**Федеральное государственное образовательное бюджетное учреждение высшего образования**
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
**(Финансовый университет)**

**Департамент информационной безопасности**

**Факультет информационных технологий и анализа больших данных**

# Программа государственной итоговой аттестации

для студентов, обучающихся по направлению подготовки
10.04.01 «Информационная безопасность»,
направленность программы магистратуры -
«Информационная безопасность финансово-кредитных организаций»

*Одобрено заседанием Совета Департамента информационной безопасности*
*протокол №5 от 14 декабря 2021 г.*

**Москва 2021**

**Перечень компетенций, подлежащих оценке в ходе государственной итоговой аттестации для студентов, обучающихся по направлению подготовки 10.04.01 «Информационная безопасность», направленность программы магистратуры - «Информационная безопасность финансово-кредитных организаций»**

| Код и наименование компетенции | Форма государственной итоговой аттестации, в рамках которой проверяется сформированность компетенции |
|---|---|
| 1 | 2 |
| способность к абстрактному мышлению, анализу, синтезу (ОК-1) | Защита ВКР |
| способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2) | Государственный экзамен<br><br>Защита ВКР |
| способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1) | Государственный экзамен<br><br>Защита ВКР |
| способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2) | Государственный экзамен<br><br>Защита ВКР |
| способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1) | Защита ВКР |
| способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2) | Защита ВКР |
| способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3) | Защита ВКР |
| способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4) | Государственный экзамен<br><br>Защита ВКР |
| способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5) | Защита ВКР |
| способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6); | Защита ВКР |
| способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7) | Государственный экзамен<br><br>Защита ВКР |

| | |
|---|---|
| способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8) | Защита ВКР |
| способность проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9) | Государственный экзамен<br>Защита ВКР |
| способность проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10) | Государственный экзамен<br>Защита ВКР |
| способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности (ПК-11) | Защита ВКР |
| способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12) | Защита ВКР |
| способностью организовать управление информационной безопасностью (ПК-13) | Государственный экзамен<br>Защита ВКР |
| способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14) | Защита ВКР |
| способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15). | Государственный экзамен<br>Защита ВКР |
| способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации па системы и средства обеспечения информационной безопасности (ПК-16) | Государственный экзамен<br>Защита ВКР |
| способность разрабатывать модели угроз и оценивать возможности внешних и внутренних нарушителей безопасности автоматизированной системы финансово-кредитной организации (ДКН-1) | Государственный экзамен<br>Защита ВКР |
| способность классифицировать и оценивать угрозы информационной безопасности для объекта информатизации предприятий финансово-кредитной сферы (ДКН-2) | Государственный экзамен<br>Защита ВКР |
| способность осуществлять меры противодействия нарушениям сетей безопасности предприятий финансово-кредитной сферы с использованием различных программных и аппаратных средств защиты и принимать меры защиты информации при выявлении новых угроз безопасности информации (ДКН-3) | Государственный экзамен<br>Защита ВКР |
| способность формирования политик информационной безопасности организации предприятий финансово-кредитной сферы, с учетом порядка аттестации компьютерных систем на предмет их соответствия требованиям по информационной безопасности и выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний (ДКН-4) | Государственный экзамен<br>Защита ВКР |

**Федеральное государственное образовательное бюджетное учреждение высшего образования**
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
**(Финансовый университет)**

**Департамент информационной безопасности**

**Факультет информационных технологий и анализа больших данных**

УТВЕРЖДАЮ
Проректор по учебной работе по
учебной и методической работе

_____Е.А. Каменева

# Баранов А.П.

# Программа государственного экзамена

для студентов, обучающихся по направлению подготовки
10.04.01 «Информационная безопасность»,
направленность программы магистратуры -
«Информационная безопасность финансово-кредитных организаций»

*Одобрено заседанием Совета Департамента информационной безопасности*

*протокол №5 от 14 декабря 2021 г.*

**Москва 2021**

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ 6

1 Перечень вопросов, выносимых на государственный экзамен. Перечень рекомендуемой литературы для подготовки к государственному экзамену 7

1.1 Вопросы на основе содержания общепрофессиональных и профессиональных дисциплин направления подготовки 7

1.2 Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам общепрофессиональных и профессиональных дисциплин 99

1.3 Вопросы на основе содержания дисциплин направленности программы магистратуры 13

1.4 Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам дисциплин направленности программы магистратуры 15

2 Примеры практико-ориентированных заданий 22

3 Рекомендации обучающимся по подготовке к государственному экзамену 30

4 Критерии оценки результатов сдачи государственных экзаменов 30

# ВВЕДЕНИЕ

В соответствии с Федеральным государственным образовательным стандартом высшего образования подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1513, государственный экзамен, как форма итоговой государственной аттестации, направлен на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВО.

