Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)

Владикавказский филиал Финуниверситета

Кафедра «Математика и информатика»

Программа государственной итоговой аттестации

для студентов, обучающихся по направлению подготовки
10.04.01 Информационная безопасность
направленность программы магистратуры «Управление информационной безопасностью в кредитно-финансовой сфере»

Одобрено заседанием кафедры «Математика и информатика»
(протокол от «27» мая 2025 г. № 11)

Владикавказ 2025

Перечень компетенций, подлежащих оценке в ходе государственной итоговой аттестации для студентов, обучающихся по направлению подготовки 10.04.01 Информационная безопасность, направленность программы магистратуры «Управление информационной безопасностью в кредитно-финансовой сфере»

Код и наименование компетенции	Форма государственной итоговой аттестации, в рамках которой проверяется сформированность компетенции
Способность к абстрактному мышлению, критическому анализу проблемных ситуаций на основе системного подхода, выработке стратегии действий (УК-1)	Государственный экзамен и выпускная квалификационная работа
Способность применять коммуникативные технологии, владеть иностранным языком на уровне, позволяющем осуществлять профессиональную и исследовательскую деятельность, в т.ч. в иноязычной среде (УК-2)	Государственный экзамен и выпускная квалификационная работа
Способность определять и реализовывать приоритеты собственной деятельности в соответствии с важностью задач, методы повышения ее эффективности (УК-3)	Государственный экзамен и выпускная квалификационная работа
Способность к организации межличностных отношений и межкультурного взаимодействия, учитывая разнообразие культур (УК-4)	Государственный экзамен и выпускная квалификационная работа
Способность руководить работой команды, принимать организационно-управленческие решения для достижения поставленной цели, нести за них ответственность (УК-5)	Государственный экзамен и выпускная квалификационная работа
Способность принимать управленческие решения и решать управленческие задачи на всех этапах жизненного цикла проекта (УК-6)	Государственный экзамен и выпускная квалификационная работа
Способность проводить научные исследования, оценивать и оформлять их результаты (УК-7)	Государственный экзамен и выпускная квалификационная работа
Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов (ПКН-1)	Государственный экзамен и выпускная квалификационная работа
Способность проектировать системы обеспечения информационной безопасности конкретных объектов (ПКН-2)	Государственный экзамен и выпускная квалификационная работа
Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности (ПКН-3)	Государственный экзамен и выпускная квалификационная работа

Способность осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПКН-4)	Государственный экзамен и выпускная квалификационная работа
Способность проводить фундаментальные и прикладные исследования, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПКН-5)	Государственный экзамен и выпускная квалификационная работа
Способность обосновывать необходимость защиты информации в автоматизированной системе ФКС (ПК-1)	Государственный экзамен и выпускная квалификационная работа
Способность определять угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы (ПК-2)	Государственный экзамен и выпускная квалификационная работа
Способность разрабатывать архитектуры системы защиты информации автоматизированной системы кредитно-финансовой сферы (ПК-3)	Государственный экзамен и выпускная квалификационная работа
Способность моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации (ПК-4)	Государственный экзамен и выпускная квалификационная работа

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)

Владикавказский филиал Финуниверситета

Кафедра «Математика и информатика»

УТВЕРЖДАЮ
Директор филиала
_____ Т.А. Хубаев
«29» мая 2025 г.

А.М. Кумаритов

Программа государственного экзамена

для студентов, обучающихся по направлению подготовки
10.04.01 Информационная безопасность, направленность программы магистратуры «Управление информационной безопасностью в кредитно-финансовой сфере»

Рекомендовано Ученым советом Владикавказского филиала Финуниверситета
(протокол от «29» мая 2025 г. № 10)

Одобрено заседанием кафедры «Математика и информатика»
(протокол от «27» мая 2025 г. № 11)

Владикавказ 2025

СОДЕРЖАНИЕ

1. Перечень вопросов, выносимых на государственный экзамен. Перечень рекомендуемой литературы для подготовки к государственному экзамену

1.1. Вопросы на основе содержания общепрофессиональных и профессиональных дисциплин направления подготовки

1. Методы и технологии защиты информации в цифровой среде электронного документооборота.
2. Криптографические средства защиты информации в технологиях автоматизированной обработки информации.
3. Информационная война: содержание понятия, современное состояние.
4. Информационно-техническая война: становление, субъекты, объекты, развитие в современном мире.
5. Виды конфиденциальной информации и информация, содержащая государственную тайну. Особенности работы.
6. Программные, аппаратные и программно-аппаратные средства защиты информации.
7. Методы и средства технической защиты информации (ТЗИ).
8. Показатели оценки систем обнаружения вторжений: уровни наблюдения, методы обнаружения вторжений, адаптивность к неизвестным атакам, виды управления, устойчивость, расширяемость, виды ответных реакций, собственная защищённость, максимальная скорость съема информации.
9. Модель нарушителя и модель угроз при проектировании комплексных систем защиты информации объектов информатизации.
10. Каналы и способы скрытного внедрения в программно-техническую среду компьютерных и телекоммуникационных систем.
11. Технологии и средства идентификации и аутентификации при автоматизированной обработке информации.
12. Дискреционное, мандатное и ролевое управление доступом: описание, достоинства и недостатки.
13. Технологии и средства защиты информации в телекоммуникационных сетях и при сетевой организации автоматизированной обработки информации.
14. Концепция построения структурно-функциональной схемы системы защиты информации от несанкционированного доступа при автоматизированной обработке информации.

15. Достоинства и недостатки защиты информации в автоматизированных информационных системах, основанной на архитектуре сегментации среды обработки по признаку конфиденциальности, выделение контуров безопасности.

16. Структура комплексной системы защиты информации объекта информатизации.

17. Системные технологии обеспечения информационной безопасности корпораций как сложный организационно-технологический и программно-технический процесс с системной организацией и управлением.

18. Основные положения и организационно-технические технологии проведения аудита информационной безопасности автоматизированных информационных систем и объектов информатизации.

19. Содержание процессного подхода к управлению информационной безопасностью.

20. Стадии жизненного цикла автоматизированных систем. Особенности обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла.

21. Принципы построения имитационных моделей для анализа рисков в деятельности по обеспечению информационной безопасности.

22. Дискретно-событийное моделирование для учета риска.

23. Односторонние функции в криптографии. Схемы криптографии открытого ключа. Длина ключа и уровень безопасности.

24. Адреса в системе Биткоин. Транзакции. Верификация транзакций. Смарт-контракты.

25. Бизнес-модели блокчейн-проектов, построенных на основе токенов и обеспечение информационной безопасности.

1.2. Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам общепрофессиональных и профессиональных дисциплин

а) основная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2024. — 336 с. — (Высшее образование). — ISBN 978-5-369-01761-6. - URL: https://znanium.ru/catalog/product/2082642 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

б) дополнительная литература:

1. Понятийный аппарат информационной безопасности финансово-экономических систем = *The conceptual apparatus of the information security of financial and economic systems*: Энциклопедический словарь / Финуниверситет, Каф. "Информационная безопасность"; авт. - сост.: Г. О. Крылов, В. Л. Никитина. – Москва: Финуниверситет, 2016. – 255 с. – ЭБ Финуниверситета. – URL: http://elib.fa.ru/rbook/krylov.pdf - ЭБ Финуниверситета. - Текст: электронный.

2. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва: Гор. линия-Телеком, 2013. - 220 с.: ил. - ISBN 978-5-9912-0323-4 - URL: https://znanium.ru/catalog/product/421968 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

3. Рассолов, И. М. Информационное право: учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — URL: https://urait.ru/bcode/559788 – Режим доступа: Электронно-библиотечная система Юрайт. – Текст: электронный.

4. Ищейнов, В. Я. Информационная безопасность и защита информации: словарь терминов и понятий: словарь / В. Я. Ищейнов. — Москва: Русайнс, 2024. — 226 с. — ISBN 978-5-466-04502-4. — URL: https://book.ru/book/951881 — Режим доступа: Электронно-библиотечная система Book.ru. – Текст: электронный.

в) нормативные правовые акты

1. Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и защите информации» (с дополнениями и изменениями). – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ – Текст: электронный.

2. Федеральный закон № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ – Текст: электронный

3. Федеральный закон № 63-ФЗ от 06.04.2011 г. «Об электронной подписи». – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/– Текст: электронный

4. Стандарт ISO/IEC 27032:2023 «Кибербезопасность. Руководящие указания по обеспечению безопасности в Интернете». – URL: https://www.gostinfo.ru/catalog/Details/?id=7334018 – Текст: электронный.

5. Приказ ФСБ РФ № 66 от 09.02.2005 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями). – URL: https://www.consultant.ru/document/cons_doc_LAW_52098/ – Текст: электронный.

6. Приказ ФСТЭК № 21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375) (с изменениями). – URL: https://www.consultant.ru/document/cons_doc_LAW_146520/ – Текст: электронный.

7. Приказ ФСТЭК № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 г. № 28608) (с изм. и доп., вступ. в силу с 01.01.2021 г.). – URL: https://www.consultant.ru/document/cons_doc_LAW_147084/ – Текст: электронный.

8. Приказ Гостехкомиссии России № 187 от 19.06.2002 г. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. Руководящий документ. –URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/rukovodyashchij-dokument-ot-19-iyunya-2002-g-n-187– Текст: электронный

9. Приказ Гостехкомиссии России №282 от 30.08.2002 г. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – URL: https://rostransnadzor.gov.ru/storage/documents/prikazy-irasporyazheniya-rostransnadzora/Приказ-282-от-30.08.2002.doc – Текст: электронный

10. Решение Гостехкомиссии России от 30.03.1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утверждена решением Государственной технической комиссии при Президенте Российской Федерации. Принятые сокращения. Руководящий документ. – URL:

https://fstec.ru/dokumenty/vsedokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g – Текст: электронный.

