

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

ОДОБРЕНО
Учебно-методический совет
университета
Протокол № 5 от 16.04.2026

УТВЕРЖДАЮ
Проректор по учебной работе
_____Максимович С.А.
«__» _____ 2026 .

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ
по направлению подготовки
09.04.03 «Прикладная информатика»

_____ (шифр и наименование направления подготовки)

Искусственный интеллект в кибербезопасности

_____ (профиль подготовки)

Магистр

_____ (Квалификация (степень) выпускника)

Очная, заочная

_____ (форма обучения)

Ставрополь, 2026

Программа государственной итоговой аттестации разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки высшего образования – магистратуры по направлению подготовки 09.04.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 года № 916.

Программа ГИА рассмотрена на заседании учебно-методической комиссии факультета цифровых технологий, протокол № 2 от 08.04.2026 г.

1. Общие положения

Заключительным этапом учебной подготовки магистров, обучающихся по направлению подготовки 09.04.03 «Прикладная информатика» (магистерская программа «Искусственный интеллект в кибербезопасности»), являются аттестационные испытания, включающие подготовку к сдаче и сдачу государственного экзамена и подготовку к защите и процедуру защиты выпускной квалификационной работы (магистерской диссертации) по утвержденной тематике и выполненной в установленные календарным планом сроки.

Государственная итоговая аттестация выпускников Ставропольского государственного аграрного университета проводится в соответствии с:

Федеральным законом Российской Федерации «Об образовании в Российской Федерации» от 29 декабря 2012 года № 273-ФЗ;

Приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

Приказом Министерства образования и науки Российской Федерации от 29 июня 2015 года № 636 «Об утверждении порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры»;

Федеральным государственным образовательным стандартом высшего образования – магистратуры по направлению подготовки 09.04.03 «Прикладная информатика», утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 916;

Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры в ФГБОУ ВО Ставропольский ГАУ;

Положением о выполнении и защите выпускной квалификационной работы в ФГБОУ ВО Ставропольский ГАУ.

2. Цель и задачи государственной итоговой аттестации

Целью государственной итоговой аттестации является установление уровня подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям государственного образовательного стандарта по направлению подготовки 09.04.03 «Прикладная информатика» (уровень магистратуры).

В задачи государственной итоговой аттестации входит:

проверка уровня сформированности компетенций, определенных федеральным государственным образовательным стандартом и ОПОП ВО по направлению подготовки 09.04.03 «Прикладная информатика»;

принятие решения о присвоении квалификации по результатам ГИА и выдаче документа о высшем образовании и присвоении квалификации «Магистр».

3. Место государственной итоговой аттестации в структуре ОП ВО

Государственная итоговая аттестация является базовой составляющей блока Б3 учебного плана и состоит из двух разделов:

Б3.01(Г) Подготовка к сдаче и сдача государственного экзамена

Б3.02(Д) Подготовка к процедуре защиты и защита выпускной квалификационной работы.

4. Формы и объем государственной итоговой аттестации

Государственная итоговая аттестация выпускников направления 09.04.03 «Прикладная информатика» магистерская программа «Искусственный интеллект в кибербезопасности» в Ставропольском государственном аграрном университете состоит из аттестационных испытаний следующих видов:

- государственный экзамен;
- защита выпускной квалификационной работы (магистерской работы).

Государственный экзамен является междисциплинарным и проводится по нескольким дисциплинам образовательной программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности обучающихся. Государственный экзамен проводится устно.

Выпускная квалификационная работа выполняется в форме магистерской работы - это самостоятельно выполненная работа, содержащая теоретическое обоснование и (или) производственно-технологическое исследование, решение профессиональных задач по соответствующему направлению.

Объем государственной итоговой аттестации – 9 з.е. (6 недель), в которые входит подготовка к сдаче и сдача государственного экзамена, а также подготовка к защите и процедура защиты выпускной квалификационной работы.

5. Подготовка к сдаче и сдача государственного экзамена

5.1. Результаты освоения ОП ВО

Государственный экзамен носит комплексный характер. Он включает проверку теоретических знаний обучающихся и практических умений самостоятельно осуществлять научную деятельность. Экзамен проводится в устной форме.

На государственном экзамене проверяется сформированность следующих компетенций:

Код компетенции	Код индикатора	Содержание	Результаты освоения ОП ВО
УК-1		Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Знать: методы системного анализа, принципы выработки стратегий в области ИБ и ИИ.
			Уметь: анализировать проблемные ситуации в проектах по ИИ и ИБ, формулировать цели и задачи исследований.
			Владеть: навыками разработки стратегий достижения целей с учетом рисков и ресурсных ограничений.
УК-2		Способен управлять проектом на всех этапах его жизненного цикла	Знать: методологии управления проектами (Agile, Scrum, Kanban), инструменты (Jira, Redmine).
			Уметь: разрабатывать концепцию и ТЭО проекта, составлять календарные планы и распределять ресурсы.
			Владеть: навыками контроля выполнения этапов проекта и оценки достигнутых результатов.
УК-3		Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной	Знать: принципы командной работы, методы разрешения конфликтов и мотивации.
			Уметь: определять роли и распределять задачи в команде, организовывать эффективные коммуникации.
			Владеть: навыками руководства командой и организации совместной работы над проектами.

		цели	
ОПК-1	ОПК-1.1	Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач	<i>Знать:</i> математические методы (теория вероятностей, статистика), методы машинного обучения и криптографии.
			<i>уметь:</i> формализовать прикладные задачи (обнаружение аномалий, анализ угроз) на языке математики и информатики.
			<i>владеть:</i> методами поиска и критического анализа научно-технической информации.
ОПК-2	ОПК-2.1	Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий	<i>знать:</i> алгоритмы обработки данных и принятия решений с элементами ИИ (нейронные сети, деревья решений).
			<i>уметь:</i> реализовывать алгоритмы в виде программного кода на Python, Java, C++.
			<i>владеть:</i> библиотеками машинного обучения (scikit-learn, TensorFlow, PyTorch) и фреймворками для кибербезопасности (Snort, Suricata).
ОПК-3	ОПК-3.1	Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	<i>знать:</i> источники информации об угрозах и уязвимостях (CVE, MITRE ATT&CK).
			<i>уметь:</i> систематизировать данные об инцидентах, составлять аналитические отчёты с графиками и таблицами.
			<i>владеть:</i> навыками формулирования практических рекомендаций по повышению уровня защищённости.
ОПК-5	ОПК-5.1	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информации	<i>знать:</i> архитектуру программных средств защиты информации, требования к производительности и масштабируемости.
			<i>уметь:</i> интегрировать программные модули (антивирус, DLP, SIEM) в единую систему.
			<i>владеть:</i> навыками настройки аппаратных

		ционных и автоматизированных систем	средств защиты (межсетевые экраны, криптошлюзы).
ОПК-7	ОПК-7.1	Способен разрабатывать и применять математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	<i>знать:</i> математические модели угроз (графовые, вероятностные, игровые).
			<i>уметь:</i> проводить имитационное моделирование поведения нарушителя и эффективности защиты.
			<i>владеть:</i> методами интерпретации результатов моделирования для оптимизации конфигурации ИС.
ПК-1	ПК-1.1	Способен проводить анализ безопасности компьютерных систем с применением методов искусственного интеллекта и машинного обучения	<i>знать:</i> методы сканирования уязвимостей (Nessus, OpenVAS) и алгоритмы кластеризации логов.
			<i>уметь:</i> разрабатывать и тестировать модели машинного обучения для обнаружения сетевых атак (DDoS, APT).
			<i>владеть:</i> навыками интерпретации результатов мониторинга защищенности и формирования научно обоснованных заключений.
ПК-3	ПК-3.1	Способен разрабатывать, модернизировать и сопровождать программное обеспечение информационных систем с использованием технологий искусственного интеллекта	<i>знать:</i> принципы защитного программирования, методологию DevOps.
			<i>уметь:</i> писать программный код на Python, C++, Go, интегрировать готовые модули ИИ.
			<i>владеть:</i> средствами отладки, рефакторинга и документирования программных интерфейсов.
ПК-5	ПК-5.1	Способен администрировать средства защиты информации и обеспечивать безопасность информационных систем	<i>знать:</i> методы установки и настройки СКЗИ, межсетевых экранов, антивирусного ПО.
			<i>уметь:</i> реализовывать политики управления доступом и мониторинга событий безопасности.
			<i>владеть:</i> навыками анализа корректности функционирования средств защиты и оперативного устранения неисправностей.

