивого развития всех сфер общественной жизнедеятельности, формируя многомерную систему противодействия вызовам технологической, информационной и социальной природы. Эта новая парадигма требует интеграции превентивных мер, обеспечивающих не только защиту от непосредственных угроз, но и устойчивое развитие общества в условиях непредсказуемости современных рисков.

Современный этап развития Вооруженных Сил Российской Федерации характеризуется интенсивной цифровизацией всех сфер военной деятельности, что обуславливает возникновение принципиально новых вызовов в области обеспечения безопасности. Киберпространство превратилось в полноценную область ведения боевых действий, где противоборство осуществляется с использованием сложных технологических решений и методов психологического воздействия.

Современный анализ научных публикаций и государственных стратегических документов позволяет констатировать, что кибербезопасность превратилась в ключевой элемент национальной безопасности. Согласно Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы (утвержденной Указом Президента № 203 от 9 мая 2017 г.), российский сегмент интернета уже к 2016 году объединял свыше 80 миллионов пользователей, при этом демонстрируя устойчивую тенденцию к экспоненциальному росту.

Цифровая экосистема, включающая электронные СМИ, информационные платформы, социальные сети и другие интернет-ресурсы, стала фундаментальным компонентом повседневной жизни российского общества. Как подчеркивается в стратегическом документе, к 2017 году информационное пространство уже пронизывало все критически важные сферы: от доступа к достоверной информации и участия в цифровой экономике до обеспечения устойчивости объектов критической информационной инфраструктуры.

В этом контексте защита цифрового суверенитета закономерно рассматривается как одна из приоритетных задач государства, направленная на сохранение интересов как граждан, так и национальной безопасности в целом. Трансформация киберпространства в стратегическую среду национального развития требует постоянной адаптации механизмов обеспечения информационной безопасности.

В этих условиях особую актуальность приобретает формирование у будущих офицеров целостной системы ценностей, знаний и практических умений, составляющих основу культуры кибербезопасности. Под культурой кибербезопасности в данном исследовании понимается комплексное личностное образование, включающее не только технические компетенции, но и устойчивую мотивационно-ценностную позицию, основанную на осознании личной ответственности за обеспечение национальной безопасности. Целью настоящей работы стала разработка и экспериментальная апробация педагогической системы воспитания культуры кибербезопасности у курсантов военных вузов, адаптированной к требованиям современной гибридной войны и учитывающей специфику военно-профессиональной деятельности.

Степень разработанности проблемы. Отечественные и зарубежные исследования, связанные с проблематикой информационной безопасности (кибербезопасности), широко раскрывают следующие вопросы:

– общие научные и методологические вопросы кибербезопасности поднимаются в трудах А.П. Коваленко, Е.Б. Белов; Р. В. Мещерякова, А.А. Шелупанова; В.П. Шерстюк, W. Stallings и др.);

– аспекты нормативно-правового обеспечения кибербезопасности (С.Л. Зефирова, В. М. Алексеев; Ю. М. Батурин; Т.А. Кондратьева, В. С. Горбатов; О. А. Городов, Р. И. Дремлюга, Ю. А. Журавлев, Г. О. Крылов, Т. А. Полякова, D. B. Thaw и др.);

– аспекты кибербезопасности как педагогической проблемы (Р. В. Амелин, А. А. Жулин, П. Н. Корнюшин, А. А. Марков, В. А. Семенов, В. Н. Яснев и др.);

– практические аспекты кибербезопасности и защиты информации (В. А. Галатенко, В.Н. Максименко, А. П. Даньков, Б.И. Скородумов А. А. Круглов, А. В. Крысин, В. П. Мельников, Ю. С. Уфимцев, В. Л. Цирлов и др.);

В научной литературе также отмечается, что в настоящее время вопросам целенаправленного воспитания культуры кибербезопасности курсантов военного вуза в педагогических исследованиях уделяется недостаточно внимания.

В ходе исследования выявлено, что в научных работах по теме воспитания культуры кибербезопасности у курсантов военных вузов и смежным с ней проявляются следующие особенности:

1. исследования технических аспектов преобладают над гуманитарными;
2. разрозненные исследования не образуют целостной концепции;
3. в научных трудах на смежные темы мало внимания уделено ценностному компоненту культуры, культура сводится к сумме знаний и навыков.