11. Меры защиты информации в государственных информационных системах. Методический документ. ФСТЭК России, 11.02.2014 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g – Текст: электронный

12. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Выписка) (утв. ФСТЭК РФ 15.02.2008). – URL: https://www.consultant.ru/document/cons_doc_LAW_99662/ – Текст: электронный.

13. ГОСТ Р 34.10-2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – URL: https://protect.gost.ru/document.aspx?control=7&id=232149 – Текст: электронный.

14. ГОСТ Р ИСО 7498-2-99 Информационная технология. Архитектура защиты информации. – URL: https://protect.gost.ru/document.aspx?control=7&id=131456 – Текст: электронный.

15. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – URL: https://protect.gost.ru/document.aspx?control=7&id=134268 – Текст: электронный

16. ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. – URL: https://protect.gost.ru/document.aspx?control=7&id=187948 – Текст: электронный

17. ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240766 – Текст: электронный

18. ГОСТ Р ИСО/МЭК 27003-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы

менеджмента информационной безопасности. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240709 – Текст: электронный.

19. ГОСТ Р ИСО/МЭК 27004-2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240761 – Текст: электронный

20. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=177398 – Текст: электронный.

г) ресурсы информационно-телекоммуникационной сети «Интернет»

1. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
2. Электронно-библиотечная система BOOK.RU http://www.book.ru
3. Электронно-библиотечная система Znanium http://www.znanium.com
4. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru
5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
6. Электронная библиотека издательского дома «Гребенников» https://grebennikon.ru
7. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com
8. Информационно-правовой портал «Гарант». – Режим доступа: http://www.garant.ru/
9. Научная электронная библиотека eLibrary.ru http://elibrary.ru
10. Национальная электронная библиотека http://нэб.рф/

1.3. Вопросы на основе содержания дисциплин направленности программы магистратуры

1. Основные принципы информационно-аналитической работы по обеспечению комплексной безопасности.
2. Принципы оценки и анализа информации.

3. Методы и способы обработки материалов средств массовой информации.

4. Способы искажения информации и дезинформации.

5. Методы выявления и анализа конкурирующих фирм. Цели и задачи конкурентной разведки.

6. Интернет-разведка - как инструмент конкурентной разведки.

7. Сбор и анализ информации из открытых источников.

8. Структурные компоненты службы сообщений.

9. Национальные интересы и национальная безопасность. Доктрина информационной безопасности Российской Федерации.

10. Федеральный закон «Об информации, информационных технологиях и о защите информации».

11. Риск-ориентированный подход к обеспечению информационной безопасности.

12. Технологические меры защиты информации.

13. Защита персональных данных.

14. Организационные меры защиты информации

15. Построение модели нарушителя.

16. Процесс менеджмента рисков информационной безопасности (в соответствии с ISO/IEC 27005 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска ИБ»)

17. Понятие кибермошенничества и основные присущие ему черты. Виды кибермошенничества и основные схемы совершения кибермошенничества.

18. Требования к защите информации в финансовой сфере и методы контроля выполнения требований.

19. Методы и модели разграничения доступа.

20. Алгоритмы цифровой подписи DSA и ECDSA. Российский стандарт электронно-цифровой подписи. Проблема эффективности и безопасности.

21. Общее понятие протокола цифровой подписи. Алгоритмы распределения ключей. Цифровая подпись, основанная на схеме RSA.

22. Хэш-функции и их свойства. Коллизии. Устойчивость функций хеширования. Российский стандарт хеширования.

23. Архитектура смарт-контрактов ICO. Их преимущества и недостатки. Угрозы кибератак.

24. Электронные деньги и мобильные платежи. Мобильная коммерция и информационная безопасность. Защищенные модели мобильной коммерции.

25. Атаки в системах блокчейн. Атака двойной траты. Атака отказ в обслуживании. Форкатака. Атака удержанием блока. Атака 51% и др.

1.4. Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам дисциплин направленности программы магистратуры

а) основная литература

1. Генкин, А. Блокчейн: Как это работает и что ждет нас завтра: Научно-популярное / Генкин А., Михеев А. - М.: Альпина Паблишер, 2018. - 592 с.: ISBN 978-5-9614-6558-7. - URL: https://znanium.ru/catalog/product/1002003 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

2. Рассолов, И. М. Информационное право: учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — URL: https://urait.ru/bcode/559788 – Режим доступа: Электронно-библиотечная система Юрайт. – Текст: электронный.

3. Крылов, Г. О. Базовые понятия информационной безопасности: учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва: Русайнс, 2025. — 257 с. — ISBN 978-5-466-09255-4. — URL: https://book.ru/book/958467 — Режим доступа: Электронно-библиотечная система Book.ru. – Текст: электронный.

б) дополнительная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL: https://urait.ru/bcode/560804 – Режим доступа: Электронно-библиотечная система Юрайт. – Текст: электронный.

2. Вейнберг, Р. Р. Интеллектуальный анализ данных и систем управления бизнес-правилами в телекоммуникациях: Монография / Р.Р. Вейнберг. - Москва: НИЦ ИНФРА-М, 2016. - 173 с. (Научная мысль) ISBN 978-5-16-011350-0. - URL: https://znanium.com/catalog/product/520998 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

3. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2024. — 336 с. — (Высшее образование). — ISBN 978-5-369-01761-6. - URL:

https://znanium.ru/catalog/product/2082642 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

4. Романьков, В. А. Введение в криптографию: курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва: ФОРУМ: ИНФРА-М, 2025. — 240 с. — (Высшее образование). - ISBN 978-5-00091-493-9. - URL: https://znanium.ru/catalog/product/2178770 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

5. Чишти, С. Финтех. Путеводитель по новейшим финансовым технологиям: пер. с англ. / С. Чишти, Я. Барберис. - Москва: Альпина Паблишер, 2017. - 343 с. - ЭБС Alpina Digital. - URL: https://finunivers.alpinadigital.ru/book/11534 - ЭБ Финуниверситета. - Текст: электронный.

6. Муссель, К. М. Платежные технологии: системы и инструменты /К. М. Муссель. – Москва: КНОРУС: ЦИПСиР, 2015. – 288 с. – ЭБС Университетская библиотека online. – URL: http://biblioclub.ru/index.php?page=book&id=441393 – Режим доступа: Электронно-библиотечная система biblioclub.ru – Текст: электронный.

7. Зобнин, А. В. Информационно-аналитическая работа в государственном и муниципальном управлении: учебное пособие / А. В. Зобнин. — 3-е изд., испр. — Москва: ИНФРА-М, 2023. — 145 с. — (Высшее образование). — ISBN 978-5-16-014763-5. - URL: https://znanium.ru/catalog/product/1904564 – Режим доступа: Электронно-библиотечная система Znanium.com – Текст: электронный.

8. Сотов, А. И., Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография / А. И. Сотов. — Москва: Русайнс, 2020. — 127 с. — ISBN 978-5-4365-1091-0. — URL: https://book.ru/book/934740 — Режим доступа: Электронно-библиотечная система Book.ru. – Текст: электронный.

в) нормативные правовые акты

1. Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации № 1632-р от 28 июля 2017 г.

2. Федеральный закон: Выпуск 12(520). О национальной платежной системе. – Москва: ИНФРА-М, 2011. – 55 с. (Федеральный закон; Выпуск 12[520]). ISBN 978-516-005125-3. – Текст: электронный. – URL: https://znanium.com/catalog/product/237826

3. СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты

информационной безопасности при осуществлении переводов денежных средств» (Приказ Банка России от 30.11.2016 г. № ОД-4234). – URL: https://www.consultant.ru/document/cons_doc_LAW_208423/

4. СТО БР ИББС 1.0-2014. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения (Распоряжение Банка России от 17.05.2014 г. № Р399). – URL: https://www.consultant.ru/document/cons_doc_LAW_163762/

5. СТО БР БФБО-1.5.-2023. Стандарт Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности» (Приказ Банка России от 08.02.2023 N ОД215). – URL: https://www.consultant.ru/document/cons_doc_LAW_442070/

6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. – URL: https://protect.gost.ru/document.aspx?control=7&id=129024

7. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – URL: https://protect.gost.ru/document.aspx?control=7&id=129071

8. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. – URL: https://protect.gost.ru/document.aspx?control=7&id=183430

9. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. – URL: https://protect.gost.ru/document.aspx?control=7&id=129132

10. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – URL: https://protect.gost.ru/document.aspx?control=7&id=174974

11. ГОСТ Р 54581-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы. – URL: https://protect.gost.ru/document.aspx?control=7&id=179425

12. ГОСТ Р 54582-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия. – URL: https://protect.gost.ru/document.aspx?control=7&id=180146 (дата обращения: 04.04.2024).

13. ГОСТ Р 54583-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия. – URL: https://protect.gost.ru/document.aspx?control=7&id=180143 (дата обращения: 04.04.2024).

14. ГОСТ Р 56045-2021 Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240781 (дата обращения: 04.04.2024).

15. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – URL: https://protect.gost.ru/document.aspx?control=8&id=120843 (дата обращения: 04.04.2024).

16. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – URL: https://protect.gost.ru/document.aspx?control=7&id=128693

17. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – URL: https://protect.gost.ru/document.aspx?control=7&id=182696 (дата обращения: 04.04.2024).

18. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=184842

19. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=184748

20. ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=218340

21. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов

информационной безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=173886

22. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. – URL: https://protect.gost.ru/document1.aspx?control=31&id=184854

23. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. – URL: https://protect.gost.ru/document1.aspx?control=31&id=175594

24. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса. – URL: https://protect.gost.ru/document1.aspx?control=31&id=176523

25. ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240708 (дата обращения: 04.04.2024).

26. ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. – URL: https://protect.gost.ru/document.aspx?control=7&id=187948 (дата обращения: 04.04.2024).

27. ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240766 (дата обращения: 04.04.2024).

28. ГОСТ Р ИСО/МЭК 27003-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240709 (дата обращения: 04.04.2024).

29. ГОСТ Р ИСО/МЭК 27004-2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240761 (дата обращения: 04.04.2024).

30. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=177398

31. ГОСТ Р ИСО/МЭК 27006-2020 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=238756

32. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. – URL: https://protect.gost.ru/document.aspx?control=7&id=187871

33. ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. – URL: https://protect.gost.ru/document.aspx?control=7&id=187948

34. ГОСТ Р ИСО/МЭК 27037-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. – URL: https://protect.gost.ru/document.aspx?control=7&id=187854 (дата обращения: 04.04.2024).

35. ГОСТ Р ИСО/МЭК 29100-2013 Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности. – URL: https://protect.gost.ru/document.aspx?control=7&id=186203

г) ресурсы информационно-телекоммуникационной сети «Интернет»

1. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
2. Электронно-библиотечная система BOOK.RU http://www.book.ru
3. Электронно-библиотечная система Znanium http://www.znanium.com
4. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru
5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/

6. Электронная библиотека издательского дома «Гребенников» https://grebennikon.ru

7. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com

8. Информационно-правовой портал «Гарант». – Режим доступа: http://www.garant.ru/

9. Научная электронная библиотека eLibrary.ru http://elibrary.ru

10. Национальная электронная библиотека http://нэб.рф/ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». – URL: https://protect.gost.ru/document.aspx?control=7&id=180151.

11. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. – URL: https://protect.gost.ru/document.aspx?control=7&id=180209.

12. Baird L. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance //Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep. – 2016. – Режим доступа: http://pages.cpsc.ucalgary.ca/~joel.reardon/blockchain/readings/hashgraph.pdf.

2. Примеры практико-ориентированных заданий

1. Организация использует облачный сервис для хранения конфиденциальных документов, доступ к которым осуществляется через веб-интерфейс. Документы содержат коммерческую тайну и персональные данные сотрудников. Определите, какие меры контроля доступа должны быть реализованы для обеспечения конфиденциальности данных. Укажите, какие механизмы аутентификации и авторизации следует применить, а также какие дополнительные меры защиты данных в облачной среде необходимо предусмотреть. Ответ обоснуйте с учётом потенциальных угроз и требований регуляторов.

2. В организации произошёл инцидент, связанный с утечкой данных клиентов через уязвимость в корпоративном мессенджере. Расследование показало, что уязвимость была известна, но обновление не было установлено вовремя из-за отсутствия регламента управления обновлениями. Определите, какие элементы процесса управления уязвимостями были нарушены, и разработайте план восстановительных мероприятий. Укажите, какие меры необходимо внедрить для предотвращения подобных инцидентов в будущем, включая периодичность сканирования уязвимостей и порядок установки обновлений. Ответ обоснуйте с учётом лучших практик информационной безопасности.

3. Организация планирует внедрить систему видеонаблюдения на территории офиса, включая зоны отдыха и коридоры. Камеры будут передавать данные на внутренний сервер хранения, доступ к которому имеют сотрудники службы безопасности. Определите, в соответствии с какими нормативными требованиями должна быть организована система видеонаблюдения, учитывая возможную обработку персональных данных. Укажите, какие организационные и технические меры необходимо применить для минимизации рисков, включая вопросы хранения и удаления записей, разграничения доступа и информирования сотрудников. Ответ обоснуйте с учётом законодательства в области защиты персональных данных.

4. В ходе внутреннего аудита выявлено, что сотрудники бухгалтерии регулярно пересылают финансовые отчёты на личные почтовые ящики для работы вне офиса. При этом используется незашифрованная электронная почта, а пароли к учётным записям не менялись более года. Определите, какие нарушения информационной безопасности были допущены, и классифицируйте их по степени критичности. Разработайте план устранения нарушений, включая меры по повышению осведомлённости сотрудников и технические способы защиты данных. Укажите, в какие сроки должен быть проведён контроль выполнения корректировок и почему. Ответ обоснуйте с учётом требований политик информационной безопасности организации.

5. В ходе проверки IT-отдела компании-разработчика выявлено, что один из инженеров использует нелицензионное программное обеспечение для тестирования компонентов банковского приложения. При этом ПО входит в перечень критически важных для бизнес-процессов организации. Определите, какие нормативные требования были нарушены, и классифицируйте нарушение по степени тяжести. Разработайте план мероприятий по устранению нарушения, включая проверку всего парка ПО на предмет легальности использования. Укажите, в какие сроки должна быть проведена внеплановая проверка соответствия и почему, учитывая возможные последствия для репутации компании и риски штрафных санкций.

6. Кредитная организация планирует внедрить сервис дистанционного открытия вкладов с использованием биометрической идентификации через мобильное приложение. Проанализируйте, какие положения Федерального закона "О национальной платежной системе" и иных нормативных актов регулируют данный процесс. Определите, какие угрозы информационной безопасности возникают при реализации такого сервиса, включая риски подделки биометрических данных и перехвата транзакций. Предложите комплекс мер защиты, таких как многофакторная аутентификация, контроль целостности данных и мониторинг аномальной активности, обосновав их соответствие требованиям Банка России.

7. Сравните правовые основы функционирования платежных систем в России, США и одной из развивающихся стран (например, Индии). Выявите ключевые различия в регулировании электронных платежей, включая вопросы лицензирования операторов, защиты персональных данных и ответственности за мошеннические операции. Определите, какие риски для участников

расчетов возникают из-за различий в законодательстве, например, при трансграничных платежах или в случае кибератак на инфраструктуру платежной системы.

8. Проанализируйте тенденции развития цифровых валют, включая стейблкоины и CBDC (цифровые валюты центральных банков). Оцените, как изменяются тарифы на платежные услуги в условиях роста конкуренции между традиционными банками и финтех-компаниями. Рассмотрите технологические аспекты, такие как использование смарт-контрактов и распределенных реестров, а также требования к безопасности при проведении операций с цифровыми активами. Дайте прогноз, как развитие интернет-торговли повлияет на распространение криптоплатежей и какие регуляторные ограничения могут быть введены.

9. Исследуйте текущее состояние рынка мобильных платежей в России, включая такие сервисы, как СБП и мобильные приложения банков. Оцените перспективы их использования в сегментах микроплатежей, peer-to-peer переводов и оплаты услуг ЖКХ. Проанализируйте уязвимости мобильных платежных приложений, такие как недостатки в защите API, риски side-channel атак и социальной инженерии. Предложите меры повышения безопасности, включая применение аппаратных ключей и поведенческую биометрию, обосновав их эффективность.

10. Рассмотрите принципы взаимодействия между участниками платежной системы, включая банки, процессинговые центры и платежных агрегаторов. Опишите, как блокчейн-технологии могут быть использованы для ускорения расчетов на финансовых рынках, например, при клиринге или торговле ценными бумагами. Определите, какие механизмы защиты данных и контроля доступа должны быть реализованы в распределенных финансовых системах, чтобы соответствовать требованиям регуляторов и минимизировать риски мошенничества.

11. Рассмотрите виды электронных платежных услуг, предусмотренных Федеральным законом "О национальной платежной системе", включая переводы денежных средств, оплату товаров и услуг, а также операции с электронными денежными средствами. Опишите поэтапный процесс выполнения перевода между клиентами разных банков через систему быстрых платежей. Проанализируйте, как внедрение технологий открытого банкинга (Open API) и биометрической аутентификации может изменить традиционную схему платежей, учитывая новые угрозы, такие как атаки типа "man-in-the-middle" на API-интерфейсы или подделку биометрических данных. Предложите меры защиты, включая усовершенствованные методы верификации транзакций и мониторинга аномальной активности.

12. Определите наиболее распространенные виды мобильных платежных услуг в России, такие как оплата через QR-коды, переводы по номеру телефона и контактные платежи через NFC. Опишите механизмы обеспечения безопасности этих операций, включая использование токенизации данных карт, двухфакторной аутентификации и поведенческого анализа. Рассмотрите перспективы внедрения новых технологий для

повышения безопасности, таких как аппаратные ключи на базе Secure Element в мобильных устройствах или децентрализованные идентификаторы (DID) на блокчейне. Оцените, как развитие 5G-сетей и интернета вещей может расширить функциональность мобильных платежей при сохранении необходимого уровня защиты.

13. Проанализируйте влияние технологии блокчейн на современные платежные системы, включая снижение стоимости трансграничных переводов и ускорение расчетов между финансовыми институтами. Выявите специфические риски, связанные с использованием распределенных реестров, такие как уязвимости смарт-контрактов, атаки 51% на публичные блокчейны и проблемы регулирования в разных юрисдикциях. Рассмотрите, как центральные банки могут применять технологию блокчейн в системах цифровых валют (CBDC), обеспечивая при этом контроль за денежной массой и соблюдение требований AML/CFT.