5.2. Содержание государственного экзамена
Содержание государственного экзамена должно соотноситься с результатами освоения ОП ВО

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Код компетенции
Блок дисциплин обязательной части			
Основы биотехнологии			
1.	Современные интеллектуальные системы и технологии	Архитектура интеллектуальных систем. Нейронные сети и глубокое обучение. Обработка естественного языка. Компьютерное зрение. Применение ИИ в АПК и кибербезопасности. Этические и правовые аспекты использования ИИ.	УК-1, ОПК-2, ПК-3
2.	Математическое и имитационное моделирование	Методы моделирования сложных систем. Вероятностные и статистические модели. Имитационное моделирование (Agent-based modeling). Моделирование угроз и поведения нарушителя. Применение математических моделей для прогнозирования инцидентов.	УК-1, ОПК-1, ОПК-7
3	Машинное обучение в кибербезопасности	Обучение с учителем и без учителя. Методы обнаружения аномалий и атак (кластеризация, классификация). Анализ сетевого трафика с использованием ML. Обнаружение вредоносного ПО с помощью ML. Борьба с атаками на системы ИИ (adversarial attacks).	ОПК-2, ПК-1, ПК-5
4.	Технологии разработки защищенного ПО	Принципы разработки безопасных приложений (Security by Design). Анализ уязвимостей кода (SAST, DAST). Технологии CI/CD для безопасной разработки. Управление конфигурациями и релизами.	ОПК-5, ПК-3
Блок дисциплин вариативной части и дисциплин по выбору			
5.	Инструментальный анализ защищённости и тестирование на проникновение	Методология пентеста. Сканеры уязвимостей (Nessus, OpenVAS). Инструменты анализа защищённости веб-приложений и сетей. Социальная инженерия. Формирование отчётов о тестировании на проникновение.	ПК-1, ПК-5
6.	Прикладные системы искусственного интеллекта	Прикладные системы ИИ в кибербезопасности: SIEM-системы с элементами ИИ, системы обнаружения вторжений (IDS/IPS) на основе ML. Автоматизация реагирования на инциденты (SOAR). Использование ИИ для анализа вредоносного ПО.	ОПК-2, ПК-3
7.	Управление информационной безопасностью	Политики безопасности. Модели управления доступом. Организация мониторинга событий безопасности. Разработка планов реагирования на инциденты. Оценка рисков ИБ.	УК-2, ПК-5

7	Инженерия требований к безопасным системам	Сбор и анализ требований к безопасным системам. Разработка технического задания на проектирование систем защиты. Управление требованиями на протяжении жизненного цикла. Методологии (Agile, Waterfall) в проектах ИБ.	УК-2, УК-3, ОПК-5
---	--	--	-------------------

5.3. Фонд оценочных средств государственной итоговой аттестации (государственный экзамен)

5.3.1. Типовые контрольные задания или иные материалы, необходимые для оценки результатов образовательной программы

Примерный перечень вопросов для итогового государственного экзамена по направлению подготовки 09.04.03 «Прикладная информатика» профиль «Искусственный интеллект в кибербезопасности»

Блок обязательной части (Б1.О):

1. Архитектура искусственных нейронных сетей: полносвязные, сверточные, рекуррентные сети.
2. Методы обнаружения аномалий в сетевом трафике с использованием машинного обучения.
3. Применение методов имитационного моделирования для анализа защищённости компьютерных систем.
4. Анализ уязвимостей кода при помощи статических анализаторов (SonarQube, PVS-Studio).
5. Понятие «состязательная атака» на системы ИИ и методы защиты от них.
6. Архитектура SIEM-систем и их роль в мониторинге событий информационной безопасности.
7. Алгоритмы кластеризации (k-means, DBSCAN) для выявления аномальных сетевых соединений.
8. Методология управления проектами Agile и Scrum в разработке систем защиты информации.
9. Модели угроз (уровневые, графовые) и методы их формализации.
10. Принципы разработки безопасного ПО (Secure Development Lifecycle – SDL).

Блок вариативной части (Б1.В):

11. Методология тестирования на проникновение (пентест): этапы, инструменты, документирование.
12. Использование методов машинного обучения для обнаружения вредоносного ПО (malware detection).
13. Принципы построения систем обнаружения вторжений (IDS/IPS) на основе нейросетей.
14. Управление конфигурациями и версиями ПО (Git, CI/CD) в проектах по кибербезопасности.
15. Интеграция средств защиты (антивирус, DLP, межсетевой экран) в корпоративную ИТ-инфраструктуру.
16. Анализ рисков информационной безопасности: качественные и количественные методы.

17. Разработка политик управления доступом (RBAC, ABAC) для информационных систем.
18. Использование ИИ для анализа и классификации вредоносных ссылок и фишинговых писем.
19. Методы оценки эффективности систем обнаружения атак (метрики: Accuracy, Precision, Recall, F1-score).
20. Инженерия требований к системам защиты информации (ГОСТ, стандарты ФСТЭК).

**Примерный перечень практико-ориентированных заданий для
государственного экзамена по направлению подготовки
09.04.03 «Прикладная информатика» профиль «Искусственный интеллект в кибер-
безопасности»**

1. Разработать блок-схему алгоритма обнаружения DDoS-атаки на основе метода кластеризации трафика.
2. Написать фрагмент кода на Python для загрузки модели машинного обучения из библиотеки Scikit-learn и её применения к тестовому набору данных.
3. Составить план тестирования на проникновение для веб-приложения, включая этапы сбора информации, сканирования и эксплуатации уязвимостей.
4. Проанализировать лог-файл сервера и определить признаки компрометации (индикаторы атак).
5. Разработать концептуальную модель угроз для информационной системы предприятия (на выбор: банк, сельхозпредприятие, университет).
6. Подобрать инструменты (Nessus, Wireshark, Metasploit) для конкретных этапов пентеста и обосновать выбор.
7. Рассчитать метрики качества модели классификации (Confusion Matrix, Accuracy, Precision, Recall) по заданным данным.
8. Составить техническое задание на разработку модуля анализа сетевого трафика с применением ИИ.

По вопросам к государственному экзамену и практико-ориентированным заданиям составляется 30 экзаменационных билетов.

5.3.2. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Государственный экзамен по направлению подготовки 09.04.03 «Прикладная информатика» профиль «Искусственный интеллект в кибербезопасности» проводится в устной форме в виде итогового междисциплинарного экзамена с учетом общих требований к выпускнику, предусмотренных федеральным государственным образовательным стандартом.

К государственной экзамену допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по осваиваемой образовательной программе высшего образования.

Перед государственным экзаменом проводится консультирование обучающихся по вопросам, включенным в программу государственного экзамена (далее – предэкзаменационная консультация).

Государственный экзамен проводится по билетам, утвержденным директором института ветеринарии и биотехнологий. Экзаменационные билеты разрабатываются на основании программы государственного экзамена по направлению подготовки 09.04.03 «Прикладная информатика» профиль «Искусственный интеллект в кибербезопасности» в полном соответствии с реализуемыми учебными программами изучаемых дисциплин. Каждый экзаменационный билет содержит 2 теоретических вопроса и одно практико-ориентированное задание.

Государственный экзамен принимает государственная экзаменационная комиссия, состав которой утверждается приказом по университету.

После того, как выпускник берет экзаменационный билет, ему предоставляется от 30 до 60 минут для подготовки к ответу.

После подготовки выпускник в устной форме представляет членам государственной экзаменационной комиссии результат выполнения задания, отвечает на уточняющие вопросы членов ГЭК.

Члены государственной экзаменационной комиссии в устной форме могут задавать вопросы по содержанию представленного ответа.

На закрытом заседании членов государственной экзаменационной комиссии принимается решение об оценке ответа студента на государственном экзамене.

Результаты государственного экзамена определяются оценками «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Студент, получивший оценку «неудовлетворительно», считается не сдавшим государственный экзамен.

Состав балльно-рейтинговой оценки государственного экзамена:

Содержание билета	Количество баллов, max
Теоретический вопрос №1 (из блока дисциплин базовой части)	30
Теоретический вопрос № 2 (из блока дисциплин вариативной части и дисциплин по выбору)	30
Практико-ориентированное задание	30
Дополнительные вопросы по блокам 1, 2	10
Итого	100

Типовой экзаменационный билет:

Теоретический вопрос №1 (оценка знаний):

1. Методы обнаружения аномалий в сетевом трафике с использованием машинного обучения.

Теоретический вопрос №2 (оценка знаний):

2. Инженерия требований к безопасным системам на всех этапах жизненного цикла

Практико-ориентированное задание (оценка умений, навыков):

3. Дан лог-файл сетевой активности (CSV-формат) с колонками:

timestamp – время события;

src_ip – IP-адрес источника;

dst_ip – IP-адрес назначения;

bytes_sent – количество переданных байт;

packets – количество пакетов;

protocol – протокол (TCP/UDP/ICMP).

Необходимо:

- Предложить алгоритм (последовательность шагов) для выявления подозрительной активности, которая может свидетельствовать о сканировании портов или DDoS-атаке, с применением метода машинного обучения (на выбор – кластеризация или классификация).

- Описать, какие признаки (features) вы выделите из исходных данных для обучения модели.

- Написать псевдокод или блок-схему процедуры подготовки данных и обучения модели.