Программа государственного экзамена по направлению подготовки 10.04.01 «Информационная безопасность» (квалификация (степень) – магистр) разработана в соответствии с ФГОС ВО, а также Приказом Министерства образования Российской Федерации № 636 от 29 июня 2015 г. «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры».

## 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. Информационная война: становление и содержание понятия.
2. Информационно-техническая война: становление, субъекты, объекты, развитие в современном мире.
3. Особенности работы с конфиденциальной информацией и информацией, содержащей государственную тайну.
4. Становление и содержание понятия «информационно-психологическая безопасность».
5. Программные и аппаратные средства противодействия угрозам.
6. Средства технической разведки.
7. Дать характеристику критериальных показателей 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).
8. Сформулировать цели и задачи модели нарушителя при проектировании комплексных систем защиты информации объектов информатизации с учётом их киберпространства.
9. Сформулировать и обосновать основные задачи развития систем обнаружения вторжений.
10. Сформулировать и обосновать понятие информационного общества, проблемы и вызовы, связанные с информационной безопасностью.
11. Предложить решения по обеспечению доверенной организационно-технологической среды и условий защищённости на объектах размещения средств автоматизированной обработки и передачи информации.
12. Определить методы и технологии защиты информации при электронном документообороте.

13. Определить и обосновать целесообразность и эффективность применения криптографических средств защиты информации в технологиях автоматизированной обработки информации.

14. Перечислить и обосновать основные каналы и способы скрытного внедрения в программно-техническую среду компьютерных и телекоммуникационных систем.

15. Выполнить анализ и сравнить по критериям эффективности и затрат на реализацию технологии и средства аутентификации при автоматизированной обработке информации.

16. Выполнить анализ и сравнить по критериям эффективности и технологичности дискреционное, мандатное и ролевое управление доступом.

17. Рассмотреть виды компьютерных вирусов и предложить технологии и средства защиты от вирусов и антивирусную политику на объекте информатизации.

18. Определить основные технологии и средства защиты информации в телекоммуникационных сетях и при сетевой организации автоматизированной обработки информации.

19. Предложить концепцию построения структурно-функциональной схемы системы защиты информации от несанкционированного доступа при автоматизированной обработке информации.

20. Обосновать достоинства и недостатки защиты информации в автоматизированных информационных системах, основанной на архитектуре сегментации среды обработки по признаку конфиденциальности (выделение контуров безопасности).

21. Предложить и обосновать структуру комплексной системы защиты информации (КСЗИ) объекта информатизации.

22. Представить системные технологии обеспечения информационной безопасности корпораций как сложный организационно-технологический и программно-технический процесс с системной организацией и управлением.

23. Сформулировать и обосновать основные положения и организационно-технические технологии проведения аудита информационной безопасности автоматизированных информационных систем и объектов информатизации.

24. Содержание процессного подхода к управлению ИБ.

25. Перечислить стадии жизненного цикла автоматизированных систем. В связи с чем возникают особенности обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла?

26. Принципы построения имитационных моделей для анализа рисков в деятельности по обеспечению ИБ.

27. Дискретно-событийное моделирования для учета риска.

28. Односторонние функции. Схемы криптографии открытого ключа. Длина ключа и уровень безопасности.

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

30. 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 . - Москва: РИОР, 2014. - 256 с. - Текст : непосредственный. 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, 2019. — 322 с. — (Высшее образование). — ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/1009606 (дата обращения: 30.01.2020). - Текст : электронный. *Может быть рекомендовано бакалаврам и магистрам.

2. 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. – Текст : непосредственный. - То же. – ЭБ

Финуниверситета. - URL: http://elib.fa.ru/rbook/krylov.pdf (дата обращения: 30.01.2020). - Текст : электронный.

**б) дополнительная:**

1. Башлы, П.Н. Информационная безопасность и защита информации: учебник/ П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва: РИОР, 2013. — 222 с. — ЭБС ZNANIUM.com. — URL: https://new.znanium.com/catalog/product/405000 (дата обращения: 30.01.2020). — Текст: электронный.