14. Приведите примеры известных атак на смарт-контракты в блокчейн-сетях, таких как реентранси-атака на DAO или эксплуатация уязвимостей в протоколах DeFi. Опишите методы защиты, которые были разработаны в ответ на эти инциденты, включая формальную верификацию кода смарт-контрактов, внедрение механизмов задержки исполнения критических операций и использование специализированных языков программирования, таких как Michelson в Tezos. Оцените эффективность этих мер с точки зрения баланса между безопасностью и децентрализацией.

15. Определите ключевые факторы, увеличивающие банковские риски при использовании систем интернет-банкинга, включая фишинг, вредоносное ПО для кражи учетных данных и атаки на банковские API. Выделите системные проблемы информационной безопасности, такие как недостаточная сегментация корпоративных сетей, слабая защита периметра и отсутствие регулярного аудита кода финансовых приложений. Предложите комплекс мер по снижению рисков, включая внедрение систем мониторинга аномалий в режиме реального времени, обязательное использование аппаратных токенов для авторизации высокорисковых операций и регулярное обучение сотрудников по противодействию социальной инженерии.

16. Опишите основные векторы заражения персональных компьютеров вредоносным ПО, такие как эксплуатация уязвимостей в устаревшем программном обеспечении, фишинговые письма с вложениями и посещение скомпрометированных веб-сайтов. Рассмотрите, как злоумышленники используют зараженные компьютеры для создания бот-сетей, кражи конфиденциальных данных, криптоджекинга или атак типа "ransomware". Проанализируйте эффективность современных методов защиты, включая песочницы для изоляции подозрительных процессов, системы предотвращения вторжений (IPS) и регулярное обновление сигнатур антивирусных программ.

17. Сравните особенности компьютерных атак на автоматизированные рабочие места сотрудников кредитных организаций (АРМ КБР), терминалы SWIFT и устройства самообслуживания. Выделите

характерные для каждого типа систем угрозы, такие как атаки через уязвимости в ПО банкоматов, компрометация учетных данных операторов SWIFT или внедрение вредоносного кода в клиентские приложения интернет-банкинга. Опишите методы защиты, специфичные для каждого случая, включая физическую защиту банкоматов от скимминга, использование специализированных протоколов связи в системе SWIFT и контроль целостности ПО на рабочих местах сотрудников банка.

18. Проведите сравнительный анализ криптостойкости электронной цифровой подписи, реализованной на основе алгоритма RSA и схемы на эллиптических кривых (ECC) в соответствии с требованиями ГОСТ Р 34.10. Рассмотрите зависимость уровня безопасности от длины ключа, вычислительной сложности атак и требований к производительности. Оцените перспективы перехода на постквантовые алгоритмы электронной подписи в условиях развития квантовых вычислений, учитывая рекомендации международных и российских стандартов в области криптографии. Проанализируйте, как выбор алгоритма подписи влияет на скорость обработки транзакций в распределенных финансовых системах.

19. Рассмотрите перспективы применения методов стеганографии в банковской сфере для защиты транзакционных данных и конфиденциальной переписки. Проанализируйте возможность скрытой передачи реквизитов банковских карт через цифровые изображения или аудиофайлы, оценив преимущества такого подхода перед традиционным шифрованием с точки зрения незаметности для систем мониторинга. Укажите основные риски, связанные с возможностью злоупотребления стеганографией для обхода систем обнаружения мошенничества, и предложите методы противодействия, включая анализ статистических аномалий в медиафайлах и использование специализированных детекторов стеганографических вложений.

20. В организации произошел сбой, приведший к потере данных за последние сутки, при этом резервные копии создавались исправным оборудованием, но с интервалом 48 часов. Определите, какой параметр - RTO или RPO - был настроен некорректно в данной ситуации, и обоснуйте свой вывод, ссылаясь на определение этих показателей. Разработайте план мероприятий по исправлению ситуации, включающий пересмотр политики резервного копирования, тестирование процедур восстановления и внедрение системы мониторинга выполнения задач резервирования. Укажите, как часто следует проводить проверки корректности настроек резервного копирования после устранения инцидента.

21. При плановой проверке офиса обнаружено, что сотрудник бухгалтерии подключил к корпоративной сети персональный маршрутизатор для доступа к развлекательным ресурсам. Классифицируйте данное нарушение по степени критичности, учитывая потенциальные риски создания точки входа для злоумышленников в корпоративную инфраструктуру. Разработайте меры по устранению нарушения, включая блокировку несанкционированных устройств на уровне сетевого оборудования, пересмотр политики BYOD и проведение внеочередного инструктажа по

информационной безопасности для всех сотрудников. Обоснуйте необходимость проведения внеплановой проверки в течение недели с момента обнаружения инцидента.

22. В компании, где система онлайн-платежей классифицирована как критическая, необходимо определить статус серверов доменных имен. Обоснуйте, почему DNS-серверы должны получить аналогичную классификацию, учитывая их роль в обеспечении доступности электронной коммерции и риски атак типа DNS spoofing или DDoS на DNS-инфраструктуру. Предложите меры по защите DNS-серверов, включая внедрение DNSSEC, настройку избыточности и регулярный аудит конфигураций, подчеркнув необходимость согласованности уровня защиты с присвоенным классом критичности.

23. В ходе аудита разработки банковского приложения выявлено использование нелицензионного средства статического анализа кода. Оцените степень серьезности данного нарушения, учитывая потенциальные риски использования неподдерживаемого ПО с неисправленными уязвимостями. Разработайте план мероприятий по устранению нарушения, включающий инвентаризацию всего используемого ПО, приобретение лицензий и внедрение процесса контроля за использованием программного обеспечения. Обоснуйте необходимость проведения внеплановой проверки соответствия в течение двух недель с момента обнаружения факта нарушения.

24. В медицинском учреждении, имеющем филиалы в разных районах города, требуется организовать защищенный сегмент для обработки персональных данных пациентов, включая информацию о состоянии здоровья. Определите, какие нормативные документы (ФЗ-152, приказы ФСТЭК и ФСБ) регулируют создание такого сегмента, и сформулируйте конкретные требования к системе защиты, включая необходимость двухфакторной аутентификации, шифрования данных при передаче между филиалами и ведения журналов учета доступа. Обоснуйте выбор мер защиты, исходя из типа обрабатываемых данных и рассматриваемых угроз второго типа.

25. Вам как руководителю службы информационной безопасности кредитной организации необходимо разработать техническое задание на создание системы мониторинга и предотвращения инцидентов ИБ для сети отделений банка, расположенных в разных регионах. Техническое задание должно быть составлено в соответствии с требованиями ГОСТ 19.102-77 и включать следующие аспекты: описание угроз информационной безопасности, характерных для распределенной банковской инфраструктуры; требования к функциональности системы, включая обнаружение аномальной активности, анализ логов безопасности и интеграцию с существующими средствами защиты; технические характеристики, такие как производительность, масштабируемость и отказоустойчивость; требования к совместимости с действующими в банке системами; условия испытаний и ввода в эксплуатацию. Особое внимание следует уделить соответствию системы требованиям регуляторов, включая Банк России и ФСТЭК, а также

возможности оперативного реагирования на инциденты в режиме 24/7. В техническом задании необходимо предусмотреть этапы внедрения системы, включая пилотную эксплуатацию в тестовом регионе, и требования к обучению персонала работе с новой системой.

3. Рекомендации обучающимся по подготовке к государственному экзамену

Подготовку к сдаче государственного экзамена необходимо начать с ознакомления с перечнем вопросов, выносимых на государственный экзамен. Пользуйтесь при подготовке ответов рекомендованной обязательной и дополнительной литературой, а также лекционными конспектами, которые составляли.

Во время подготовки к экзамену рекомендуется помимо лекционного материала, учебников, рекомендованной литературы просмотреть также выполненные в процессе обучения задания для индивидуальной и самостоятельной работы.

В процессе подготовки ответа на вопросы необходимо учитывать изменения, которые произошли в законодательстве, увязывать теоретические проблемы с практикой сегодняшнего дня и опытом, полученным в период прохождения практики.

Обязательным является посещение консультаций и обзорных лекций, которые проводятся перед государственным экзаменом.

4. Критерии оценки результатов сдачи государственных экзаменов

Максимальное количество баллов, «отлично» (5 баллов), за ответ на теоретический вопрос экзаменационного билета ставится, если студент глубоко и полно раскрывает теоретические и практические аспекты вопроса, проявляет творческий подход к его изложению, и демонстрирует дискуссионность данной проблематики, а также глубоко и полно раскрывает дополнительные вопросы.

Количество баллов за ответ на теоретический вопрос экзаменационного билета снижается, если студент недостаточно полно освещает узловые моменты вопроса, затрудняется более глубоко обосновать те или иные положения, а также затрудняется ответить на дополнительные вопросы по данной проблематике.

Минимальное количество баллов «удовлетворительно» (3 балла) за ответ на теоретический вопрос экзаменационного билета ставится, если

студент не раскрывает основных моментов вопроса, логика изложения нарушена, ответы не всегда конкретны.

Оценка «неудовлетворительно» (2 балла) выставляется в случае, если материал излагается непоследовательно, не аргументировано, бессистемно, ответы на вопросы выявили несоответствие уровня знаний выпускника требованиям образовательного стандарта высшего образования ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры) в части формируемых компетенций.