- Указать, какие инструменты и библиотеки вы будете использовать (например, Python + Pandas + Scikit-learn) и как интерпретировать результаты для принятия решения (например, выявление IP-адресов с аномальным поведением).

Ожидаемый результат:

Чёткая логическая схема решения задачи, обоснование выбора алгоритма, описание этапов предобработки и признакового пространства, а также сценарий практического применения результата в системе мониторинга безопасности.

Полученная на государственном экзамене сумма баллов переводится в оценку:

«отлично» – от 85 до 100 баллов;

«хорошо» – от 70 до 84 баллов;

«удовлетворительно» – от 55 до 69 баллов;

«неудовлетворительно» – менее 50 баллов.

Критерии оценки ответа на теоретические вопросы (оценка знаний)

30 баллов выставляется студенту при полном ответе на вопрос билета по данному блоку, демонстрации теоретических знаний, способности привести примеры.

20-29 баллов – дан недостаточно полный и недостаточно развернутый ответ. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.

10-19 баллов заслуживает студент, ответивший полностью и без ошибок на предложенные вопросы и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.

1-9 баллов – дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

0 баллов выставляется при полном отсутствии ответа, имеющего отношение к вопросу.

Критерии оценки результатов выполнения практико-ориентированного задания (оценка умений, навыков)

Критерии оценки ответа на теоретические вопросы:

- **30 баллов** – полный, развернутый ответ, демонстрация глубоких теоретических знаний, способность привести примеры из практики ИБ и ИИ.
- **20-29 баллов** – недостаточно полный или развернутый ответ, отдельные неточности, но в целом ответ правильный.
- **10-19 баллов** – ответ неполный, допущены существенные ошибки, но основные понятия известны.
- **1-9 баллов** – ответ фрагментарный, нелогичный, с грубыми ошибками.
- **0 баллов** – отказ от ответа.

Критерии оценки практического задания:

- **30 баллов** – задание выполнено полностью, правильно, рационально, с обоснованием.
- **20-29 баллов** – задание выполнено в основном правильно, но есть несущественные ошибки или нерациональные решения.
- **10-19 баллов** – задание выполнено частично, с ошибками, выводы неполные.
- **1-9 баллов** – задание выполнено неправильно, объем выполненной части недостаточен для выводов.
- **0 баллов** – задание не выполнено.

Итоговая оценка:

- «отлично» – от 85 до 100 баллов;
- «хорошо» – от 70 до 84 баллов;
- «удовлетворительно» – от 55 до 69 баллов;
- «неудовлетворительно» – менее 50 баллов.

5.4. Учебно-методическое и информационное обеспечение государственного экзамена

а) Основная литература

Блок обязательной части (Б1.О)

1. ЭБС «Лань» : Платонов В.В. Технологии машинного обучения в кибербезопасности : учебное пособие. – Москва ; Вологда : Инфра-Инженерия, 2024. – ISBN 978-5-9729-2048-8. – Режим доступа: <https://www.iprbookshop.ru>[reference:0]
2. ЭБС «Лань» : Фомичева С.Г. Методы машинного обучения в задачах обеспечения информационной безопасности : учеб. пособие. – Санкт-Петербург : ГУАП, 2023. – 136 с. – ISBN 978-5-8088-1822-4. – Режим доступа: <https://e.lanbook.com/book/341024>[reference:1]
3. ЭБС «Лань» : Мельников С.Ю. Искусственный интеллект и кибербезопасность : учебное пособие. – Москва : Российский ун-т дружбы народов им. Патриса Лумумбы, 2023. – 71 с.
4. ЭБС «Лань» : Основы искусственного интеллекта. Безопасность искусственного интеллекта : учебное пособие. – 2024.
5. ЭБС «Лань» : Калинин М.О. Технологии машинного обучения в кибербезопасности. Основы искусственного интеллекта : лабораторный практикум.

6. Зараменских Е.П. Управление жизненным циклом информационных систем : учебник и практикум для вузов. – 4-е изд. – Москва : Юрайт. – Режим доступа: <https://urait.ru>[reference:5]
7. ЭБС «Лань» : Стельмашонок Е.В., Стельмашонок В.Л. Методы моделирования и анализа сложных систем : учебник. – Режим доступа: <https://e.lanbook.com>[reference:6]
8. ЭБС «Лань» : Современные системы управления базами данных : учебник. – Режим доступа: <https://e.lanbook.com>[reference:7]
9. ЭБС «Лань» : Защита информационных систем. Кибербезопасность : учебное пособие. – Режим доступа: <https://lanbook.com>[reference:8]
10. ЭБС «Znaniium» : Мищенко В.К., Мищенко П.В. Высокопроизводительные вычислительные системы : учебное пособие. – Новосибирск : Изд-во НГТУ, 2020. – 80 с. – Режим доступа: <https://znaniium.ru>[reference:9]
11. ЭБС «Лань» : Администрирование и кибербезопасность информационных систем : учебное пособие / Часовских В.П. – Екатеринбург : УрГЭУ, 2022. – 173 с. – Режим доступа: <https://e.lanbook.com/book/417746>[reference:10]

Блок вариативной части (Б1.В)

12. ЭБС «Znaniium» : Применение автоматизированных средств тестирования на проникновение при аудите веб-приложений и сервисов : учебное пособие. – 2026. – Режим доступа: <https://znaniium.ru>[reference:11]
13. Эбнер Ю. Этичный хакинг. Инструменты тестирования на взлом и обеспечение ИТ-безопасности. – ISBN 978-5-04-218081-1
14. ЭБС «Лань» : Бессмертный И.А. Искусственный интеллект. Введение в многоагентные системы : учебник для вузов. – Москва : Юрайт.
15. Душкин Р.В. Искусственный интеллект: современный агентный подход. – Москва : ДМК Пресс.
16. Николаев Н.С. Управление информационной безопасностью : учебник. – Москва : КноРус.
17. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью : учебное пособие для вузов. – 2025.
18. Волков М.Ю., Литвинов В.В., Лобанов А.А. Разработка серверных частей интернет-ресурсов : учебное пособие. – Москва : РТУ МИРЭА, 2021. – 188 с.

Факультативные дисциплины (ФТД)

19. ЭБС «Лань» : Безопасность облачных технологий : учебное пособие.
20. ЭБС «Znaniium» : Анализ вредоносных программ : учебное пособие. – Режим доступа: <https://znaniium.ru>[reference:19]

б) Дополнительная литература

1. Stamp M. Introduction to Machine Learning with Applications in Information Security. – 2nd ed. – CRC Press, 2023.
2. Machine Learning Techniques for Cybersecurity. – Cham : Springer, 2023. – (Synthesis Lectures on Information Security, Privacy, and Trust).
3. Иванов М.А. Безопасность искусственных когнитивных систем. Методы поиска новых технических решений : учебное пособие. – Москва : НИЯУ МИФИ, 2025. – 288 с.
4. Intelligent Approaches to Cyber Security. – Boca Raton : CRC Press, Taylor & Francis Group, 2024.
5. Новиков А.М., Новиков Д.А. Методология научного исследования : учеб.-метод. пособие. – М. : ЛИБРОКОМ, 2010.
6. Кумратова А.М. Методология и технологии прикладной информатики : учебное пособие. – Москва ; Вологда : Инфра-Инженерия, 2025. – 180 с.

7. Артюхова Т.Ю., Козырева О.А. Психология и педагогика саморазвития студентов высшей школы : учебник для вузов. – Москва : Юрайт, 2025. – 230 с.
8. Боголюбова Н.М., Николаева Ю.В. Межкультурная коммуникация : учебник для вузов. – 2025. – 582 с.
9. Маралов В.Г. Психология саморазвития : учебник для вузов. – Режим доступа: [https://urait.ru\[reference:27\]](https://urait.ru[reference:27])
10. Садохин А.П. Введение в теорию межкультурной коммуникации : учебное пособие.
11. Карпова Т.А., Асламова Т.В., Закирова Е.С. Английский язык для технических вузов : учебник. – 3-е изд. – Москва : ФЛИНТА.
12. Ибатова А.З. Технический иностранный язык. Technical English : учебное пособие. – Тюмень : Тюменский индустриальный университет.
13. Вехов В.Б., Зуев С.В., Воронков Д.В. и др. Цифровая криминалистика : учебник для вузов / под ред. В.Б. Вехова.
14. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебник для вузов / отв. ред. С.В. ... – Режим доступа: [https://urait.ru\[reference:32\]](https://urait.ru[reference:32])
15. Баланов А. Комплексная информационная безопасность. Полный справочник специалиста. – ISBN 978-5-9729-1771-6
16. Кулаичев А.П. Методы и средства комплексного статистического анализа данных. – Режим доступа: [https://znanium.ru\[reference:34\]](https://znanium.ru[reference:34])