2. Гришина, Н. В. Основы информационной безопасности предприятия: учебное пособие / Н. В. Гришина. — Москва: ФОРУМ, 2019. – 216 с. – (Высшее образование: Бакалавриат). — ЭБС ZNANIUM.com. – URL: https://new.znanium.com/catalog/product/1017663 (дата обращения: 30.01.2020). - Текст : электронный.

3. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – Москва: Гор. линия – Телеком, 2013. – 220 с. - ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/421968 (дата обращения: 30.01.2020). - Текст : электронный.

4. Рассолов, И.М. Информационное право: учебник для магистров, обуч. по юридич. напр. и спец. / И.М. Рассолов. - Москва: Юрайт, 2015. - 448 с. – Текст : непосредственный. Рассолов, И. М. Информационное право : учебник и практикум / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 347 с. — (Бакалавр. Специалист. Магистр). — ЭБС Юрайт. — URL: https://www.biblio-online.ru/bcode/431833 (дата обращения: 30.01.2020). - Текст : электронный.

**в) нормативно-правовые акты**

3. Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации» (с дополнениями и изменениями).

4. Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».

5. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ.

6. Стандарт ISO 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».

7. Приказ ФСБ РФ от 09.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями).

8. 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» (с изменениями).

9. Приказ ФСТЭК № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в редакции 2019 г.).

10. Приказ Гостехкомиссии России № 187, 2002 г. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1,2,3. Руководящий документ.

11. Приказ Гостехкомиссии России № 282, 2002 г. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).

12. Решение Гостехкомиссии России, 1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ.

13. Меры защиты информации в государственных информационных системах. Методический документ. ФСТЭК России, 2014 г.

14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методический документ. ФСТЭК России, 2008 г. (обновление 2013 г.).

15. ГОСТ Р 34.10-2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

16. ГОСТ Р ИСО 7498-2-99 Информационная технология. Архитектура защиты информации.

17. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

18. 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.

19. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002.

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

21. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

22. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

**г) ресурсы информационно-телекоммуникационной сети «Интернет»**

25. Справочная правовая система «Консультант Плюс»http:/consultant.ru/

26. Справочная правовая система «Гарант»http:/garant.ru/

27. Российская научная библиотека www.rsl.ru.

28. Код безопасности - www.securitycode.ru.

29. Искусство управления информационной безопасностью. (Руководящие документы Гостехкомиссии, ФСТЭК, ФСБ) - www.iso27000.ru.

30. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/(http://library.fa.ru/files/elibfa.pdf)

31.Электронно-библиотечная система BOOK.RU http://www.book.ru

32.Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/

33.Электронно-библиотечная система Znanium http://www.znanium.com

34. «Деловая онлайн библиотека» издательства «Альпина Паблишер» http://lib.alpinadigital.ru/en/library

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

36. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/

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

38. Информационно-образовательный портал Финансового университета при Правительстве Российской Федерации http://portal.ufrf.ru/.

**1.3 Вопросы на основе содержания дисциплин направленности программы магистратуры**

1. Содержание информационно-аналитической работы по обеспечению комплексной безопасности.
2. Основные показатели качества информации, используемой для анализа.
3. Основные принципы информационно-аналитической работы по обеспечению комплексной безопасности.
4. Принципы оценки и анализа информации.
5. Методы и способы обработки материалов средств массовой информации.
6. Способы искажения информации и дезинформации.
7. Методы выявления и анализа конкурирующих фирм.
8. Цели и задачи конкурентной разведки.
9. Интернет-разведка - как инструмент конкурентной разведки.
10. Сбор и анализ информации из открытых источников.
11. Структурные компоненты службы сообщений
12. Национальные интересы и национальная безопасность
13. Доктрина информационной безопасности Российской Федерации.

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

15. Риск-ориентированный подход к обеспечению информационной безопасности.

16. Технологические меры защиты информации

17. Защита персональных данных.

18. Организационные меры защиты информации

19. Построение модели нарушителя

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

21. Федеральный закон «О государственной тайне».

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

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

24. Классы межсетевых экранов. Применение межсетевых экранов в АС в банковской сфере.

25. Методы и модели разграничения доступа.

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

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

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

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

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

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

32. Основные факторы, повышающие уровни банковских рисков при использовании систем электронного банкинга и наиболее серьезные проблемы системного характера с точки зрения банковского надзора в условиях применения систем электронного банкинга.

33. Основные способы заражения персонального компьютера вредоносным программным обеспечением.

34. Основные способы использования зараженного компьютера.