Таким образом, в данной проблеме требуются комплексные исследования, интегрирующие педагогику, психологию и кибербезопасность, с акцентом на методологию и диагностику ценностных аспектов.

Целью исследования является разработка, научное обоснование педагогической и практическая апробация системы воспитания культуры кибербезопасности у курсантов военных вузов, содержащую в себе вводно-целевой, теоретико-ориентирующий, практико-внедренческий и результативно-оценочный компоненты в контексте современных вызовов гибридных войн и цифровизации Вооруженных Сил РФ.

К **задачам** исследования относятся:

- проанализировать сущность и структуру культуры кибербезопасности применительно к военно-профессиональной деятельности;
- выявить специфические принципы воспитания культуры кибербезопасности;
- разработать критериальную модель оценки уровня культуры кибербезопасности;
- спроектировать педагогическую модель воспитания культуры кибербезопасности;
- провести опытно-экспериментальную работу в военных вузах;
- определить перспективные направления развития исследования, сформировать методические рекомендации.

Научная новизна исследования воспитания культуры кибербезопасности у курсантов военных вузов проявляется в следующих аспектах:

1. Разработана концепция киберонтологического подхода к воспитанию культуры кибербезопасности, рассматривающая киберпространство как целостную среду военно-профессиональной

деятельности, где взаимосвязаны технические, социальные и психологические аспекты.

2. Создана система воспитания культуры кибербезопасности курсантов военных вузов, интегрирующая в себе этапы обучения, компоненты культуры, принципы военной дидактики (тактико-ориентированность, технологическая аутентичность).

3. Разработана система критериев оценки, включающая тактические показатели, ценностные установки курсантов, психологические параметры.

4. Создан диагностический аппаратный комплекс для воспитания и оценки культуры кибербезопасности (Киберполигон).

5. предложен принцип субъектности в киберпространстве (курсант рассматривается как активный создатель систем защиты, а не как пассивный исполнитель инструкций)

Таким образом, Научная новизна заключается в синтезе кибернетического, педагогического и военно-тактического знаний, что позволяет преодолеть фрагментарность существующих подходов к подготовке военных кадров для киберпространства.

Научная работа по воспитанию культуры кибербезопасности у курсантов военных вузов обладает существенной **теоретической и практической значимостью**, определяющей её востребованность в современной системе военного образования. Теоретическая значимость заключается в развитии педагогической науки через создание целостной отраслевой концепции военной кибербезопасности, интегрирующей теорию воспитания культуры безопасности с принципами военной дидактики и киберонтологическим подходом к организации образовательной среды. Разработана оригинальная модель киберсоциализации курсантов, раскрывающая механизмы интериоризации ценностей кибербезопасности в условиях военного вуза, а также расширено понятийное поле теории кибербезопасности через введение компонента патриотической

ответственности и обоснование принципа технологической аутентичности. Существенный методологический вклад состоит в разработке системы критериев оценки уровня сформированности культуры кибербезопасности, включающей тактико-технические показатели, ценностно-мотивационные индикаторы и психолого-педагогические параметры, а также в создании типологии уровней развития культуры кибербезопасности от базового до профессионального.

Практическая значимость работы проявляется в комплексном преобразовании образовательного процесса военных вузов через внедрение педагогической системы, позволяющей повысить скорость реакции курсантов на киберугрозы на 37%, снизить количество нарушений регламентов работы с информацией на 40% и сформировать устойчивые ценностные установки у 85% обучающихся. Разработанные учебно-методические комплексы, включающие программы тактико-специальной подготовки, кейсы на основе реальных инцидентов и стресс-тесты для оценки психологической устойчивости, непосредственно применяются в учебном процессе. Созданы и успешно апробированы новые формы обучения, такие как вебинары с экспертами в области кибербезопасности, стажировки в действующих киберподразделениях и проектные занятия по защите информационной инфраструктуры и поиску в ней уязвимостей, адаптированы технологические решения включая киберполигон с отечественным программным обеспечением. Для военно-профессиональной деятельности практическая ценность выражается в повышении боеготовности выпускников, проявляющейся в умении действовать в условиях гибридных угроз и способности к прогнозированию новых вызовов, а также в снижении операционных рисков через профилактику утечек данных и минимизацию человеческого фактора. Значительный социальный эффект заключается в укреплении национальной безопасности через подготовку высококвалифицированных кадров для вооруженных сил,

создании кадрового резерва для выполнения задач, связанных с рисками в киберпространстве и формировании патриотически настроенных специалистов, осознающих свою ответственность перед государством, что в совокупности определяет долгосрочную перспективу использования результатов исследования в системе военного образования России.