Критерии оценки умений выпускников в ходе решения комплексных профессионально-ориентированных заданий:

- максимальное количество баллов «отлично» (5 баллов) ставится, если выпускник полностью справился с выполнением комплексного профессионально-ориентированного задания, обосновал полученные результаты;

- количество баллов снижается, если комплексное профессионально-ориентированное задание выполнено, но допускаются неточности в обосновании результатов;

- минимальное количество баллов «удовлетворительно» (3 балла) ставится, если практико-ориентированное задание, в основном, выполнено, намечен правильный ход решения, но допущены ошибки в процессе подсчетов, расчетов, в формировании выводов;

- оценка «неудовлетворительно» (2 балла) выставляется в случае, если отсутствует ответ на практико-ориентированное задание, либо нет решения, что означает несоответствие уровня подготовки выпускника требованиям к результатам освоения образовательной программы, включая дополнительные профессиональные компетенции, формируемые вузом;

Перед процедурой обсуждения ответов, экзаменующихся каждый член государственной экзаменационной комиссии, выставляет свою персональную оценку для каждого студента, используя сумму баллов, полученную после заполнения листа оценки студента.

Далее государственная экзаменационная комиссия рассматривает каждого выпускника отдельно: итоговая оценка представляет среднее арифметическое от суммы оценок, выставленных каждым членом комиссии.

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)

Владикавказский филиал Финуниверситета

Кафедра «Математика и информатика»

УТВЕРЖДАЮ
Директор филиала
Владикавказский филиал Финуниверситета
Т.А. Хубаев
«29» мая 2025 г.

А.М. Кумаритов

Методические рекомендации по подготовке и защите выпускной квалификационной работы

для студентов, обучающихся по направлению подготовки
10.04.01 Информационная безопасность,
направленность программы магистратуры «Управление информационной безопасностью в кредитно-финансовой сфере»

Одобрено заседанием кафедры «Математика и информатика»
(протокол от «27» мая 2025 г. № 11)

Владикавказ 2025

1. Общие положения

Образовательная программа высшего образования – программа магистратуры, реализуемая Владикавказским филиалом Финуниверситета по направлению подготовки 10.04.01 Информационная безопасность, направленность программы магистратуры «Управление информационной безопасностью в кредитно-финансовой сфере» (далее – ОП), разработана и реализуется в соответствии с основными положениями Федерального закона «Об образовании в Российской Федерации» (от 29.12.2012 г. № 273-ФЗ) и на основе образовательного стандарта высшего образования федерального государственного образовательного бюджетного учреждения высшего образования «Финансовый университет при Правительстве Российской Федерации» (далее – ОС ВО ФУ) с учетом требований рынка труда.

1.1. Выпускник, освоивший данную программу магистратуры, должен обладать следующими компетенциями:

Способность к абстрактному мышлению, критическому анализу проблемных ситуаций на основе системного подхода, выработке стратегии действий (УК-1)

Способность применять коммуникативные технологии, владеть иностранным языком на уровне, позволяющем осуществлять профессиональную и исследовательскую деятельность, в т. ч. в иноязычной среде (УК-2)

Способность определять и реализовывать приоритеты собственной деятельности в соответствии с важностью задач, методы повышения ее эффективности (УК-3)

Способность к организации межличностных отношений и межкультурного взаимодействия, учитывая разнообразие культур (УК-4)

Способность руководить работой команды, принимать организационно-управленческие решения для достижения поставленной цели, нести за них ответственность (УК-5)

Способность принимать управленческие решения и решать управленческие задачи на всех этапах жизненного цикла проекта (УК-6)

Способность проводить научные исследования, оценивать и оформлять их результаты (УК-7)

Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов (ПКН-1)

Способность проектировать системы обеспечения информационной безопасности конкретных объектов (ПКН-2)

Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности (ПКН-3)

Способность осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПКН-4)

Способность проводить фундаментальные и прикладные исследования, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПКН-5)

Способность обосновывать необходимость защиты информации в автоматизированной системе ФКС (ПК-1)

Способность определять угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы (ПК-2)

Способность разрабатывать архитектуры системы защиты информации автоматизированной системы кредитно-финансовой сферы (ПК-3)

Способность моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации (ПК-4)

2. Правила подготовки к защите ВКР

2.1. Требования к содержанию и продолжительности доклада по ВКР.

Для программ магистратуры доклад должен включать:

- обоснование актуальности избранной темы;
- описание научной проблемы и формулировку цели работы – положения, выносимые на защиту; – практическую значимость работы.

В заключительной части доклада перечисляются общие выводы и интересные результаты.

На доклад обучающемуся отводится не более 15 минут.

2.2. Требования к презентации ВКР.

Доклад должен сопровождаться презентацией, иллюстрирующей основные положения работы с использованием мультимедийных средств, выполненной в программе *PowerPoint*. Количество слайдов – 10-15.

2.3. Порядок определения результатов защиты ВКР в соответствии с пунктом 5.14 Положения о выпускной квалификационной работе по программам бакалавриата и магистратуры в Финансовом университете.

3. Критерии оценки ВКР

Оценка уровня сформированности компетенций выпускника программы магистратуры производится по результатам продемонстрированных выпускником навыков в соответствии с перечнем индикаторов достижения компетенций.

Оценка «*отлично*» выставляется при условии, что работа выполнена самостоятельно, носит творческий характер, прошла апробацию, охвачен широкий спектр теорий, концепций, подходов, обоснована авторская позиция; собран, обобщен, и проанализирован достаточный объем нормативных правовых актов, литературы, статистической информации и других практических материалов, позволивший всесторонне изучить тему и сделать аргументированные выводы и практические рекомендации; при написании и защите работы выпускником продемонстрирован высокий уровень развития компетенций, глубокие теоретические знания и наличие практических навыков; работа хорошо оформлена и своевременно представлена на кафедру, полностью соответствует требованиям, предъявляемым к содержанию и оформлению ВКР; на защите освещены все вопросы исследования, ответы обучающегося на вопросы профессионально грамотны, исчерпывающие, подкрепляются положениями нормативно-правовых актов, выводами и расчетами, отраженными в работе.

Оценка «*хорошо*» ставится, если тема работы раскрыта, однако выводы и рекомендации не всегда оригинальны и/или не имеют практической значимости, есть неточности при освещении отдельных вопросов темы; собран, обобщен и проанализирован необходимый объем нормативных правовых актов, литературы, статистической информации и других практических материалов, но не по всем аспектам исследуемой темы сделаны выводы и обоснованы практические рекомендации; при написании и защите работы выпускником продемонстрирован средний уровень развития компетенций, наличие теоретических знаний и достаточных практических навыков; работа своевременно представлена на кафедру, есть отдельные недостатки в оформлении; в процессе защиты работы дана общая характеристика основных положений работы, были неполные ответы на вопросы.

Оценка «*удовлетворительно*» ставится, когда тема работы раскрыта частично, но в основном правильно, допущено поверхностное изложение

отдельных вопросов темы; в работе не использован весь необходимый для исследования темы объем нормативных правовых актов, литературы, статистической информации и других практических материалов, выводы и практические рекомендации не всегда обоснованы; при написании и защите работы выпускником продемонстрированы удовлетворительный уровень развития компетенций, отсутствие глубоких теоретических знаний и устойчивых практических навыков; работа своевременно представлена на кафедру, однако не в полном объеме по содержанию и/или оформлению соответствует предъявляемым требованиям; в процессе защиты выпускник недостаточно полно изложил основные положения работы, испытывал затруднения при ответах на вопросы.

Оценка «*неудовлетворительно*» ставится, если в работе отсутствует формулировка положений, выносимых на защиту; содержание работы не раскрывает тему, вопросы изложены бессистемно и поверхностно, нет анализа практического материала, основные положения и рекомендации не имеют обоснования; работа не оригинальна, основана на компиляции публикаций по теме; при написании и защите работы выпускником продемонстрирован неудовлетворительный уровень развития компетенций; работа несвоевременно представлена на кафедру, не в полном объеме по содержанию и оформлению соответствует предъявляемым требованиям; на защите выпускник показал поверхностные знания по исследуемой теме, отсутствие представлений об актуальных проблемах по теме работы, плохо отвечал на вопросы.

Форма титульного листа ВКР

Федеральное государственное образовательное бюджетное
учреждение высшего образования

«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Владикавказский филиал Финуниверситета

Кафедра «Математика и информатика»

Выпускная квалификационная работа

на тему

«_____»

(наименование темы выпускной квалификационной работы)

Направление подготовки _____

(код и наименование направления подготовки)

_____

(наименование направленности)

Выполнил студент учебной группы

_____

(номер учебной группы)

_____

(фамилия, имя, отчество полностью)

Руководитель

_____

(ученая степень, ученое звание)

_____

(И.О. Фамилия)

ВКР соответствует
предъявляемым требованиям
Руководитель кафедры

_____

(ученая степень, ученое звание)

_____

(И.О. Фамилия)

«___» _____ 202_г.

Владикавказ – 202_ г.

Структура и содержание разделов ВКР, требования к оформлению ВКР

1. Структура и содержание разделов ВКР

1.1. ВКР должна включать следующие разделы:

– титульный лист (по форме согласно приложению № 8 к Положению о выпускной квалификационной работе по программам бакалавриата и магистратуры в Финансовом университете);

– содержание;

– введение;

– основная часть, структурированная на главы и параграфы;

– заключение;

– список использованных источников;

– – приложения (при наличии).

1.2. В содержании приводятся заголовки разделов, глав и параграфов, а также указываются страницы, с которых начинаются.

1.3. Во введении обосновывается актуальность темы ВКР, степень разработанности; цель, задачи, объект и предмет исследования; круг рассматриваемых проблем, описывается информационная база, выбираются методы научного исследования, обязательно отражается теоретическая и практическая значимость работы.