35. Особенности компьютерных атак на АРМ КБР, АРМ SWIFT и на устройства самообслуживания (банкоматы, терминалы и др.).

36. Основные факторы, повышающие уровни банковских рисков при использовании систем электронного банкинга.

37. Особенности использования систем электронного банкинга в противоправных действиях (отмывание денег и финансирование терроризма).

### 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 / А. Генкин, А. Михеев. — Москва: Альпина Паблишер, 2018. — 592 с. - ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/1002003 (дата обращения: 30.01.2020). - Текст: электронный.

2. Рассолов, И.М. Информационное право: учебник для магистров, обуч. по юридич. напр. и спец. / И.М. Рассолов. - Москва: Юрайт, 2015. - 448 с. – Текст : непосредственный. Рассолов, И. М. Информационное право : учебник и практикум / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 347 с. — (Бакалавр. Специалист. Магистр). — ЭБС Юрайт. — URL: https://www.biblio-online.ru/bcode/431833 (дата обращения: 30.01.2020). - Текст : электронный.

3. Крылов, Г.О. Базовые понятия информационной безопасности: учебное пособие / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина. - Москва: Русайнс, 2017. - 258 с. – Текст : непосредственный. - То же.- ЭБС BOOK.ru. - URL: https://www.book.ru/book/922531(дата обращения: 30.01.2020). - Текст : электронный.

**б) дополнительная**

4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Юрайт, 2017. — 209 с. — Текст: непосредственный. — (Серия : Бакалавр. Академический курс). - То же. - 2019.- ЭБС Юрайт. — URL: https://biblio-online.ru/bcode/433420 (дата обращения: 30.01.2020). - Текст : электронный.

5. Вейнберг, Р.Р. Интеллектуальный анализ данных и систем управления бизнес-правилами в телекоммуникациях : монография / Р.Р. Вейнберг. — Москва: НИЦ ИНФРА-М, 2016. — 173 с. — ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/520998 (дата обращения: 30.01.2020). — Текст : электронный.

6. Башлы, П.Н. Информационная безопасность и защита информации: учебник/ П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва: РИОР, 2013. — 222 с. — ЭБС ZNANIUM.com. — URL: https://new.znanium.com/catalog/product/405000 (дата обращения: 30.01.2020). — Текст: электронный.

7. Романьков, В. А. Введение в криптографию : Курс лекций/ В.А. Романьков. - Москва: ФОРУМ : ИНФРА-М, 2018. - 240 с. – ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/924700 (дата обращения: 30.01.2020). - Текст : электронный.

8. Чишти, С. Финтех. Путеводитель по новейшим финансовым технологиям: пер. с англ. / С. Чишти, Я. Барберис. - Москва: Альпина Паблишер, 2017. - 343 с. - Текст : непосредственный. - То же. - ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/1003177 (дата обращения: 30.01.2020). – Текст : электронный.

9. Дербин, Е.А. Организационные основы обеспечения информационной безопасности предприятия: учебное пособие / Е.А. Дербин, С.М. Климов; Финуниверситет, Каф. "Информационная безопасность" — Москва: Финуниверситет, 2013. — Информационно-образовательный портал Финуниверситета.—URL: http://http://portal.ufrf.ru/Content/Data/bfe5ac2d-d57d-4f4a-9929-3d440cab52cb/Elektr_uch._posobie_OOIB1.pdf (дата обращения: 30.01.2020) — Текст : электронный.

10. 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 (дата обращения: 30.01.2020). – Текст : электронный.

11. Зобнин, А. В. Информационно-аналитическая работа в государственном и муниципальном управлении : учебное пособие / А. В.Зобнин, Д. И. Полывянный. - Москва: Вузовский учебник, 2015. - 144 с. – ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/491423 (дата обращения: 30.01.2020). - Текст : электронный.

12. Сотов, А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации : монография / А.И. Сотов. — Москва: Русайнс, 2017. — 128 с. — ЭБС BOOK.ru. — URL: https://www.book.ru/book/920258 (дата обращения: 30.01.2020). —Текст : электронный.

**в) нормативно-правовые акты**

1. Программа "Цифровая экономика Российской Федерации". Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. N 1632-р 11.

2. Федеральный закон: Выпуск 12 (520). О национальной платежной системе. — Москва: ИНФРА-М, 2011. — 55 с. — Режим доступа: http://znanium.com/catalog.php?bookinfo=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».