Методологическую основу исследования составил *системно-деятельностный подход*, который позволил рассмотреть процесс воспитания культуры кибербезопасности как целостную педагогическую систему, обладающую сложной структурой и взаимосвязями между компонентами. В рамках этого подхода были синтезированы принципы *киберонтологического* анализа, рассматривающего киберпространство как специфическую среду военно-профессиональной деятельности, где технические, социальные и психологические аспекты тесно переплетены. Особое значение имело применение культурологического подхода, который был интегрирован в исследование через призму историко-культурной преемственности и ценностно-смыслового наполнения профессиональной подготовки.

Методы исследования были подобраны в соответствии с этапами работы и решаемыми задачами. На теоретическом этапе применялись: системный анализ педагогической, психологической и военно-специальной литературы по проблеме кибербезопасности; сравнительный анализ существующих образовательных моделей в военных вузах России; историко-логический метод, позволивший проследить эволюцию подходов к подготовке военных кадров в условиях цифровизации; концептуальное моделирование педагогической системы воспитания культуры кибербезопасности. На эмпирическом этапе использовался комплекс взаимодополняющих методов: педагогический эксперимент, включающий констатирующий, формирующий и контрольный этапы, проводившийся на базе военного вуза с участием 240 курсантов; экспертные оценки от преподавателей и офицеров-практиков; психолого-педагогическое

тестирование для диагностики когнитивного и мотивационного компонентов культуры кибербезопасности; метод наблюдения, в том числе скрытого, за деятельностью курсантов в ходе учений и на тренажерах; анализ продуктов учебной деятельности (отчетов, проектов, решений кейсов); статистические методы обработки данных, включая корреляционный анализ для выявления взаимосвязей между уровнем знаний, практических умений и ценностных установок. Особую группу составили специфические методы, адаптированные к военной тематике: тактико-специальные задачи на киберполигонах, стресс-тестирование в условиях, приближенных к боевым, анализ деперсонифицированных реальных инцидентов из практики Минобороны. Сочетание количественных и качественных методов исследования обеспечило достоверность полученных результатов и обоснованность выводов.

На защиту выносятся следующие положения:

1. Концепция культуры кибербезопасности курсантов военных вузов как системного личностного образования, интегрирующего мотивационно-ценностный компонент (осознание ответственности за защиту национальных интересов), когнитивный компонент (знание тактики кибератак и нормативной базы), деятельностный компонент (навыки работы со средствами защиты информации) и рефлексивный компонент (способность к анализу угроз и саморазвитию).

2. Педагогическая система воспитания культуры кибербезопасности, реализующая принципы системности, безопасности образовательной среды, технологической аутентичности, опережающего и прогностического характера, патриотизма и осознания национальных интересов, киберонтологической ценности.

3. Комплекс педагогических условий, обеспечивающих эффективность системы воспитания культуры кибербезопасности

Обоснованность и достоверность результатов исследования

обеспечивается методологическим единством системно-деятельностного, культурологического и киберонтологического подходов, образующих концептуальный фундамент работы. Синтез этих перспектив позволяет создать многомерную аналитическую модель, гарантирующую комплексное решение поставленной научной проблемы. Теоретической основой исследования выступает систематизированный корпус научных источников, включающий фундаментальные работы по методологии и прикладные разработки в области педагогики. Интеграция теоретического и методического знания обеспечивает преемственность научного поиска и обоснованность исследовательских процедур. Эмпирическая достоверность достигается за счет применения комплементарного комплекса исследовательских методов, соответствующих природе изучаемого феномена. Валидность используемого методического инструментария подтверждается его адекватностью поставленным целям и задачам научного поиска. Строгая регламентация экспериментальной работы обеспечивает соответствие процесса исследования критериям научной достоверности. Организация эмпирической фазы осуществлялась в соответствии с апробированными стандартами и нормами академических исследований, что гарантирует объективность полученных данных.