в) Интернет-ресурсы

1. **CVE (Common Vulnerabilities and Exposures)** – каталог общеизвестных уязвимостей информационной безопасности. – Режим доступа: [https://www.cve.org\[reference:35\]](https://www.cve.org[reference:35])
2. **MITRE ATT&CK®** – глобальная база знаний о тактиках и техниках злоумышленников. – Режим доступа: [https://attack.mitre.org\[reference:36\]](https://attack.mitre.org[reference:36])
3. **NIST Computer Security Resource Center (CSRC)** – ресурсный центр компьютерной безопасности Национального института стандартов и технологий США. – Режим доступа: [https://csrc.nist.gov\[reference:37\]](https://csrc.nist.gov[reference:37])
4. **NIST Cybersecurity Framework (CSF) 2.0** – руководство по управлению рисками кибербезопасности. – Режим доступа: [https://www.nist.gov/cyberframework\[reference:38\]](https://www.nist.gov/cyberframework[reference:38])
5. **Научная электронная библиотека eLIBRARY.RU** – крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования. – Режим доступа: <https://elibrary.ru>
6. **Электронная библиотека диссертаций РГБ** – Режим доступа: <http://elibrary.rsl.ru>
7. **Международная реферативная база данных Scopus** – Режим доступа: <http://www.scopus.com>
8. **Международная реферативная база данных Web of Science** – Режим доступа: <http://wokinfo.com/russian>
9. **Сайт ФГБОУ ВО Ставропольский ГАУ, Научная библиотека** – Режим доступа: <https://bibl-stgau.ru>
10. **Словари и энциклопедии On-line** – Режим доступа: www.dic.academic.ru
11. **GitHub** – платформа для хостинга IT-проектов и совместной разработки (инструменты для пентеста, ML-библиотеки). – Режим доступа: <https://github.com>
12. **Kali Linux** – официальный сайт дистрибутива для тестирования на проникновение. – Режим доступа: <https://www.kali.org>

13. **OWASP (Open Web Application Security Project)** – сообщество, посвящённое безопасности веб-приложений. – Режим доступа: <https://owasp.org>

14. **Российский государственный университет правосудия – ЭБС Znanium** – Режим доступа: [https://znanium.ru\[reference:39\]](https://znanium.ru[reference:39])

г) Справочные системы

1. **Справочно-правовая система «КонсультантПлюс»** – содержит законодательную базу, нормативно-правовые акты РФ, в т.ч. в сфере информационной безопасности. – Режим доступа: <http://www.consultant.ru>

2. **Справочно-правовая система «Гарант»** – нормативно-правовая база РФ. – Режим доступа: <http://www.garant.ru>

3. **Справочно-правовая система по информационной безопасности «Прометей»** – электронная база данных юридических документов, включающая тексты нормативных правовых актов, судебных решений, справочные и аналитические материалы по ИБ

4. **Регуляторный хаб «Лаборатории Касперского»** – комплексный навигатор по законодательству и требованиям информационной безопасности

5. **NIST Cybersecurity and Privacy Reference Tool (CPRT)** – инструмент для доступа к эталонным данным стандартов, руководств и фреймворков NIST в области кибербезопасности и конфиденциальности

6. **Справочник «Комплексная информационная безопасность»** – всесторонний обзор ключевых аспектов ИБ

7. **ФСТЭК России** – официальный сайт Федеральной службы по техническому и экспортному контролю (нормативные документы, стандарты защиты информации). – Режим доступа: <https://fstec.ru>

8. **Роскомнадзор** – официальный сайт (законодательство в сфере персональных данных, 152-ФЗ). – Режим доступа: <https://rkn.gov.ru>

д) Программное обеспечение и инструментальные средства

1. **Языки программирования:** Python, C++, Java, Go.

2. **Библиотеки машинного обучения:** scikit-learn, TensorFlow, PyTorch, Keras.

3. **Средства сканирования уязвимостей:** Nessus, OpenVAS, Nmap.

4. **Средства тестирования на проникновение:** Metasploit, Burp Suite, Kali Linux.

5. **SIEM-системы и анализаторы трафика:** Suricata, Snort, Wireshark.

6. **Средства разработки и CI/CD:** Git, Jenkins, GitLab CI, SonarQube.

7. **Системы управления проектами:** Jira, Redmine, MS Project.

6. Подготовка к защите и процедура защиты выпускной квалификационной работы

6.1. Результаты освоения ОП ВО

В процессе подготовки и защиты ВКР проверяется сформированность всех универсальных, общепрофессиональных и профессиональных компетенций, указанных в п. 5.1, а также дополнительных компетенций, формируемых в части, формируемой участниками образовательных отношений (ПК-2 – экспертиза и расследование инцидентов, ПК-4 – управление жизненным циклом ПО).

6.2. Общие требования к выпускной квалификационной работе

Выпускная квалификационная работа (магистерская диссертация) представляет собой самостоятельно выполненное исследование, демонстрирующее уровень подготовленности выпускника к самостоятельной профессиональной деятельности в области прикладной информатики, ИИ и кибербезопасности.

Тематика ВКР разрабатывается выпускающей кафедрой (Кафедра информационных систем и Кафедра инжиниринга IT-решений) и доводится до сведения обучающихся не позднее, чем за 6 месяцев до ГИА.

Требования к структуре ВКР:

- Титульный лист
- Задание на выполнение ВКР
- Реферат (аннотация)
- Содержание
- Введение (актуальность, цели, задачи, объект, предмет, методы, научная новизна, практическая значимость)
 - Глава 1. Аналитический обзор (анализ предметной области, существующих решений, стандартов ИБ)
 - Глава 2. Методологическая часть (разработка моделей, алгоритмов, архитектуры решения)
 - Глава 3. Экспериментальная/проектная часть (реализация прототипа, тестирование, экспериментальные данные, оценка эффективности)
 - Глава 4. Охрана труда и информационная безопасность (при необходимости)
- Заключение (выводы и предложения)
- Список использованных источников (не менее 50 наименований)
- Приложения (исходные коды, протоколы тестирования, скриншоты)

Объём – 60-80 страниц печатного текста.

Примерные темы ВКР (составлены на основе учебного плана и ПС):

1. Разработка системы обнаружения сетевых аномалий на основе сверточных нейронных сетей.
2. Применение методов машинного обучения для анализа вредоносного программного обеспечения.
3. Разработка модуля автоматизированного реагирования на инциденты ИБ (на базе SOAR).
4. Исследование и реализация методов защиты систем искусственного интеллекта от состязательных атак.
5. Разработка инструментария для тестирования на проникновение веб-приложений с использованием ИИ.
6. Моделирование поведения нарушителя информационной безопасности с использованием агентного подхода.
7. Разработка системы мониторинга защищённости корпоративной сети на основе SIEM-платформы с элементами интеллектуального анализа данных.

8. Применение методов глубокого обучения для выявления DDoS-атак в распределённых компьютерных системах.
9. Разработка программного модуля для анализа конфигураций межсетевых экранов на предмет уязвимостей.
10. Интеграция технологии блокчейн в системы управления доступом для обеспечения целостности данных.

По письменному заявлению обучающегося (нескольких обучающихся, выполняющих выпускную квалификационную работу совместно) организация может в установленном ею порядке предоставить обучающемуся (обучающимся) возможность подготовки и защиты выпускной квалификационной работы по теме, предложенной обучающимся (обучающимися), в случае обоснованности целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности в виде стартапа. В этом случае студент подает заявление на имя заведующего выпускающей кафедрой с просьбой закрепить данную тему за ним. Студенты могут выбрать, разработать и защитить ВКР в формате «Стартап как диплом».

После того как тема выбрана, сформулирована и согласована с научным руководителем, студент пишет заявление на имя заведующего кафедрой о закреплении за ним темы выпускной квалификационной работы.

Выбор темы выпускной квалификационной работы и её утверждение должны быть завершены до окончания 7 семестра. Формулировка темы выпускной квалификационной работы с указанием научного руководителя, утверждается приказом по университету и изменениям не подлежит. После выхода приказа студент получает от своего научного руководителя задание на выпускную квалификационную работу, которое утверждается заведующим кафедрой

6.3. Руководство и консультирование

Руководитель ВКР оказывает обучающемуся помощь в разработке содержания темы на весь период выполнения ВКР, рекомендует необходимую литературу, справочные материалы и другие источники по теме, проводит систематические консультации, составляет задания на преддипломную практику, проверяет выполнение работы по частям и в целом.

Рекомендуется составление календарного графика выполнения выпускной квалификационной работы.

Закрепление тем ВКР и руководителей, консультантов рассматривается на заседаниях выпускающих кафедр, оформляется протоколом. По представлению выпускающих кафедр дирекция формирует проект приказа, который передается в учебно-методическое управление для оформления приказа по университету об утверждении тем, руководителей, научных руководителей, консультантов (при необходимости). Ответственность за подготовку приказа в указанные сроки несет заведующий выпускающей кафедрой, директор.

Закрепление темы ВКР утверждается приказом курирующего проректора по представлению директора института и заведующего выпускающей кафедрой и согласовании с учебно-методическим управлением. Ответственность за подготовку приказа в указанные сроки несет заведующий выпускающей кафедрой, директор института.