4. СТО БР ИББС 1.0-2014. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

5. СТО БР БФБО-1.5.-2018. Стандарт Банка России. Безопасность финансовых (банковских) операций управления инцидентами информационной безопасности.

6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

7. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

8. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения.

9. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества.

10. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

11. ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.

12. ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.

13. ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.

14. ГОСТ Р 56045-2021Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности.

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.

16. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.

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.

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.

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.

20. ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

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

22. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

23. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

24. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.

25. ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

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.

27. ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.

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

29. ГОСТ Р ИСО/МЭК 27004-2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание.

30. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

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.

32. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

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.

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.

35. ГОСТ Р ИСО/МЭК 29100-2013 Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности.

**г) ресурсы информационно-телекоммуникационной сети «Интернет»**

36. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/(http://library.fa.ru/files/elibfa.pdf)

37. Электронно-библиотечная система BOOK.RU http://www.book.ru

38. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/

39. Электронно-библиотечная система Znanium http://www.znanium.com

40. «Деловая онлайн библиотека» издательства «Альпина Паблишер» http://lib.alpinadigital.ru/en/library

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

42. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/

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

44. Информационно-образовательный портал Финансового университета при Правительстве Российской Федерации http://portal.ufrf.ru/.

45. Справочная правовая система «Консультант Плюс»http:/consultant.ru/.

46. Справочная правовая система «Гарант»http:/garant.ru/.

47. Российская научная библиотека www.rsl.ru.

48. Код безопасности - www.securitycode.ru.

49. Искусство управления информационной безопасностью. (Руководящие документы Гостехкомиссии, ФСТЭК, ФСБ) - www.iso27000.ru.

50. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» http://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

51. ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи http://kaf403.rloc.ru/POVS/Crypto/GOST_R_34.10-2001.pdf

52. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования http://kaf403.rloc.ru/POVS/Crypto/GOST_R_34.10-2001.pdf

53. Развитие технологии распределенных реестров. М: ЦБР, 2017, 1-16 Режим доступа: https://www.cbr.ru/content/document/file/36007/reestr_survey.pdf

54. Технология распределенного реестра: за рамками блокчейн. — Правительство. Управление науки. Отчет главного научного советника Правительства Великобритании, 2015. — с. 1-88. — Режим доступа: https://mpdblog.ru/wp-content/uploads/2017/07/bitkoin-tekhnologia-raspredelennogo.pdf

55. 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

56. Buterin V. A next-generation smart contract and decentralized application platform. White paper. — Режим доступа: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

## 2 Примеры практико-ориентированных заданий

1. Организация использует схему классификации, позволяющую определить критичность системы с точки зрения возможности аварийного восстановления. Основное приложение организации для ведения электронной коммерции классифицировано как «Критическое». Продумайте и опишите: как организация должна классифицировать DNS-серверы организации? Ответ обоснуйте.

2. При аварии были потеряны все необходимые для возобновления бизнес-операций данные. Известно, что оборудование, производившее резервное копирование не было повреждено, а причина кроется в неправильных настройках резервного копирования. Продумайте и опишите какое из значений RTO или RPO

было установлено неверно? Какие действия необходимо предпринять? Ответ обоснуйте.

3. В организации, имеющей несколько территориально-распределённых объектов (в разных частях города), необходимо выделить отдельный сегмент компьютеров, которые бы занимались обработкой персональных данных. Обрабатываются данные клиентов компании. Количество записей - менее 100000. Тип персональных данных – специальные. Рассматриваемые угрозы 2 типа.

Определите, в соответствии с какими нормативными документами необходимо провести работы по выделению отдельного сегмента компьютеров. Уточните требования безопасности к данной системе и обоснуйте их.

4. В ходе обследования отдела кадров в районе рабочего места одного из сотрудников была обнаружена точка доступа. Сотрудник объяснил, что точка доступа приобретена для личных целей как обеспечение соединения ноутбука с сетью для посещения web-сайтов и просмотра фильмов online в обеденное время.

Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

5. Во время интервью с программистом IT компании было выяснено, что он работает над разработкой софта для клиента. На вопрос аудитора об авторизации прикладного программного обеспечения, использованного для разработки логического симулятора, было выяснено, что одна из программ не была зарегистрирована у поставщика.

Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

6. ПАО «Локобанк» запускает сервис по выдаче онлайн-кредитов без посещения офиса. Какие возможности в настоящее время предоставляет российское законодательство для реализации подобной идеи? Можно ли получить кредит без посещения офиса в соответствии с банковским законодательством? Какие угрозы ИБ здесь присутствуют и как им противодействовать?