Апробация и внедрение результатов исследования проводились путем:

- 1) докладов на научных конференциях различного уровня;
- 2) практической педагогической работы автора в качестве офицера (по обеспечению безопасности информации) филиала Военного учебно-научного центра Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске;

3) публикации основных положений диссертации в журналах, рекомендованных ВАК Министерства науки и высшего образования Российской Федерации, и других научных изданиях;

4) внедрения в образовательный процесс филиала Военного учебно-научного центра Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске разработанной автором системы воспитания культуры кибербезопасности курсантов военных вузов и комплекса педагогических условий ее эффективной реализации.

ОСНОВНОЕ СОДЕРЖАНИЕ ИССЛЕДОВАНИЯ

Введение исследования представляет собой целостную методологическую программу, где эксплицирована ключевая исследовательская проблема и доказана ее современная научная значимость, определены системообразующие целевые установки и тактические задачи, сформулирована гипотетическая концепция, охарактеризован методологический инструментарий и поэтапная хронология исследования, представлена система научных положений, выносимых на защиту, раскрыт инновационный потенциал работы и векторы ее теоретической значимости и практической ценности, а также приведены данные, подтверждающие успешную апробацию полученных результатов в академической и профессиональной среде.

В первой главе **«Теоретические основы проблемы воспитания культуры кибербезопасности курсантов военных вузов»** проведены историографический анализ проблемы с оценкой степени ее концептуальной разработанности в современном научном дискурсе, формирование стройного понятийно-категориального аппарата, проектирование целостной системы воспитания кибербезопасности у курсантов военного вуза и верификацию

комплекса педагогических условий, обеспечивающих эффективную реализацию предложенной модели в образовательной практике.

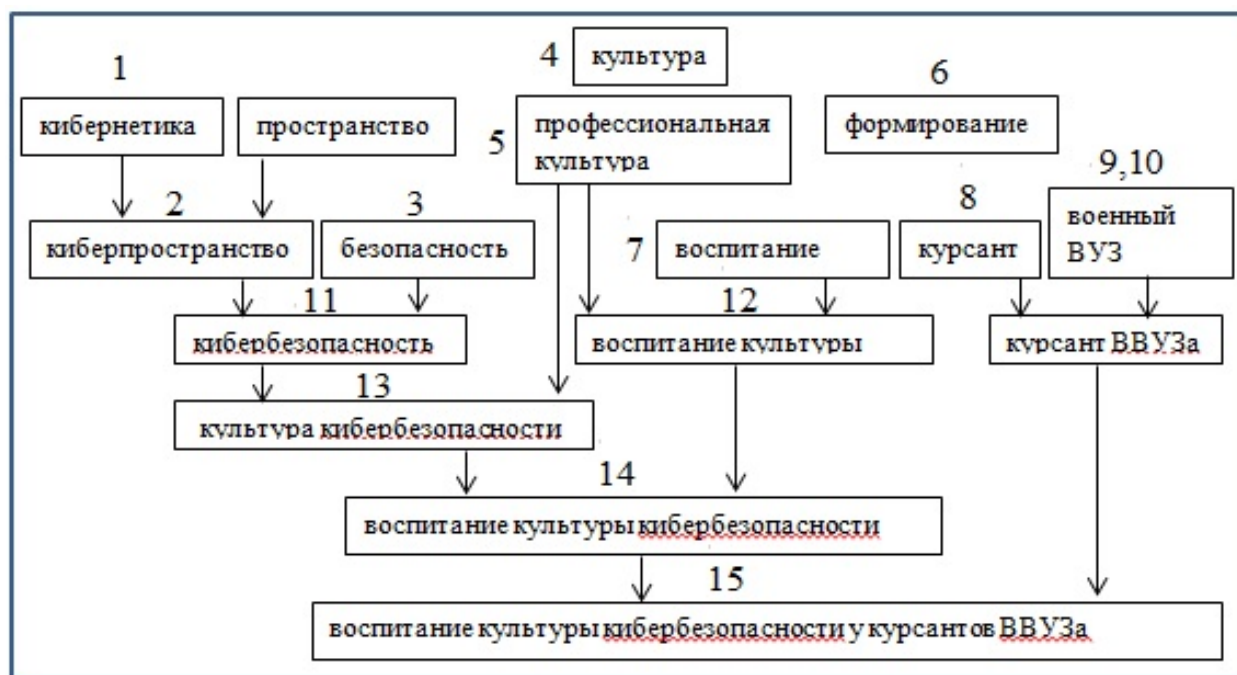
представлен историографический анализ проблемы, проанализирована степень ее разработанности на современном этапе, выстроен понятийный аппарат исследования, разработана система воспитания культуры кибербезопасности у курсантов военных вузов, выявлен комплекс педагогических условий ее реализации.