Первичным является объект исследования (более широкое понятие) – процесс или явление, избранное для изучения, т.е. объектом исследования является то, на что направлен научный поиск. Предметом исследования (некое частное, аспект объекта) принято считать ту из сторон или свойств объекта исследования, которая непосредственно подлежит изучению. Предмет исследования чаще всего близок к формулировке темы.

Цель исследования – это то, что в самом общем виде должно быть достигнуто в итоге исследования выпускной квалификационной работы. Определение цели исследования является центральной проблемой, при этом целью исследования в ВКР должно быть получение определенных результатов, а не сам процесс исследования.

Задачи вытекают из общей цели, определение начинается терминами исследовательских действий: изучить, уточнить, проанализировать, выяснить, обобщить, выявить, доказать, внедрить, определить, найти, описать, установить, разработать, выработать, экспериментально доказать и т.д. Формулировки задач необходимо делать как можно точнее и обычно

формулировки раскрывают содержание глав, параграфов ВКР (не больше 5 задач).

В качестве апробации результатов исследования (приоритетно для магистрантов) во введении также указывается участие обучающегося в НИР: гранты, конкурсы, выступления на конференциях, круглых столах и иных научных мероприятиях, выполнение НИР в рамках государственного задания или по договорам с организациями; имеющиеся научные публикации по теме исследования.

В конце введения раскрывается структура работы (дается краткий перечень структурных элементов, например, работа состоит из введения, двух глав, заключения, списка использованной литературы, который представлен 36 источниками, в том числе 3 на иностранном языке, и 8 приложений.

Введение должно быть кратким (2-3 стр.).

1.4. Основная часть ВКР включает главы и параграфы в соответствии с логической структурой изложения. Название главы не должно дублировать название темы, а название параграфов – названия глав. Формулировки должны быть лаконичными и отражать суть главы (параграфа).

Основная часть ВКР программ бакалавриата может включать две или три главы. ВКР программ магистратуры, как правило состоит из трех глав. Количество глав и параграфов в главе определяется обучающимся совместно с руководителем при составлении плана работы над ВКР.

При подготовке основной части выпускной квалификационной работы обязательными являются ссылки на использованные источники (научную, методическую или учебную литературу и т.д.). Наличие ссылок свидетельствует о качестве изучения темы, научной добросовестности автора работы. Воспроизведение материала без указания на источник квалифицируется как плагиат.

1.5. Первая глава содержит исторические, теоретические и методические аспекты исследуемой проблемы. Содержится обзор и анализ используемых источников информации по теме ВКР, раскрытие объекта и предмета исследования, различные теоретические концепции, принятые понятия и их классификации, а также своя аргументированная позиция по данному вопросу.

Сведения, содержащиеся в главе, должны давать полное представление о состоянии и степени изученности поставленной проблемы. В рамках главы, в частности, обобщается и систематизируется понятийный аппарат, дается критическая оценка имеющихся понятий, уточнение, приводятся классификации основных понятий по различным многокритериальным признакам, описываются теоретические концепции и эволюция взглядов научного сообщества по предмету исследования, а также имеющиеся средства

и методы измерения и решения рассматриваемой проблемы; характеризуется степень проработанности проблемы в России и за рубежом и др.

Подготовка первой главы проводится на базе предварительно подобранных литературных источников, в которых освещаются вопросы, в той или иной степени раскрывающие тему ВКР. Особое внимание следует обратить на законодательную, нормативную и специальную документацию, посвященную вопросам, связанным с предметом и объектом исследования.

Объем главы должен составлять 30-35% от всего объема ВКР.

Завершается первая глава обоснованием необходимости проведения аналитической части работы.

Глава должна иметь название, отражающее существо изложенного в нем материала. Не допускается выносить в качестве названия этой главы заголовки «*Теоретическая часть*», «*Обзор литературных источников*» и т. д.

1.6. Во второй главе ВКР анализируются особенности объекта исследования, а также практические аспекты проблем, рассмотренных в первой главе ВКР. Вторая глава посвящена анализу практического материала, собранного во время производственной (в том числе преддипломной) практики, содержит:

– анализ материала по избранной теме (на примере конкретной организации, отрасли, региона, страны, сферы) желательно за период не менее 3-х лет; сравнительный анализ с действующей практикой (на примере ряда организаций, отрасли/отраслей, региона/регионов, страны;

– описание выявленных закономерностей, проблем и тенденций развития объекта и предмета исследования;

– оценка эффективности принятых решений (на примере конкретной организации, отрасли, региона, страны).

В ходе анализа используются аналитические таблицы, расчеты, формулы, схемы, диаграммы и графики. Проведенный анализ в этой части работы позволит разработать конкретные мероприятия и предложения по совершенствованию и дальнейшему развитию объекта исследования. Предложения и рекомендации должны носить конкретный характер. Анализ современного состояния исследуемой проблемы включает в себя характеристику исследуемого объекта той или иной степени глубины, в зависимости от поставленных цели и задач, рассмотрение возможных причин, мешающих эффективному функционированию рассматриваемого объекта.

Практическая часть работы должна содержать самостоятельно проведенные обучающимся расчеты, составленный иллюстративный материал: рисунки (графики, диаграммы, схемы), таблицы. Весь иллюстративный материал должен быть проанализирован и использован для подтверждения выводов по исследуемой проблеме.

Объем второй главы должен составлять, как правило, 30-45% от всего объема ВКР.

1.7. В третьей главе рассматриваются и обосновываются направления решения выявленных проблем, предлагаются пути решения исследуемой/разрабатываемой проблемы; конкретные практические рекомендации и предложения по совершенствованию исследуемых/разрабатываемых явлений и процессов (если ВКР состоит из двух глав, указанное здесь содержание третьей главы находит отражение во второй практической главе). В главе должны быть сделаны самостоятельные выводы и представлены экономические расчеты.

В третьей главе ВКР программ магистратуры на основе проведенных исследований, как правило, анализируются результаты апробации авторского алгоритма (авторской методики) по решению рассматриваемой проблемы; формулируются конкретные практические рекомендации и предложения по совершенствованию исследуемых явлений и процессов, в том числе по внесению изменений в нормативные правовые акты; разрабатываются пути решения проблемной ситуации и определяется научный вклад автора.

Объем третьей главы должен составлять, как правило, 20-30% от всего объема ВКР.

1.8. Завершающей частью текста ВКР является заключение, которое содержит выводы и предложения из всех глав ВКР с их кратким обоснованием в соответствии с поставленной целью и задачами, раскрывает значимость полученных результатов. При этом выводы общего порядка, не вытекающие из результатов и содержания ВКР, не допускаются. Выводы также не могут подменяться механическим повторением выводов по отдельным главам.

Объем заключения, должен составлять, как правило, до пяти страниц. Заключение является основой доклада обучающегося на защите ВКР.

1.9. Список использованных источников должен содержать сведения об источниках, которые использовались или были изучены при подготовке ВКР (не менее 60 наименований – для программ магистратуры) и характеризует осведомленность обучающегося по изучаемой проблеме.

Список использованных источников располагаться в следующем порядке:

– законы Российской Федерации (в прямой хронологической последовательности);

– указы Президента Российской Федерации (в той же последовательности); постановления Правительства Российской Федерации (в той же очередности); нормативные акты, инструкции (в той же очередности);

– иные официальные материалы (резолюции-рекомендации международных организаций и конференций, официальные доклады, официальные отчеты, материалы судебной практики и др.);

– монографии, учебники, учебные пособия (в алфавитном порядке);

– авторефераты диссертаций (в алфавитном порядке);

– научные статьи (в алфавитном порядке);

– литература на иностранном языке (в алфавитном порядке); интернет-источники.

1.10. Приложения включают дополнительные справочные и расчетные материалы, необходимые для полноты исследования, но имеющие вспомогательное значение, например: копии документов, выдержки из отчетных материалов, статистические данные, схемы, таблицы, диаграммы, программы, положения, детальные расчеты, описания и т.п.

2. Требования к оформлению ВКР

2.1. На титульном листе выпускной квалификационной работы указывается наименование кафедры, группы, название темы выпускной квалификационной работы, фамилия и инициалы автора работы и руководителя, год написания работы.

2.2. Оформление ВКР должно производиться по общим правилам ГОСТ 7.322017 в ред. изменения от 12.09.2018 г. «Отчет о научно-исследовательской работе. Структура и правила оформления».

2.3. Научно-справочный аппарат оформляется в соответствии с российскими национальными и межгосударственными ГОСТами:

– ГОСТ Р 7.0.100-2018 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии № 1050-ст от 03.12.2018 г.); – ГОСТ 7.80-2000 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Заголовок. Общие требования и правила составления» (утвержден и введен в действие Постановлением Государственного комитета Российской Федерации по стандартизации и метрологии № 253-ст от 06.10.2000 г.);

- ГОСТ 7.82-2001 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание электронных ресурсов» (утвержден и введен в действие

Постановлением Государственного комитета Российской Федерации по стандартизации и метрологии № 369-ст от 04.09.2001 г.);

– ГОСТ Р 7.0.12-2011 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов на русском языке. Общие требования и правила» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии № 813-ст от 13.12.2011 г.);

– ГОСТ 7.11-2004 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на иностранных европейских языках» (принят Межгосударственным советом по стандартизации, метрологии и сертификации (протокол № 24 от 05.12.2003 г.).