6.4. Требования к объему, структуре и оформлению выпускной квалификационной работы

Требования к выпускным квалификационным работам, их структуре, требованиям к оформлению текстовой части, таблиц, графиков, графических элементов, списка используемой литературы, нормативных правовых документов, Интернет-источников и т. д.

представлены в методических рекомендациях по выполнению выпускной квалификационной работы и являются приложением к данной программе.

6.4.1. Требования к объему и структуре выпускной квалификационной работы

Выпускная квалификационная работа по направлению подготовки 09.04.03 «Прикладная информатика» профиль «Искусственный интеллект в кибербезопасности» должна полностью соответствовать утвержденной теме и включать графическую часть и пояснительную записку к ней.

По объёму ВКР должна быть не менее 60 страниц печатного текста. Выпускная работа может активно использовать материалы и подходы, использованные в курсовых проектах и курсовых работах, которые выполняются студентом в течение обучения.

На защиту студент представляет пояснительную записку и иллюстрационный (графический) материал, который может быть представлен на бумажных или электронных носителях.

Требования к структуре ВКР:

- Титульный лист
- Задание на выполнение ВКР
- Реферат (аннотация)
- Содержание
- Введение (актуальность, цели, задачи, объект, предмет, методы, научная новизна, практическая значимость)
 - Глава 1. Аналитический обзор (анализ предметной области, существующих решений, стандартов ИБ)
 - Глава 2. Методологическая часть (разработка моделей, алгоритмов, архитектуры решения)
 - Глава 3. Экспериментальная/проектная часть (реализация прототипа, тестирование, экспериментальные данные, оценка эффективности)
 - Глава 4. Охрана труда и информационная безопасность (при необходимости)
- Заключение (выводы и предложения)
- Список использованных источников (не менее 50 наименований)
- Приложения (исходные коды, протоколы тестирования, скриншоты)

Объём – 60-80 страниц печатного текста.

6.4.2. Общие требования к оформлению текста выпускной квалификационной работы

На листе оставляются поля: слева – 3 см, справа – 1,5 см, снизу и сверху – 2 см. При использовании текстового редактора Microsoft Word должен применяться шрифт Times New Roman 14 размера с полуторным интервалом между строк.

Рубрикация и нумерация страниц. Разделы (главы) должны быть пронумерованы арабскими цифрами. Подразделы следует нумеровать арабскими цифрами в пределах каждого раздела. Номер подраздела состоит из номера раздела (главы) и номера подраздела, разделенных точкой.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номера раздела (главы), подраздела и пункта, разделенных точками.

Заголовки разделов (глав) начинаются на отдельной строке прописными буквами, например: «ВВЕДЕНИЕ» и т. д. Заголовки подразделов пишутся строчными буквами (кроме первой прописной). В конце заголовка точку не ставят. Подчеркивание и переносы в заголовках не допускаются.

Каждый раздел следует начинать с нового листа (страницы), а подразделы продолжают на странице.

Нумерация страниц должна быть сквозной: первой страницей является титульный лист, второй – оглавление и т. д. Номер страницы проставляется арабскими цифрами в правом верхнем углу. На странице 1 (титульный лист) номер страницы не ставят.

Если имеются рисунки и таблицы, которые располагаются на отдельных страницах, их необходимо включать в общую нумерацию. Приложения и библиографический список также включаются в сквозную нумерацию.

Оформление таблиц. Каждая таблица должна иметь порядковый номер и краткий четкий заголовок (при наличии в работе лишь одной, слово «Таблица» и ее номер не ставится). Нумерация таблиц последовательная и сквозная. Слева над таблицей (на уровне «красной строки») помещают надпись: «Таблица» с указанием порядкового номера и через тире – заголовок таблицы.

По своему строению таблицы должны быть простыми и удобными для размещения на странице. Следует избегать громоздких таблиц. Построение таблиц с размещением материала лишь в одну строку недопустимо. Многоэтажные заголовки граф нежелательны. Разделение заголовков граф таблицы по диагонали не допускается.

При необходимости, таблицу с большим количеством строк допускается переносить на другой лист. При переносе части таблицы на другой лист слово «Таблица» и номер ее указывают один раз слева над первой частью таблицы; над другими частями пишут слово «Продолжение». Если в работе несколько таблиц, то после слова «Продолжение» указывают номер таблицы, например: «Продолжение табл. 1».

Нумерацию граф, если таблица не переносится, делать не следует.

Основные заголовки таблицы пишутся с прописной буквы, а подчиненные, расположенные ниже объединяющего их текста, – со строчной.

Пустые графы в таблице оставлять нельзя. Если в графе необходимо указать, что исследования не проводились, можно употреблять знак умножения, а в примечании, которое помещается под таблицей, объяснить его значение. При отсутствии явления ставится знак тире.

Единицы измерения давать без предлога «в» через запятую. Например: объемная доля этилового спирта, %; массовая концентрация сахаров, г/дм³. Если размеры не сокращаются, то их дают также через запятую в именительном падеже множительного числа.

Все слова в таблице пишутся полностью, кроме принятых сокращений. Текст и цифровой материал должны быть напечатаны через 1,5 интервала. На все таблицы должна быть ссылка в тексте.

Иллюстрации. Иллюстрации (рисунки, графики, схемы и т. п.) обозначают словом «Рисунок» и их следует помещать в выпускной квалификационной работе только в том случае, если они дополняют текстовый материал.

Графики, схемы, диаграммы должны быть четко выполнены на листах белой бумаги, представлять графический материал в виде фотографий нельзя.

На все иллюстрации должна быть ссылка в тексте. В связи с тем, что все иллюстрации (схемы, чертежи и пр.) именуются рисунками, они последовательно нумеруются арабскими цифрами в пределах раздела. Содержание рисунков отображается в подрисуночных подписях, в которых объясняются все цифровые и буквенные обозначения (позиции). Нумерация иллюстраций должна быть сквозной. Например: Рисунок 2. Далее через дефис с заглавной буквы указывается название рисунка, а в скобках автор и год издания литературного источника, откуда взят рисунок. Рисунок, выполненный с натуры, отмечается словом «Оригинальный».

Если в работе одна иллюстрация, то ее не нумеруют.

Знаки и числа в тексте. Математические знаки применяются при используемых в вариационной статистике символах ($P > 0,1$; +, -), в формулах и таблицах при цифрах. В тексте их пишут словами.

Не допускается употребление символов и условных обозначений вместо соответствующих им терминов.

Знаки °, №, % и т. п. применяют только при цифрах. В других случаях их пишут словами.

Все числа с размерностями в научной литературе пишут цифрами.

Порядковые числительные, обозначаемые арабскими цифрами, сопровождаются падежными наращенными. Порядковые числительные, обозначенные римскими цифрами пишутся без наращенного.

Сложные прилагательные, первой частью которых является числительное, пишутся через дефис.

При написании дат после числа ставится точка, потом следует месяц арабскими цифрами и год.

Для указания многолетнего периода между годами ставится тире, цифры не сокращаются и слово «год» пишется во множественном числе, например: 2008-2009 гг.

Оформление ссылок на литературные источники. При ссылке на литературные источники в тексте указываются инициалы и фамилия автора, в скобках – номер, под которым указан источник в библиографическом списке или год издания. Например: «В работах В. И. Иванова (2016) указывается». Иногда ссылаются на автора в конце абзаца, в этом случае в скобках указывается фамилия без инициалов и снова год. Например: (Теодоронский, 2009).

Составные фамилии пишутся через дефис, например: Иванов-Крамской. Если же речь идет о каком-нибудь методе или способе, принадлежащем нескольким авторам, то их отделяют с помощью тире. Например: метод Романовского-Гимза.

Фамилии типа Белоконь, Гребень, Пилипчук изменяются по падежам, если они принадлежат мужчинам, и не изменяются, если принадлежат женщинам.

Оформление библиографического списка. Библиографический список начинается с официально-документальных материалов. Нумерация источников сплошная.

Сведения об отечественной литературе располагаются строго в алфавитном порядке авторов книг, статей в журналах и сборниках научных трудов, а если автор отсутствует, то заглавия книг, сборников и т. д.

Перечень иностранной литературы дается в порядке латинского алфавита, после ссылок на отечественных авторов и издания.

Библиография составляется по алфавиту авторов, сначала отечественных, затем зарубежных. Работы одного автора размещаются в хронологическом порядке. Библиографическое описание проводится в соответствии с ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления».