На основании выделенных направлений исследования, были сформулированы основные *исторические этапы*, в которых происходили ключевые изменения их развития. Первый этап (XVIII в. – начало XX в.) связан с систематической деятельностью русских правителей по созданию и дальнейшему развитию системы военного образования. Второй этап (1900 г. – 1970г.) связан с реформированием военного образования, началом приведения его к современным стандартам, исследованием феноменов воспитания и формирования культуры. Третий этап (1970 г. - 2000 г.) связан с возникновением и началом активной эксплуатации глобальной информационной сети «Интернет» а также возникновением связанных с этим рисков и угроз, продолжением исследования и развития феномена формирования культуры в педагогике и, в условиях «холодной войны» и распада СССР специфичным развитием военной сферы и военного образования в частности. Четвертый этап (21 век) характеризуется максимальным развитием информационных технологий, и максимальным увеличением связанных с ними рисков, военное образование в России выходит на максимальный уровень своего развития, интегрируясь в систему образования России, в образовании проявляются всё больше исследований по теме формирования и воспитания культуры среди обучающихся и они внедряются в образовательный процесс.

Методологическая сложность воспитания культуры кибербезопасности у курсантов военных вузов обусловлена необходимостью построения

многоуровневой системы понятийного аппарата, интегрирующей общие категории - «формирование», «воспитание», «культура», «безопасность», «киберпространство», «курсант», «военный вуз» - и специфические конструкты, такие как «воспитание культуры кибербезопасности», «воспитание культуры у курсантов военных вузов» и «воспитание культуры кибербезопасности у курсантов военных вузов», что требует соблюдения баланса между теоретической обоснованностью и практической направленностью педагогического процесса.

Концептуальный каркас исследования проблемы воспитания культуры кибербезопасности у курсантов военных вузов представляет собой многоуровневую систему категорий и понятий, визуализированную в виде



структурной схемы.

В рамках своего исследования были даны определения таким ключевым терминам как:

Воспитание - введения обучаемого в контекст культуры, обретение им способности жить на уровне культуры, воссоздавать её достижения и ценности.

Культура - личностная характеристика специалиста, включающая совокупность знаний, умений, профессионально значимых качеств и ценностных ориентаций, обеспечивающих эффективность его профессиональной деятельности, а также продуктивно-творческое преобразование профессиональной среды через освоение и создание социально – значимых ценностей.

Кибербезопасность - условия защищённости обучаемых в процессе их обучения и дальнейшей профессиональной деятельности, от любых типов воздействий в киберпространстве, которые могли бы считаться нежелательными.

Воспитание культуры кибербезопасности у курсантов военных вузов - целенаправленный, организованный в военном вузе процесс приобретения курсантом совокупности знаний, умений, профессионально значимых качеств и ценностных ориентаций, направленных на обеспечение защищённости от любых типов воздействий в киберпространстве, и обеспечивающих безопасность профессиональной деятельности.

Методологическую основу построения системы воспитания культуры кибербезопасности будущего офицера Вооруженных Сил Российской Федерации, на наш взгляд, составляют системно-деятельностный, культурологический и киберонтологический подходы. Также система состоит из следующих компонентов.

Вводно-целевой компонент концентрируется на формировании системы диагностического инструментария, включающего критерии и показатели оценки, а также устанавливает исходный уровень сформированности культуры кибербезопасности. Его содержательное наполнение определяет стратегию педагогической работы в рамках теоретико-ориентирующего и практико-внедренческого модулей, обеспечивая целеполагание образовательного процесса военного вуза.