7. Сравнить законодательную основу национальных платежных систем развитых и развивающихся стран (на примере 3-х стран, включая Россию). Определить потенциальные риски для участников систем электронных расчетов.

8. Описать перспективы развития электронных денег и криптовалют: тарифы, технологии, инфраструктура, статус денежных посредников. Оценить влияние развития Интернет-торговли на выбор методов платежа. Описать современные требования к платежам в Интернет с позиций ИБ.

9. Провести анализ построения системы мобильной коммерции в России. Оценить перспективы их развития в конкретных сегментах розничных платежей. Дать оценку безопасности мобильных приложений. Ответ обосновать.

10. Описать, как осуществляется взаимодействие инфраструктур платежной системы на финансовом рынке. Дать предложение, как технология блокчейн может использоваться при расчетах на финансовых рынках и обеспечению их ИБ.

11. Назвать виды платежных услуг, перечисленных в российском законодательстве. Описать процесс совершения платежной услуги и дайте предложения по его возможному изменению с новыми технологиями и новыми информационными угрозами.

12. Перечислить розничные платежные услуги, наиболее часто совершаются с мобильного устройства. Как решается проблема безопасности мобильных платежей? Описать возможные перспективы развития безопасных платежных услуг на основе мобильных устройств.

13. Оценить влияние технологии блокчейн на платежную индустрию и возникающие при этом риски.

14. Привести примеры реальных атак на функционирующие смарт-контракты и раскрыть примененные способы защиты.

15. Указать основные факторы, повышающие уровни банковских рисков при использовании систем электронного банкинга и наиболее серьезные проблемы системного характера с точки зрения ИБ в условиях применения систем электронного банкинга.

16. Перечислить основные пути заражения персонального компьютера вредоносным программным обеспечением. Описать основные способы использования зараженного компьютера.

17. Перечислить особенности компьютерных атак на АРМ КБР, АРМ SWIFT и на устройства самообслуживания (банкоматы, терминалы и др.).

18. Предположим, что агенты $A_1$ и $A_2$ передают друг другу информацию, используя систему кодирования RSA. Пусть $N_i$, $e_i$, $d_i$ соответственно открытый модуль, открытый ключ и секретный ключ агента $A_i$, $i = 1,2$. Для передачи подписанного сообщения $m$ агенту $A_2$ агент $A_1$ поступает следующим образом. Кодирует свое сообщение, вычисляя $c \equiv m^{e_2} \bmod N_2$; применяя функцию хеширования, вычисляет $s \equiv Hash(m)^{d_1} \bmod N_1$ и пересылает агенту $A_2$ пару $(c, s)$. Описать алгоритм извлечения агентом $A_2$ исходного сообщения $m$ и верификации подписи. Оценить возможность подделки подписи злоумышленником.

19. Провести сравнительный анализ стойкости ЭЦП, основанной на схеме кодирования RSA и на эллиптических кривых, опираясь на алгоритмы и значения параметров, содержащиеся в ГОСТ.

20. Оценить возможности и перспективы использования компьютерной стеганографии в банковской сфере.

21. При аварии были потеряны все необходимые для возобновления бизнес-операций данные. Известно, что оборудование, производившее резервное копирование не было повреждено, а причина кроется в неправильных настройках резервного копирования. Задание: Продумайте и опишите какое из значений RTO или RPO было установлено неверно? Какие действия необходимо предпринять? Ответ обоснуйте.

22. Во время посещения отдела кадров на столе была обнаружена точка доступа. Сотрудник объяснил, что точка доступа приобретена для личных целей как обеспечение соединения ноутбука с сетью для посещения web-сайтов и просмотра фильмов online в обеденное время. Задание: Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

23. Организация использует схему классификации, позволяющую определить критичность системы с точки зрения возможности аварийного восстановления. Основное приложение организации для ведения электронной коммерции классифицировано как «Критическое». Задание: Продумайте и опишите: как организация должна классифицировать DNS-серверы организации? Ответ обоснуйте.

24. Во время интервью с программистом IT компании было выяснено, что он работает над разработкой софта для клиента. На вопрос аудитора об авторизации прикладного программного обеспечения, использованного для разработки логического симулятора, было выяснено, что одна из программ не была зарегистрирована у поставщика. Задание: Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

25. В организации, имеющей несколько территориально-распределённых объектов (в разных частях города), необходимо выделить отдельный сегмент компьютеров, которые бы занимались обработкой персональных данных. Обрабатываются данные клиентов компании. Количество записей - менее 100000. Тип персональных данных – специальные. Рассматриваемые угрозы 2 типа. Задание: Определите, в соответствии с какими нормативными документами необходимо провести работы по выделению отдельного сегмента компьютеров. Уточните требования безопасности к данной системе и обоснуйте их.