6.5. Рецензирование выпускной квалификационной работы

ВКР по программам бакалавриата подлежат рецензированию специалистами других кафедр институтов, что оформляется отдельным документом (рецензией). ВКР, допущенные выпускающей кафедрой к защите, распоряжением директора института направляются на рецензирование. Для ВКР в форме бакалаврской работы рецензент назначается из числа профессорско-преподавательского состава других кафедр институтов. В рецензиях должны быть раскрыты следующие вопросы: актуальность и оригинальность темы, соответствие её профилю подготовки биолога; полнота разработки темы в целом и по разделам; положительные стороны и недостатки отдельных частей работы, точность и достоверность полученных данных; теоретическая и практическая подготовленность студента при решении поставленных задач; грамотность, ясность и последовательность изложения материала; качество оформления работы и иллюстративного материала; обоснованность выводов и предложений. В заключении рецензенты дают общую оценку работы и рекомендации о присвоении конкретному автору соответствующей квалификации.

Текст ВКР, отзыв и рецензия передаются в государственную экзаменационную комиссию не позднее, чем за 2 календарных дня до дня защиты ВКР. Допуск к защите ВКР осуществляет заведующий выпускающей кафедрой. Если заведующий кафедрой, исходя из содержания отзывов руководителя и рецензента, не считает возможным допустить студента к защите ВКР, вопрос об этом должен рассматриваться на заседании учебно-

методической комиссии института с участием руководителя и автора ВКР. Решение учебно-методической комиссии доводится до сведения дирекции.

6.6. Процедура защиты выпускной квалификационной работы

Оформленная в соответствии Положением о выполнении и защите выпускной квалификационной работы в ФГБОУ ВО Ставропольский ГАУ, выпускная квалификационная работа, отзыв, рецензия, отчет и заключение о степени оригинальности ВКР передаются в государственную экзаменационную комиссию не позднее, чем за 2 календарных дня до начала работы ГЭК.

Обучающийся допускается к защите выпускной квалификационной работы вне зависимости от степени оригинальности, полученной в результате автоматизированной проверки системой «Антиплагиат.СтГАУ» с согласия руководителя и заведующего выпускающей кафедры. До защиты обучающийся должен быть ознакомлен с заключением о степени оригинальности его работы, а во время защиты обучающемуся должна быть предоставлена возможность дать пояснения относительно самостоятельности выполнения им работы. Государственная экзаменационная комиссия, признавшая факт несамостоятельности выполнения работы в результате собеседования с обучающимся в процессе защиты работу, оценивает её как неудовлетворительную. Решение государственной экзаменационной комиссии обязательно отражается в протоколе защиты выпускной квалификационной работы.

Результаты защиты выпускных квалификационных работ определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются непосредственно после защиты и оформления в установленном порядке протоколов заседаний государственной экзаменационной комиссии и заполнения зачетных книжек обучающихся. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания в форме защиты выпускной квалификационной работы.

Обучающимся, не явившимся на защиту по уважительной причине, предоставляется право защитить выпускную квалификационную работу в течение 6 месяцев после завершения государственной итоговой аттестации.

Обучающиеся, не защитившие выпускную квалификационную работу в связи с неявкой на защиту по неуважительной причине или в связи с получением оценки «неудовлетворительно», отчисляются из Университета с выдачей им справки об обучении как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана. Повторная защита ВКР возможна не ранее чем через год и не позднее чем через пять лет после срока проведения государственной итоговой аттестации, которая не пройдена обучающимся.

В тех случаях, когда защита выпускной квалификационной работы признана неудовлетворительной, государственная экзаменационная комиссия решает вопрос о том, предоставить ли обучающемуся возможность повторной защиты этой же работы с доработкой или указать ему на необходимость разработки новой темы, которая устанавливается выпускающей кафедрой. Решение комиссии отмечается в протоколе защиты выпускной квалификационной работы.

Обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения защиты ВКР и (или) несогласии с результатами защиты ВКР. Порядок организации и проведения апелляции результатов сдачи государственных аттестационных испытаний регламентируется Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры в ФГБОУ ВО Ставропольском ГАУ.

6.8. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Оформленная в соответствии Положением о выполнении и защите выпускной квалификационной работы в ФГБОУ ВО Ставропольский ГАУ, выпускная квалификационная работа, отзыв, рецензия, отчет и заключение о степени оригинальности ВКР передаются в государственную экзаменационную комиссию не позднее, чем за 2 календарных дня до начала работы ГЭК.

Защита выпускной квалификационной работы проходит на заседании ГЭК, утверждаемой в установленном порядке. Начало работы ГЭК возможно при наличии ее кворума (не менее 2/3 списочного состава при обязательном присутствии председателя) и в присутствии выпускников. На каждом заседании заслушивается не более 25 защит ВКР. В день проводится не более двух заседаний. Заседания ГЭК являются открытыми, т.е. на них могут присутствовать все желающие. Перед началом работы ГЭК председатель приветствует выпускников, знакомит их с членами ГЭК и оглашает регламент защиты ВКР.

При проведении защиты ВКР на каждого студента секретарем комиссии, заполняется протокол с указанием темы ВКР, руководителя (и консультанта, при его наличии) и перечня вопросов, заданных студенту по ходу защиты ВКР. Протоколы заседаний ГЭК оформляются с помощью технических средств, установленных в аудитории, в которых проходит заседания. После заполнения протокол подписывается председателем ГЭК и секретарем.

К защите ВКР допускаются студенты, освоившие образовательную программу в соответствии с учебным планом, прошедшие предзащиту на кафедре и получившие на выпускающей кафедре допуск к защите.

В докладе изложение материала должно быть последовательным и логичным. Отдельные положения исследуемого вопроса должны быть иллюстрированы данными из выпускной квалификационной работы, при необходимости оформленными в рисунки, таблицы, диаграммы, графики. При подготовке доклада следует составить план выступления, в котором отразить актуальность темы, главные выводы и/или предложения, их краткое обоснование и теоретическое или практическое значение – с тем, чтобы в течение 15 минут представить достоинства выпускной квалификационной работы.

Состав балльно-рейтинговой оценки выпускных квалификационных работ

№	Наименование	Оценка, балл
1.	Содержание выпускной квалификационной работы: новизна, актуальность, соответствие выводов и предложений содержанию работы	40
2.	Оформление выпускной квалификационной работы: оформление текстового и графического материала в соответствии с ГОСТ	20
3.	Наличие презентации, отражающей основные положения и выводы выпускной квалификационной работы	15
4.	Доклад	15
5.	Ответы на вопросы по теме выпускной квалификационной работы	10
ИТОГО		100

Критерии оценки содержания выпускной квалификационной работы

31-40 баллов выставляется, если работа представляет собой логически завершенное, самостоятельное исследование, посвящено решению актуальных проблем с учётом современных достижений науки и техники; базируется на современных научных концепциях и подходах, нормативных документах; отличается оригинальностью, включает эле-

менты новизны; в работе широко представлен графический материал, выводы и предложения в полной мере соответствуют содержанию работы.

21-30 баллов выставляется, если работа представляет собой вполне логически завершённое, самостоятельное исследование, посвящено решению актуальных проблем, не учтены современные достижения науки и техники; базируется на современных научных концепциях и подходах, нормативных документах; включает элементы новизны; в работе представлен графический материал, выводы и предложения не вполне соответствуют содержанию работы.

11-20 баллов выставляется, если работа представляет собой не вполне логически завершённое исследование; в работе не учтены современные достижения науки и техники; в работе отсутствуют элементы новизны; графический материал представлен ограничено, выводы и предложения не вполне соответствуют содержанию работы.

1-10 баллов выставляется, если работа представляет собой не вполне логически завершённое исследование; в работе не учтены современные достижения науки и техники; в работе отсутствуют элементы новизны; графический материал отсутствует, выводы и предложения не соответствуют содержанию работы.

0 баллов – при отсутствии выпускной квалификационной работы.

Критерии оценки оформления выпускной квалификационной работы (оформление текстового и графического материала в соответствии с ГОСТ)

15-20 баллов выставляется, если работа выполнена в полном соответствии с методическими указаниями; библиографический список оформлен в соответствии с ГОСТ; графический материал выполнен в соответствии с ГОСТ.

10-15 баллов выставляется, если работа выполнена в полном соответствии с методическими указаниями; библиографический список оформлен не в соответствии с ГОСТ; графический материал выполнен в соответствии с ГОСТ.

1-10 баллов выставляется, если работа выполнена в несоответствии с методическими указаниями; библиографический список оформлен не в соответствии с ГОСТ; графический материал выполнен не в соответствии с ГОСТ.

0 баллов – при полном отсутствии выпускной квалификационной работы.

Критерии оценки презентации

12-15 баллов – все части презентации связаны с целью и предметом обсуждения. Презентация основана на ключевых моментах, полностью раскрывает тему. Демонстрируется свободное владение профессиональными терминами при раскрытии поставленных задач. Грамматические ошибки отсутствуют. Имеются графические иллюстрации, статистика, диаграммы, графики, примеры сравнения. Выдержана тематическая последовательность. Читаемый шрифт, корректно выбран цвет (не более трех). Используется изображения, видео, аудио.