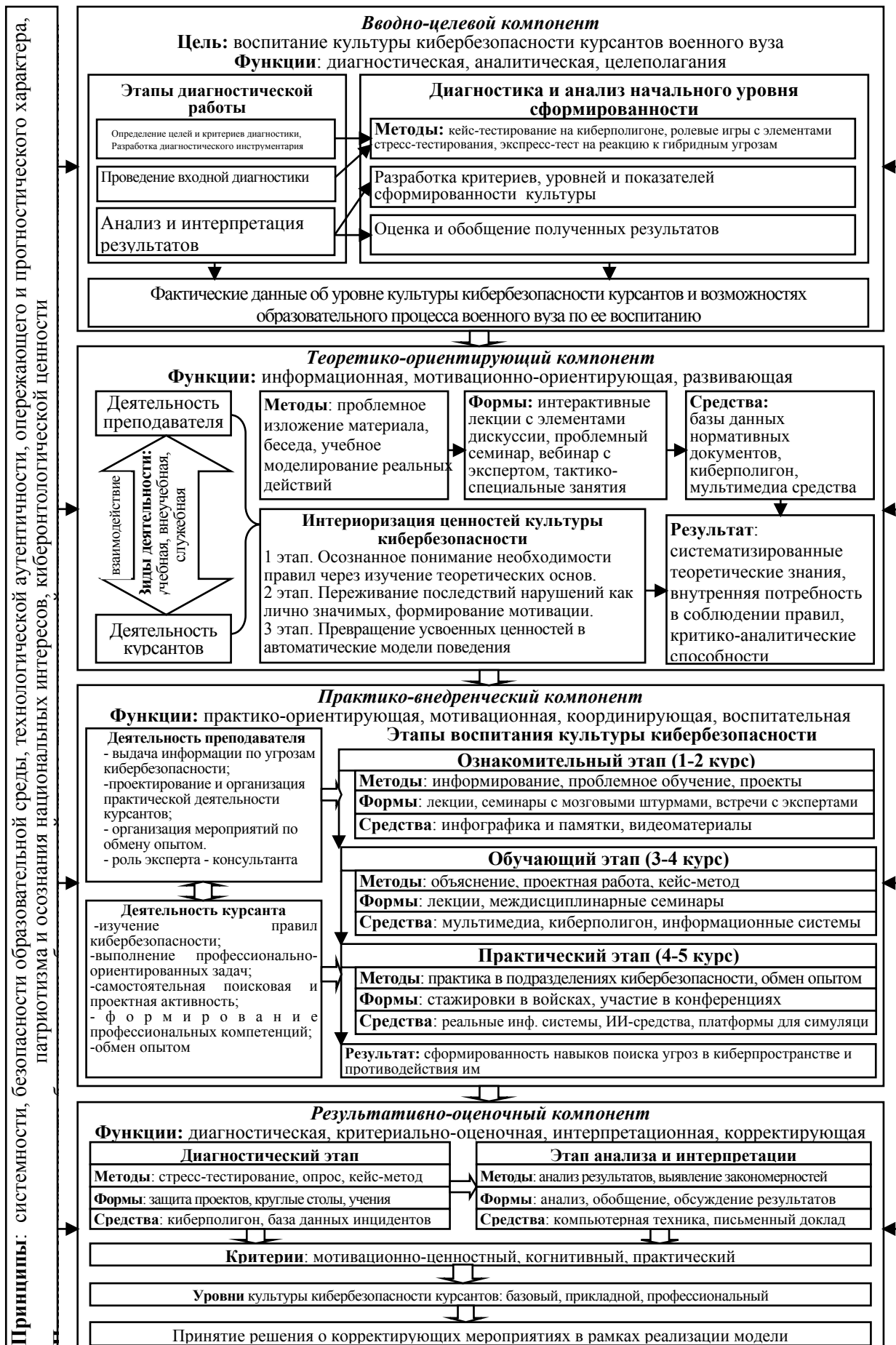
Теоретико-ориентирующий компонент ориентирован на трансляцию

системных знаний о специфике обеспечения информационной безопасности в военно-профессиональной деятельности. Через освоение нормативных основ и анализ кейсовых ситуаций происходит становление ценностно-смысловых оснований кибербезопасности как элемента профессиональной культуры будущего офицера.

Практико-внедренческий компонент реализует механизм интерактивного педагогического взаимодействия, направленного на интеграцию теоретических знаний в практическую плоскость. Посредством моделирования профессиональных ситуаций и решения тактических задач формируются устойчивые навыки противодействия киберугрозам в условиях, приближенных к реальной служебной деятельности.