26. Вы – главный специалист по защите информации в ПАО «АКБ «Абсолют Банк». Задание: Разработать техническое задание для информационно-аналитической системы безопасности в соответствии с ГОСТ 19.102-77

27. Вы – руководитель отдела исследований и разработок в АО «Автоградбанк» Задание:

Разработать технический проект информационно-аналитической системы безопасности в соответствии с ГОСТ 19.102-77

28. Вы – руководитель отдела исследований и разработок в ПАО «Азиатско-Тихоокеанский Банк». Задание: Сформировать требования по реализации функций

обеспечения информационной безопасности к техническому заданию на создание автоматизированной системы (в соответствии с ГОСТ 34.601-90)

29. Вы – заместитель руководителя отдела исследований и разработок в АО «Банк «Агророс». Задание: Составить план основных мероприятий на этапе «внедрения» проекта информационно-аналитической системы безопасности в соответствии с ГОСТ 19.102-77

30. Вы – руководитель отдела исследований и разработок в ПАО «Азиатско-Тихоокеанский Банк». Задание: Сформировать требования по реализации функций обеспечения информационной безопасности к техническому заданию на создание автоматизированной системы (в соответствии с ГОСТ 34.601-90)

31. Вы – руководитель отдела исследований и разработок в ПАО «АКБ «Ак Барс». Задание: Сформировать требования по взаимодействию с создаваемыми и (или) эксплуатируемыми обеспечивающими системами к техническому заданию на создание автоматизированной системы (в соответствии с ГОСТ 34.601-90)

32. Вы – руководитель отдела исследований и разработок в ПАО «Банк Уралсиб». Задание: Сформировать требования к составу ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин, ресурсов доступа, расположенных на серверах электронной почты, ресурсов доступа, расположенных на WEB-серверах информационно-телекоммуникационной сети Интранет, ресурсов доступа, расположенных на WEB-серверах информационно-телекоммуникационной сети Интернет), в соответствии с ГОСТ 34.601-90.

33. Организация использует схему классификации, позволяющую определить критичность системы с точки зрения возможности аварийного восстановления. Основное приложение организации для ведения электронной коммерции классифицировано как «Критическое». Задание: Продумайте и опишите: как организация должна классифицировать DNS-серверы организации? Ответ обоснуйте.

34. Во время интервью с программистом IT компании было выяснено, что он работает над разработкой софта для клиента. На вопрос аудитора об авторизации прикладного программного обеспечения, использованного для разработки

логического симулятора, было выяснено, что одна из программ не была зарегистрирована у поставщика. Задание:

Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

35. В организации, имеющей несколько территориально-распределённых объектов (в разных частях города), необходимо выделить отдельный сегмент компьютеров, которые бы занимались обработкой персональных данных. Обрабатываются данные клиентов компании. Количество записей - менее 100000. Тип персональных данных – специальные. Рассматриваемые угрозы 2 типа. Задание: Определите, в соответствии с какими нормативными документами необходимо провести работы по выделению отдельного сегмента компьютеров. Уточните требования безопасности к данной системе и обоснуйте их.

36. При аварии были потеряны все необходимые для возобновления бизнес-операций данные. Известно, что оборудование, производившее резервное копирование не было повреждено, а причина кроется в неправильных настройках резервного копирования. Задание: Продумайте и опишите какое из значений RTO или RPO было установлено неверно? Какие действия необходимо предпринять? Ответ обоснуйте.