8-11 баллов – все части презентации содержат важные утверждения по теме. Презентация основана на нескольких ключевых моментах, не полностью раскрывающих тему. Демонстрируется использование профессиональными терминами при раскрытии поставленных задач. Грамматические ошибки практически отсутствуют. Графические иллюстрации, статистика, диаграммы, графики, примеры сравнения представлены не в полной мере. Выдержана тематическая последовательность. Читаемый шрифт, корректно выбран цвет. Используется изображения, видео.

4-7 баллов – основные части презентации содержат важные утверждения по теме, однако некоторые фрагменты не имеют к ней отношения. Некоторые выводы нелогичны или необоснованны. Презентация содержит ключевые моменты, однако они излишне многословны или лишены информации. Наблюдается некоторое затруднение при подборе слов и отдельные неточности в их употреблении. Допускаются ошибки, затрудняющие понимание. Представлены 2-3 графических иллюстрации (и «или» диаграмм, графиков,

примеров). Выдержана тематическая последовательность. Читаемый шрифт, корректно выбран цвет. Используется изображения, видео.

1-3 баллов – у презентации есть тема, однако многие ее части к теме отношения не имеют. Выводы отсутствуют или нелогичны. Не выделены ключевые моменты. Допускаются многочисленные ошибки, затрудняющие понимание. Отсутствует иллюстрационный материал. Используется изображения, видео.

0 баллов – при полном отсутствии презентации.

Критерии оценки доклада

11-15 баллов – доклад производит выдающееся впечатление, сопровождается иллюстративным материалом, в котором автор прекрасно ориентируется, аргументировано отвечает на все поставленные вопросы, показано владение специальным аппаратом, выводы полностью характеризуют работу.

6-10 баллов – доклад четко выстроен, демонстрационный материал, используемый в докладе хорошо оформлен, но есть неточности, на ряд вопросов ответы слабо аргументированы, используются общенаучные и специальные термины, выводы нечетко характеризуют работу.

1-5 баллов – доклад рассказывается, но не объясняется суть работы, представленный демонстрационный материал не использовался докладчиком или оформлен плохо, неграмотно, не может четко отвечает на вопросы, использует базовые понятия и термины, выводы имеются, но не доказаны.

0 баллов – при полном отсутствии презентации.

Критерии оценки ответов на вопросы по теме выпускной квалификационной работы

7- 10 баллов – аргументировано отвечает на все поставленные вопросы, показано владение специальным аппаратом.

4- 6 баллов – на ряд вопросов ответы слабо аргументированы, использует общенаучные и специальные термины.

1-3 баллов – не может четко отвечает на вопросы, использует базовые понятия и термины.

0 баллов – при полном отсутствии ответов на вопросы.

Полученная на защите выпускной квалификационной работы сумма баллов переводится в оценку:

«отлично» – от 85 до 100 баллов;

«хорошо» – от 70 до 84 баллов;

«удовлетворительно» – от 55 до 69 баллов;

«неудовлетворительно» – менее 50 баллов.

Оценка выставляется каждым членом государственной экзаменационной комиссии.

Итоговая оценка выставляется коллегиально с учетом оценок всех членов ГЭК.

Студент имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения защиты выпускной квалификационной работы.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для подготовки и прохождения государственной итоговой аттестации

1. ЭБС «Znanium» – материалы по машинному обучению (Гудфеллоу И., Бенджио И., Курвилль А. «Глубокое обучение»).

2. ЭБС «Лань» – учебники по информационной безопасности (Бабаш А.В., Шаньгин В.Ф.).
3. Документация по фреймворкам TensorFlow, PyTorch, Scikit-learn.
4. Материалы по стандартам ФСТЭК России и NIST.
5. Научные статьи из баз данных Scopus, Web of Science по тематике ИИ и кибербезопасности.

Программное обеспечение:

- Инструменты пентеста: Kali Linux, Metasploit, Nmap, Burp Suite.
- Средства разработки: Python, PyCharm, Jupyter Notebook.
- Средства моделирования: AnyLogic, MATLAB.
- Средства для ML: TensorFlow, PyTorch, scikit-learn.

Интернет-ресурсы:

- Реестр уязвимостей CVE (eve.mitre.org).
- База знаний MITRE ATT&CK.
- Портал «Антиплагиат.СтГАУ».
- Научная электронная библиотека eLibrary.ru.

Интернет-ресурсы:

1. Интернет-библиотека образовательных изданий [Электронный ресурс]. – Режим доступа: <http://www.iqlib.ru>.
2. Интернет-университет информационных технологий [Электронный ресурс]. – Режим доступа: <http://www/intuit.ru>.
3. Международная реферативная база данных SCOPUS [Электронный ресурс]. – Режим доступа: <http://www.scopus.com/>.
4. Международная реферативная база данных Web of Science [Электронный ресурс]. – Режим доступа: <http://wokinfo.com/russian/>.
5. Российская Государственная Библиотека (РГБ) [Электронный ресурс]. – Режим доступа: www.pnb.rsl.ru.
6. Российская национальная библиотека (РНБ) [Электронный ресурс]. – Режим доступа: www.nlr.ru.
7. Сайт СтГАУ, Библиотека – электронная библиотека СтГАУ [Электронный ресурс]. – Режим доступа: <http://www/stgau.ru>.
8. Словари и энциклопедии On-line [Электронный ресурс]. – Режим доступа: www.dic.academic.ru.
9. Справочно-правовая система. Содержит законодательную базу, нормативно-правовую базу [Электронный ресурс]. – Режим доступа: <http://www.consultant.ru>.
10. Электронная библиотека диссертаций Российской государственной библиотеки [Электронный ресурс]. – Режим доступа: <http://elibrary.rsl.ru/>.

8. Порядок организации и проведения апелляции результатов сдачи государственных аттестационных испытаний

По результатам государственной итоговой аттестации обучающийся имеет право на апелляцию. Обучающийся имеет право подать в апелляционную комиссию по направлению подготовки 09.04.03 «Прикладная информатика» профиль «Искусственный интеллект в кибербезопасности» письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного экзамена.

Апелляция подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного

испытания.

Для рассмотрения апелляции секретарь государственной экзаменационной комиссии направляет в апелляционную комиссию протокол заседания государственной экзаменационной комиссии, заключение председателя государственной экзаменационной комиссии о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также письменные ответы обучающегося (при их наличии) (для рассмотрения апелляции по проведению государственного экзамена), либо выпускную квалификационную работу, отзыв и рецензию (рецензии) (для рассмотрения апелляции по проведению защиты выпускной квалификационной работы).

Апелляция рассматривается не позднее 2 рабочих дней со дня подачи апелляции на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляцию.

Решение апелляционной комиссии доводится до сведения обучающегося, подавшего апелляцию, в течение 3 рабочих дней со дня заседания апелляционной комиссии. Факт ознакомления обучающегося, подавшего апелляцию, с решением апелляционной комиссии удостоверяется подписью обучающегося.

При рассмотрении апелляции о нарушении процедуры проведения государственного аттестационного испытания апелляционная комиссия принимает одно из следующих решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях процедуры проведения государственного аттестационного испытания обучающегося не подтвердились и (или) не повлияли на результат государственного аттестационного испытания;

- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях процедуры проведения государственного аттестационного испытания обучающегося подтвердились и повлияли на результат государственного аттестационного испытания.

В последнем случае результат проведения государственного аттестационного испытания подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в государственную экзаменационную комиссию для реализации решения комиссии. Обучающемуся предоставляется возможность пройти государственное аттестационное испытание в дополнительные сроки, но не позднее даты завершения обучения в Университете в соответствии со стандартом.

При рассмотрении апелляции о несогласии с результатами государственного экзамена апелляционная комиссия выносит одно из следующих решений:

- об отклонении апелляции и сохранении результата государственного экзамена;
- об удовлетворении апелляции и выставлении иного результата государственного экзамена.

Решение апелляционной комиссии не позднее следующего рабочего дня передается в государственную экзаменационную комиссию. Решение апелляционной комиссии является основанием для аннулирования ранее выставленного результата государственного экзамена и выставления нового.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Повторное проведение государственного аттестационного испытания обучающегося, подавшего апелляцию, осуществляется в присутствии одного из членов апелляционной комиссии не позднее даты завершения обучения в организации в соответствии со стандартом.

Апелляция на повторное проведение государственного аттестационного испытания не принимается.

Порядок организации и проведения апелляции результатов сдачи государственных аттестационных испытаний регламентируется Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования

– программам бакалавриата, программам специалитета и программам магистратуры в ФГБОУ ВО Ставропольском ГАУ.

9. Порядок организации и проведения государственной итоговой аттестации для обучающихся из числа лиц с ограниченными возможностями здоровья Университета

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на экзамене/защите ВКР присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе записывая под диктовку);

- задания для выполнения, а также инструкция о порядке проведения экзамена оформляются увеличенным шрифтом;

- задания для выполнения на экзамене зачитываются ассистентом;

- письменные задания выполняются на бумаге, надиктовываются ассистенту;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе записывая под диктовку);

- экзамен проводится в письменной форме;

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости предоставляется звукоусиливающая аппаратура индивидуального пользования;

- по желанию студента экзамен может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту.