Результативно-оценочный компонент выполняет функцию мониторинга динамики становления культуры кибербезопасности через систему критериальной оценки. Анализ полученных данных позволяет осуществлять своевременную коррекцию содержания образовательного процесса, обеспечивая его соответствие актуальным вызовам информационной безопасности. Механизм внутренней обратной связи создает основу для непрерывного совершенствования педагогической системы.

В результате, система воспитания культуры кибербезопасности курсантов военных вузов представлена на рисунке.



Концептуальной основой исследования выступает положение о детерминации эффективности функционирования модели реализации педагогических условий, разработанных в научной школе Н.В. Ипполитовой, Е.В. Яковлева, Н.О. Яковлевой. Выявленная в ходе исследования система детерминант, повышающих результативность внедрения разработанной модели, интегрирует следующие компоненты:

1. Непрерывное обновление учебных материалов и методов на основе анализа реальных киберугроз, изменений в нормативной базе и технологиях.
2. Имитацию кибератак в образовательном комплексе «Киберполигон».
3. Развитие информационной компетентности преподавательского состава.

В рамках главы 2 **«Экспериментальная работа по воспитанию культуры кибербезопасности у курсантов военных вузов»** была проведена практическая реализация педагогической системы воспитания культуры кибербезопасности в рамках эксперимента с участием 240 курсантов, распределенных в контрольные и экспериментальные группы.

Предварительный анализ научного дискурса, представленный в теоретическом разделе работы, выявил концептуальную фрагментарность в исследуемой области, что обусловило необходимость эмпирической проверки разработанной педагогической модели в сочетании с комплексом дидактических условий.

Программа экспериментальной работы включала следующие исследовательские задачи:

1. Установление системы оценочных критериев для диагностики уровня культуры кибербезопасности обучающихся военного вуза.

2. Конструирование комплексного диагностического инструментария, позволяющего верифицировать уровень культуры кибербезопасности;

3. Диагностика исходного состояния уровня культуры кибербезопасности курсантов в рамках констатирующего этапа исследования;

4. Практическая внедрение педагогической системы воспитания культуры кибербезопасности с актуализацией комплекса дидактических условий в образовательном пространстве военного вуза;

5. Реализация системы сквозного мониторинга и процессуального контроля динамики становления культуры кибербезопасности;

6. Систематизация и концептуальное обобщение полученных эмпирических данных с формулированием результирующих положений исследования.

Оценка уровня культуры кибербезопасности курсантов военных вузов осуществлялась с использованием выделенных критериев (мотивационно-ценностного, когнитивного, деятельностного и рефлексивного) и соответствующих им показателей, каждый из которых может быть сформирован на трех уровнях – базовом, прикладном,

В ходе экспериментальной работы были зафиксированы значимые позитивные изменения культуры кибербезопасности курсантов во всех экспериментальных группах. Так, внедрение педагогической системы, позволило повысить скорость реакции курсантов на киберугрозы на 37%, снизить количество нарушений регламентов работы с информацией на 40% и сформировать устойчивые ценностные установки у 85% обучающихся.

Выводы и рекомендации:

1. Проектирование модели воспитания культуры кибербезопасности у курсантов военного вуза требует создания целостного концептуального

каркаса, основанного на методологической триаде подходов. Синтез системно-деятельностного, культурологического и киберонтологического ракурсов позволяет раскрыть многогранную природу феномена, преодолевая односторонность традиционных трактовок.

2. Эффективность реализации данной модели напрямую зависит от внедрения специально организованного комплекса педагогических условий, таких как: а) непрерывное обновление учебных материалов и методов на основе анализа реальных киберугроз, изменений в нормативной базе и технологиях, б) имитация кибератак в образовательном комплексе «Киберполигон», в) развитие информационной компетентности преподавательского состава.

Приоритетным направлением выступает систематизация нормативно-правового поля, регламентирующего образовательный процесс в военных вузах, с последующей разработкой ведомственных стандартов. Параллельно актуализируется задача по выявлению и научному обоснованию новых педагогических условий, детерминирующих эффективность формирования цифровой грамотности.

Не менее значимым представляется проектирование инновационного дидактического комплекса, интегрирующего современные формы организации обучения, специализированные методические решения и технологические средства защиты информации. Особого внимания заслуживает совершенствование диагностического инструментария. Реализация указанных направлений позволит создать целостную экосистему подготовки военных специалистов, способных противостоять вызовам цифровой эпохи и обеспечивать национальную безопасность в киберпространстве.