2.4. ВКР оформляется в текстовом редакторе на листах бумаги формата *А4*, содержит примерно 1800 знаков на странице (включая пробелы и знаки препинания). Текст следует набирать через 1,5 интервала, шрифт *Times New Roman*, размер шрифта – *min* – 13, *max* – 14, в таблицах – размер шрифта 12, в подстрочных сносках – размер шрифта 10. Подчеркивание слов и выделение их курсивом не допускается.

2.5. Страницы, на которых излагается текст, должны иметь поля: верхнее и нижнее – не менее 20 мм; левое – не менее 30 мм; правое – не менее 10 мм; колонтитулы: верхний – 2; нижний – 1,25.

2.6. Названия структурных элементов «введение», «заключение», «список литературы (использованных источников) и интернет-ресурсов», «приложение» являющиеся заголовками, печатаются прописными буквами, а названия параграфов (подзаголовки) – строчными буквами (кроме первой прописной). Заголовки и подзаголовки при печатании текста письменной работы на принтере выделяются полужирным шрифтом.

Заголовки, подзаголовки и подстрочные сноски (состоящие из нескольких строк) печатаются через одинарный интервал.

2.7. Абзацный отступ должен соответствовать 1,25 см и быть одинаковым по всей работе.

2.8. Нумерация разделов производится арабскими цифрами, а именно:

Пример − 1. Понятие и виды сделок.

1.1. Понятие сделки

Главы делятся на параграфы и нумеруются арабскими цифрами, а именно: **Пример** − Глава 1. Понятие и виды сделок

1.1. Понятие сделки

Параграфы/разделы должны иметь нумерацию в пределах каждой главы/раздела, а главы/разделы – в пределах всего текста работы.

Если глава содержит только один параграф (что нежелательно), то нумеровать не нужно.

Нумерация страниц.

Страницы ВКР должны нумероваться арабскими цифрами, нумерация должна быть сквозная, по всему тексту работы. Номер страницы проставляют, начиная со второй, в центре нижней части листа без точки.

Титульный лист включается в общую нумерацию страниц работы, однако номер страницы не ставится.

Если в работе имеются иллюстрации и таблицы на отдельном листе, то включаются в общую нумерацию страниц работы.

Каждую главу работы следует начинать с нового листа.

Параграф начинать с нового листа не следует.

2.9. Иллюстрации и таблицы.

Если в работе имеются схемы, таблицы, графики, диаграммы, рисунки, то следует располагать непосредственно после текста, в котором упоминаются впервые, или на следующей странице. Иллюстрации следует нумеровать арабскими цифрами сквозной нумерацией (то есть по всему тексту) – 1, 2, 3, и т.д., либо внутри каждой главы – 1.1, 1.2 и т.д.

При наличии в работе таблицы наименование (краткое и точное) должно располагаться над таблицей без абзацного отступа в одну строку. Таблицу, как и рисунок, располагать непосредственно после текста, в котором она упоминаются впервые, или на следующей странице. Таблицы в тексте следует нумеровать сквозной нумерацией арабскими цифрами по всему тексту или в рамках главы (2.1 и т.д.). Если таблица вынесена в приложение, то она нумеруется отдельно арабскими цифрами с добавлением перед номером слова «Приложение» – Приложение 1.

Если таблица имеет заголовок, то пишется с прописной буквы, и точка в конце не ставится. Разрывать таблицу и переносить часть ее на другую страницу можно только в том случае, если целиком не умещается на одной странице. При этом на другую страницу переносится и шапка таблицы, а также заголовок «*Продолжение таблицы*».

Пример оформления таблицы:

Таблица 2.1.

Расходы на оплату труда

Должность	**Количество**	**Зарплата, руб.**
1	**2**	**3**
Генеральный директор	1	55000
Исполнительный директор	1	40000
Бухгалтер	1	25000
Итого:		

2.11. Цитирование, ссылки и сноски.

При дословном использовании материала для подтверждения важной мысли или существенного положения используется цитирование. При цитировании необходимо соблюдать следующие правила:

–текст цитаты заключается в кавычки, и приводится в той грамматической форме, в какой дан в источнике, с сохранением особенностей авторского написания; цитирование должно быть полным, без произвольного сокращения цитируемого фрагмента и без искажения смысла. Пропуск слов, предложений, абзацев при цитировании допускается, если не влечет искажение всего фрагмента, и обозначается многоточием, которое ставится на место пропуска;

–если цитата включается в текст, то первое слово пишется со строчной буквы;

–если цитата выделяется из основного текста, то пишут от левого поля страницы на расстоянии абзацного отступа, при этом каждая цитата должна сопровождаться ссылкой на источник.

В случае цитирования необходима ссылка на источник, откуда приводится цитата, оформленная в соответствии с национальным стандартом Российской Федерации ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28.04.2008 г. № 95-ст).

В ВКР используются ссылки в форме подстрочных сносок, которые оформляются внизу страницы, где расположен текст, например, цитата. Для этого в конце текста/цитаты ставится цифра или звездочка, обозначающая порядковый номер сноски на данной странице. Например,

«*Накачка мировой экономики деньгами усилилась, когда в 1999 г. администрация США сняла ограничения на запрет банкам, венчурным, пенсионным и другим фондам заниматься инвестициями, выпуском*

ипотечных бумаг, игрой на валютных биржах и фондовых рынках, другими высокорискованными, но приносящими максимальные прибыли спекулятивными операциями. Неконтролируемый рост денежной массы привел к тому, что с 2006 г. ФРС США вообще перестал контролировать общий индекс».[1]

---

[1].Бушуев В.В. Финансовые кризисы и волатильность нефтяного рынка // Мировой кризис и глобальные перспективы энергетических рынков: (материалы совместного заседания Ученых советов Института мировой экономики и международных отношений РАН и Фонда «Институт энергетики и финансов» 22.05.2009 г.) / сост. и науч.

ред. С. В. Чебанов. М.: ИМЭМО РАН, 2009. С. 67.

Нумерация подстрочных сносок может быть сквозной по всему тексту письменной работы.

Ссылки на главы, рисунки, таблицы должны начинаться со строчной буквы, например, см. рис. 2.5., результаты приведены в табл. 3.1.

2.12. Список литературы (использованных источников) и интернет-ресурсов. После заключения, начиная с новой страницы, необходимо поместить список литературы (использованных источников) и интернет-ресурсов.

Список литературы (использованных источников) должен содержать подробную и достаточную информацию о каждом использованном источнике. Такая информация различна в зависимости от вида источника.

В любом случае, основой оформления списка использованных источников является библиографическое описание источников в соответствии с вышеперечисленными ГОСТами.

2.13. Образцы библиографических описаний документов в списках литературы.

1. Описание книги одного автора

Никифорова Н.А. Комплексный экономический анализ: учеб, для напр. бакалавриата «Экономика» и «Менеджмент»/Н.А. Никифорова; Финуниверситет. – Москва: Кнорус, 2021. – 439 с. – (Бакалавриат).

Шитов В.Н. История финансов России: учеб, пособие для студентов вузов, обуч. по спец. «Финансы и кредит», напр. «Экономика» (квалиф. (степень) «бакалавр»)/В.Н. Шитов. – 3-е изд., стер. – Москва: Кнорус, 2020. – 156 с. – (Бакалавриат).

2. Описание книги 2, 3-х авторов

Перская В. В. Интеграция в условиях многополярности. Эволюция теории и практики реализации = Integration processes amid multipolarity. Evolution of theory and practice of implementation: монография / Перская В. В., Эскиндаров М.А. – Москва: Экономика, 2016. – 383 с.

Валишин Е. Н. Теория и практика управления человеческими ресурсами: учеб, пособие / Е. Н. Валишин, И. А. Иванова, В. Н. Пуляева; Финуниверситет. – Москва: Русайнс, 2020. – 127 с.

Rose P. S. Bank Management & Financial Services / P.S. Rose, S. Hudgins. – 8-th ed. – Boston: Me Graw Hill, 2010. – 734 p.

3. Описание книги 4-х авторов

История России: учебник / А. С. Орлов, В.А. Георгиев, Н. Г. Георгиева, Т. А. Сивохина; МГУ им. М.В. Ломоносова. – 4-е изд., перераб. и доп. – Москва: Проспект, 2020. – 528 с. IELTS Foundation: Student's Book. CEF Levels B1-B2 / Andrew Preshous, Rachael Roberts, Joanna Preshous, Joanne Gakonga. – 2-nd ed. – Oxford: Macmillan Publishers Limited, 2014. – 176 с. – (Macmillan Exams).

4. Описание книги 5-ти и более авторов

Современная архитектура финансов России: монография/М. А. Эскиндаров, В. В. Масленников, М.А. Абрамова [и др.]; под ред. М. А. Эскиндарова, В. В. Масленникова; Финуниверситет. – Москва: Когито-Центр, 2020. – 487 с.

Сто лет развития. 1919-2019 / авт.-сост.: Я. А. Пляйс, С. Л. Анохина, Т. А. Мирошникова [и др.]; под общ. ред. М. А. Эскиндарова; Финансовый ун-т при Правительстве Российской Федерации. – Москва: Международные отношения, 2019. – 696 с.

5. Описание сборников

Сборник научных статей V Международной научной конференции «Институциональная экономика: развитие, преподавание, приложения», 15 ноября 2017 г. – Москва: ГУУ, 2017. – 382 с. Сборник избранных статей молодых ученых / Ин-т экономики РАН; под ред.

И. А. Болдырева, М. Ю. Головнина, Р. С. Гринберга. – Москва: Экономика, 2010. – 288 с. – (Библиотека Новой экономической ассоциации /ред. кол. серии: В. М. Полтерович, М. А. Эскиндаров, Б. М. Смитиенко [и др.]).