Программа государственной итоговой аттестации составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.04.03 «Прикладная информатика», квалификация Магистр и учебного плана по профилю подготовки «Искусственный интеллект в кибербезопасности».

Автор



к.э.н., Березницкий А.С.

Рецензенты



к.т.н., доцент Шлаев Д.В.



к.т.н., доцент Крон Р.В.

Программа государственной итоговой аттестации рассмотрена и рекомендована кафедрой информационных системы

Протокол от «07» апреля 2026 года № 9

Зав. кафедрой



А.С. Березницкий

Образец заявления на выполнение магистерской диссертации

И.о. декана факультета цифровых технологий,
доценту Шлаеву Д.В.

(ученое звание, ученая степень, И.О. Фамилия)

ФГБОУ ВО Ставропольский ГАУ

студента(ки) _____ курса _____ группы

очной формы обучения

факультета цифровых технологий

направления подготовки 09.04.03 «Прикладная

информатика», профиль – Искусственный ин-
теллект в кибербезопасности

(шифр, наименование)

ФИО студента полностью

Заявление

Прошу Вас разрешить выполнение выпускной квалификационной работы в
виде бакалаврской работы на кафедре: _____

на тему: _____

руководителем прошу назначить

ФИО руководителя, должность, место работы

Дата _____

Подпись _____

Согласовано:

Руководитель _____ Фамилия И.О.

Зав. кафедрой _____ Фамилия И.О.

Образец задания
ФГБОУ ВО СТАВРОПОЛЬСКИЙ ГАУ
Факультет цифровых технологий
кафедра информационных систем

Утверждаю:
Зав. кафедрой
А.С. Березницкий
подпись И.О. Фамилия

« ___ » _____ 20__ г

ЗАДАНИЕ НА БАКАЛАВРСКУЮ РАБОТУ

Обучающемуся _____

(фамилия, имя, отчество, курс, группа, направление подготовки/специальность, профиль, специализация, магистерская программа)

Тема ВКР « _____ »

Утверждена приказом по университету № ___ от « ___ » _____ 20__ г.

1. Срок представления работы к защите « ___ » _____ 20__ г.

2. Исходные данные для выполнения работы _____

3. Содержание работы:

_____ Аннотация

_____ Введение

_____ Основная часть

_____ Экономическая эффективность

_____ Заключение

_____ Список используемой литературы

4. Перечень графического материала (с полным указанием обязательных чертежей)

5. Консультанты по разделам _____

6. Дата выдачи задания _____

7. Руководитель работы _____

подпись

(Фамилия И.О., учёная степень, должность, место работы)

Задание к исполнению принял « ___ » _____ 20__ г. _____

(подпись обучающегося)

Образец календарного графика выполнения бакалаврской работы

ФГБОУ ВО СТАВРОПОЛЬСКИЙ ГАУ

Факультет цифровых технологий

кафедра информационных систем

Утверждаю:

Зав. кафедрой

А.С. Березницкий

подпись И.О. Фамилия

« ____ » _____ 20__ г

КАЛЕНДАРНЫЙ ГРАФИК ВЫПОЛНЕНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ (БАКАЛАВРСКОЙ РАБОТЫ)

Студента _____

(фамилия, имя, отчество, курс, группа, направление подготовки/специальность, профиль, специализация, магистерская программа)

Темы ВКР « _____ »

№ п/п	Выполнение работ и мероприятия	Срок выполнения
1.	Выбор темы и оформление заявления на выполнение бакалаврской работы	
2.	Составление плана работы и согласование его с руководителем	
3.	Подбор литературы, ее изучение и проработка.	
4.	Разработка и предоставление на проверку первой главы	
5.	Накопление, систематизация и анализ практических материалов	
6.	Сбор данных	
7.	Анализ полученных данных	
8.	Разработка и предоставление на проверку второй, третьей глав	
9.	Разработка и предоставление на проверку четвертой, пятой глав	
10.	Согласование с руководителем выводов и предложений	
11.	Предзащита и переработка (доработка) работы в соответствии с замечаниями (за 2 недели до защиты)	
12.	Представление готовой работы на проверку руководителю, нормоконтролеру (за 2 недели до защиты)	
13.	Получение отзыва и заключения о степени оригинальности ВКР от руководителя (за 14 календарных дней до защиты)	
14.	Предоставление завершенной работы, отзыва и заключения о степени оригинальности ВКР на кафедру (за 14 календарных дней до защиты)	
15.	Получение допуска к защите от зав. кафедрой и получение рецензии (за 14 календарных дней до защиты)	
16.	Передача оформленной ВКР с отзывом, рецензией и заключением о степени оригинальности ВКР в государственную экзаменационную комиссию (за 2 календарных дня до защиты)	

Руководитель ВКР: _____

(подпись) ФИО руководителя, должность, место работы

Студент: _____

Фамилия, имя, отчество

(подпись)

Образец заключения о степени оригинальности бакалаврской работы

ФГБОУ ВО СТАВРОПОЛЬСКИЙ ГАУ
Факультет цифровых технологий
кафедра информационных систем

ЗАКЛЮЧЕНИЕ
о степени оригинальности выпускной квалификационной работы

Выпускная квалификационная работа (бакалаврская работа) обучающегося

_____ (Ф.И.О. полностью)
_____ курса _____ группы, на тему
« _____

В соответствии с п.п. 1.12, 1.14, 1.15 Положения о выполнении и защите выпускных квалификационных работ в ФГБОУ ВО Ставропольский ГАУ» **прошла** автоматизированный анализ а системе «Антиплагиат.СтГАУ», **сохранена** в электронной информационно-образовательной среде университета и **загружена** в электронно-библиотечную систему университета.

Доля авторского текста (оригинальности) в результате автоматизированной проверки составила « _____ %».

Анализ результата автоматизированной проверки системой «Антиплагиат.СтГАУ» и мнение руководителя ВКР о достоверности, фактической доле оригинального текста и степени самостоятельности обучающегося при написании работы:

Руководитель ВКР

(уч.степень, должность, Фамилия И.О.)
« _____ » _____ 20__ г.

(Подпись)

Образец отзыва руководителя

ФГБОУ ВО СТАВРОПОЛЬСКИЙ ГАУ
Факультет цифровых технологий
кафедра информационных систем

**ОТЗЫВ о работе _____ (фамилия, имя, отчество обучающегося)
период подготовки выпускной квалификационной работы**

На тему «

_____»

В тексте отзыва следует указать степень самостоятельности и способности обучающегося к исследовательской работе (умение и навыки искать, обобщать, анализировать материал и делать выводы), дать оценку деятельности обучающегося в период выполнения работы (степень добросовестности, работоспособности, ответственности, аккуратности и т.п.).

Руководитель

(фамилия, имя, отчество, должность, ученая степень, ученое звание)

Дата: « ____ » _____ 20__ г.

Подпись: _____

РЕЦЕНЗИЯ

на выпускную квалификационную работу обучающегося _____ курса
направления
подготовки _____

факультета _____

(Фамилия, имя, отчество студента)

Тема выпускной квалификационной работы _____

Выпускная квалификационная работа выполнена на кафедре

_____ под руководством _____

(уч.степень, должность Фамилия И.О. руководителя)

Общая характеристика работы:

Положительные стороны работы: _____

Недостатки: _____

Заключение: _____

« _____ » _____ 20 _____ г.

Рецензент

_____/_____/_____
Фамилия И.О. (подпись)

Ученая степень, ученое звание, место работы и должность

**Согласие на размещение текста
выпускной квалификационной работы обучающегося
в ЭБС ФГБОУ ВО Ставропольский ГАУ**

Я, _____
(фамилия, имя, отчество)

даю согласие ФГБОУ ВО Ставропольский ГАУ безвозмездно размещать (доводить до всеобщего сведения) написанную мною в рамках выполнения образовательной программы направления подготовки

_____ выпускную квалификационную работу
(далее – ВКР) бакалавра/ специалиста/ магистра – *нужное подчеркнуть*.
на тему: « _____

_____»

в следующем содержании:

- титульный лист ВКР;
 - содержание (план) ВКР;
 - введение (аннотация);
 - главы (разделы) ВКР, в которых излагается интеллектуальный труд;
 - заключение;
 - список использованных источников.
- (отметить нужное)

в сети Интернет в ЭБС ФГБОУ ВО Ставропольский ГАУ по адресу: <http://pps.stgau.ru/ebs/>, таким образом, чтобы любое лицо могло получить доступ к ВКР из любого места и в любое время по собственному выбору, в течение всего срока действия исключительного права на ВКР.

Я подтверждаю, что ВКР написана мною лично, в соответствии с правилами академической этики и не нарушает интеллектуальных прав иных лиц.

« _____ » _____ 20 г.
Дата

Подпись