6. Описание статей из газет, журналов и сборников

Четвериков В. М. Особенности и интенсивность распространения COVID-19 в странах большой экономики//Вопросы статистики. – 2020. – № 6. – С. 86-104.

Баталова А. Пусть в финансовую элиту. Более 400 школьников стали победителями и призерами олимпиады «Миссия выполнима!»/Баталова А., Дуэль А.// Российская газета. – 2020. – 5 марта. – № 48. – С. 10.

Рыкова И.Н. Оценка кредитоспособности компаний нефтегазовой отрасли в современных условиях развития банковской деятельности/И. Н.

Рыкова, Д. Ю. Табуров, А. В. Борисова//Банковское дело. – 2019. – № 12. – С. 41-50.

Пивоварова М.А. Кластерные инициативы: общее и особенное/ М.А.Пивоварова//Кластерные инициативы в формировании прогрессивной структуры национальной экономики: сб. науч. тр. 2-й Международной науч.-практич. конф. (1718 марта 2016 г.). Т. 1 / Юго-Западный гос. ун-т; отв. ред. А.А. Горохов. – Курск, 2016. – С. 173-177.

Morozko N. I. (Морозко Н. И.) Business management strategy based on value- oriented concepts / Morozko N. I. (Морозко Н. И.), Didenko V.Y. (Диденко В. Ю.) // The Strategies of Modem Science Development: Proceedings of the X International scientific-practical conference (North Charleston, USA, 12-13 April 2016). – USA, North Charleston, 2016. – pp. 79-81.

7. Описание нормативных правовых актов

Бюджетный кодекс Российской Федерации: по состоянию на 20 февраля 2019 г.: сравнительная таблица изменений. – Москва: Проспект, 2019. – 368 с.

Об общих принципах организации местного самоуправления в Российской Федерации: Федер, закон № 131-ФЗ: [принят Государственной думой 16 сент. 2003 г.: одобрен Советом Федерации 24 сент. 2003 г.]. – Москва: Проспект; Санкт-Петербург: Кодекс, 2017. – 158 с.

О внесении изменений в Федеральный закон «О специальной оценке условий труда»: Федер, закон от 27 дек. 2019 г. № 451-ФЗ: принят Государственной Думой 17 дек. 2019 г.: одобрен Советом Федерации 23 дек. 2019 г. // Российская газета. – 2019. – 30 дек. – № 295. – С. 14.

Об образовании в Российской Федерации: Федер, закон от 29 дек. 2012 г. №273ФЗ: [принят Государственной Думой 21 дек. 2012 г.: одобрен Советом Федерации 26 дек. 2012 г.] // Собрание законодательства Российской Федерации. – 2012. – 31 дек. – № 53. – Ст. 7598.

ГОСТ Р 57564-2017. Организация и проведение работ по международной стандартизации в Российской Федерации = *Organization and implementation of activity on international standardization in Russian Federation*: изд. офиц.: утв. и введен в действие Приказом Федерального агентства по технич. регулированию и метрологии от 28 июля 2017 г. № 767-ст: дата введения 2017-12-01 / разработан Всероссийским науч.-исслед. ин-том стандартизации и сертификации в машиностроении (ВНИИНМАШ). – Москва: Стандартинформ, 2017. – V, 44 с.

8. Описание диссертаций, авторефератов диссертаций, депонированных рукописей

Славин Б. Б. Теоретические основы и инструментальная поддержка технологий коллективного интеллекта в управлении организацией: дис. д-ра экон, наук; спец. 08.00.13; защищена 17.06.2020; утверждена 23.06.2020 /

Славин Б. Б.; Место защиты: Финуниверситет; Работа выполнена: Финуниверситет, Департамент анализа данных. – Москва, 2020. – 342 с.: ил.

Величковский Б. Б. Функциональная организация рабочей памяти: автореф. дисс. докт. психол. наук: спец. 19.00.01 / Величковский Б. Б.; Московский гос. ун-т им. М. В. Ломоносова; Место защиты: Ин-т психологии РАН. – Москва, 2017. – 44 с.

Лабынцев Н. Т. Профессионально-общественная аккредитация и независимая оценка квалификаций в области подготовки кадров и осуществления бухгалтерской деятельности/Н. Т. Лабынцев, Е. А. Шароватова; Ростовский гос. экон, ун-т (РИНХ). – Ростов-на-Дону, 2017. – 305 с. – Деп. в ВИНИТИ РАН 10.01.2017 г. № 1-В2017.

9. Описание дисков и других ресурсов локального доступа

Эриашвили Н.Д. Банковское право: электрон, учеб, для студентов вузов/Н. Д. Эриашвили. – 8-е изд., перераб. и доп. – Электрон, дан. – Москва: ЮНИТИ-ДАНА, 2011. – 1 электрон, опт. диск (CD-ROM). – Загл. с этикетки диска.

Развитие промышленного производства Сибирского федерального округа: стат. сб. / Федер, служба гос. статистики, Территор. органы Федер, службы гос. статистики. – Электрон, дан. – Омск, 2012. – 1 электрон, опт. диск (CD-ROM). – Загл. с контейнера.

10. Описание электронных ресурсов сетевого распространения

Веснин В. Р. Основы менеджмента: учебник/В.Р. Веснин. – Москва: Проспект, 2016. – 500 с. – ЭБС Проспект. – URL: http://ezpro.fa.ru:3180/book/23323 (дата обращения: 19.01.2024). – Текст: электронный.

Салин В.Н. Банковская статистика: учеб, и практикум для вузов/В. Н. Салин, О.Г. Третьякова. – Москва: Юрайт, 2020. – 215 с. – (Высшее образование). – ЭБС Юрайт. – URL: https://ezpro,fa.ru:3217/bcode/450266 (дата обращения: 18.01.2024). – Текст: электронный.

Adhiry B.K. Crowdfunding: Lessons from Japan’s Approach / Bishnu Kumar Adhiry, Kenji Kutsuna, Takaaki Hoda; Kobe University Social Science Research Series. – Singapore: Springer Ltd., 2018. – 110 с. – SpringerLink. – URL: https://link.springer.com/chapter/10.1007/978-981-13-1522-0 7 (дата обращения: 10.12.2024). – Текст электронный.

Российская социально-экономическая система: реалии и векторы развития: монография / П.В. Савченко, Р.С. Гринберг, М.А. Абрамова [и др.]; отв. ред. Р.С. Гринберг, П.В. Савченко. – 3-е изд., перераб. и доп. – 3-е изд. – Москва: ИНФРА-М, 2019. – 598 с. – (Научная мысль). – ЭБС Znanium.com. – URL: https://new.znanium.com/catalog/product/961584 (дата обращения: 10.12.2020). – Текст: электронный.

Дадашев А.З. К вопросу о финансовой самостоятельности муниципальных образований и методах оценки ее уровня / А.З. Дадашев, А.И. Золотько. – Текст: электронный // Финансы и кредит. – 2018. – № 9. – С. 2017-2032. – НЭБ ELibrary. – URL: https://www.elibrary.ru/download/elibrary 35648256 50368935.pdf (дата обращения: 10.12.2024).

Конъюнктурный анализ практики внедрения профессиональных стандартов в России в 2018 году / А.А. Цыганов, А.С. Ермолаева, С.В. Бровчак, Е.В. Богданова. – Текст: электронный // Перспективы науки и образования. – 2019. – № 5. – С. 517-528. – ЭБ Финуниверситета. – URL: https://pnoiournal.files.wordpress.eom/2019/l1/pdf 190537.pdf. – Дата публикации: 31.10.2019.

2.14. Общие требования к приложениям.

Приложения – дополнительные к основному тексту материалы справочного, документального, иллюстративного или другого характера. Приложения размещаются в конце работы, после списка использованной литературы в порядке упоминания в тексте. Каждое приложение должно начинаться с нового листа, и иметь тематический заголовок и общий заголовок «Приложение № ___».

Если приложение представляет отдельный рисунок или таблицу, то оформляется в соответствии с требованиями, предъявляемыми к иллюстрациям, таблицам.

Иллюстрации и таблицы нумеруются в пределах каждого приложения в отдельности. Например: рис. 3.1 (первый рисунок третьего приложения), таблица 1.1 (первая таблица первого приложения).

Приложения могут оформляться отдельной брошюрой. В этом случае на титульном листе брошюры указывается: Приложение к выпускной квалификационной работе, и далее приводится название работы и автор.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения учебных занятий, предусмотренных программой магистратуры, оснащенная оборудованием и техническими средствами обучения.

Аудитория № 33.

Специализированная мебель:

Стол (учительский) – 1 шт.

Стол компьютерный – 1 шт.

Стол (студенческий) двухместный – 13 шт.

Стулья – 28 шт.

Доска меловая – 1 шт.

Шкаф для документов – 3 шт.

Технические средства обучения:

Компьютер в сборе – 1 шт.

Интерактивная панель – 1 шт.

Комплект (2 шт.) аудио колонок для воспроизведения аудио файла – 1 шт.

Подключение к сети «Интернет» и обеспечение доступа к электронной информационно-образовательной среде Финансового университета.

Помещение для самостоятельной работы.

Кабинет № 55. Читальный зал.

Специализированная мебель:

Стол – 20 шт.

Стул – 40 шт.

Шкаф для книг – 4 шт.

Стеллаж книжный – 13 шт.

Стеллаж выставочный – 4 шт.

Технические средства обучения:

Компьютер в сборе – 6 шт.

Телевизор – 1 шт.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети «Интернет»

и обеспечением доступа к электронной информационно - образовательной среде Финансового университета.