37. Во время посещения отдела кадров на столе была обнаружена точка доступа. Сотрудник объяснил, что точка доступа приобретена для личных целей как обеспечение соединения ноутбука с сетью для посещения web-сайтов и просмотра фильмов online в обеденное время. Задание: Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

38. Вы – руководитель отдела исследований и разработок в ПАО «Банк Уралсиб». Задание: Сформировать требования к составу ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин, ресурсов доступа, расположенных на серверах электронной почты, ресурсов доступа, расположенных на WEB-серверах информационно-телекоммуникационной сети Интранет, ресурсов

доступа, расположенных на WEB-серверах информационно-телекоммуникационной сети Интернет), в соответствии с ГОСТ 34.601-90

39. Вы – руководитель отдела исследований и разработок в АО «Банк Жилищного Финансирования». Задание: Представить и пояснить назначение эталонной и функциональной моделей отношений доступа между пользователями и ресурсами вычислительной системы

40. Вы – заместитель руководителя отдела исследований и разработок в ПАО «Банк «Возрождение». Задание: Раскрыть проблему скрытного внедрения в программно-техническую и телекоммуникационную среду и её возможные деструктивные последствия

41. Вы – заместитель руководителя отдела исследований и разработок в ООО «Банк Корпоративного Финансирования». Задание: Выполнить анализ технологий и средств защиты информации от утечки по техническим каналам

42. Вы – руководитель отдела защиты информации в АО «БайкалИнвестБанк. Задание: Сформулировать понятие Единого информационного пространства, обосновать типовой состав компонентов и основные задачи по обеспечению информационной безопасности

43. Вы – заместитель руководителя отдела исследований и разработок в АО «Альфа-Банк». Задание: Представить информационную сферу социотехнического объекта информатизации (организации, предприятия) как интегрированный объект защиты

44. Вы – руководитель отдела защиты информации в АО «АКБ «Алеф-Банк». Задание: Предложить методы и способы создания доверенной организационно-технологической среды обработки информации и условий защищённости на объектах информатизации.

## 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 вы 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, задачи, лабораторные и курсовые работы.

В процессе подготовки ответа на вопросы необходимо учитывать изменения, которые произошли в законодательстве, увязывать теоретические проблемы с практикой сегодняшнего дня.

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

## 4 Критерии оценки результатов сдачи государственных экзаменов

Максимальное количество баллов (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 (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 ФГОС ВО 3+ в части формируемых компетенций, а также дополнительным компетенциям, установленным вузом.

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

Максимальное количество баллов (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 (3 балла) ставится, если комплексное профессионально-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 комплексное профессионально-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» (Финансовый университет)**

**Департамент информационной безопасности**

**Факультет информационных технологий и анализа больших данных**

# Методические рекомендации по подготовке и защите выпускной квалификационной работы по программе магистратуры направления подготовки 10.04.01 «Информационная безопасность» Направленность программы: «Информационная безопасность финансово-кредитных организаций»

Москва 2021

Федеральное государственное образовательное бюджетное
учреждение высшего образования

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

**Департамент информационной безопасности**

**Факультет информационных технологий и анализа больших данных**

Баранов А.П., Коннова И.Г.

# Методические рекомендации по подготовке и защите выпускной квалификационной работы по программе магистратуры направления подготовки 10.04.01 «Информационная безопасность» Направленность программы магистратуры: «Информационная безопасность финансово-кредитных организаций»

*Одобрено заседанием Совета Департамента информационной безопасности протокол №5 от 14 декабря 2021 г.*

Москва 2021

**УДК 004.056**
**ББК 74.58В-**

Методические рекомендации по подготовке и защите выпускной квалификационной работы по программе магистратуры направления подготовки 10.04.01 «Информационная безопасность», «Информационная безопасность финансово-кредитных организаций».
Составители: – Баранов А.П., Коннова И.Г. - М.: Финансовый университет, 2021 – 43с.

*Учебное пособие*
Баранов А.П.
Коннова И.Г.

Методические рекомендации по подготовке и защите выпускной квалификационной работы по программе магистратуры направления подготовки 10.04.01 «Информационная безопасность», «Информационная безопасность финансово-кредитных организаций».
Размещение на портале одобрено на заседании Совета Департамента информационной безопасности, протокол от 14 декабря 2021 г. №5

Компьютерный набор, верстка: Коннова И.Г.
*Формат60х90/16. Гарнитура Times New Roman*
*Усл. п.л.2,6*
Заказ № _____

Отпечатано в Финансовом университете

© Баранов А.П., 2021
© Коннова И.Г., 2021
© Финуниверситет, 2021

## СОДЕРЖАНИЕ

1 Общие положения…… 5

2 Определение темы выпускной квалификационной работы …..…….. 7

3 Руководство и контроль подготовки выпускной квалификационной работы …… 8

4 Структура и содержание выпускной квалификационной работы …….. 11

5 Порядок подготовки к защите и защита выпускной квалификационной работы... 17

6 Требования к оформлению выпускной квалификационной работы …….. 22

7 Критерии оценки выпускной квалификационной работы …….. 34

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ…….. 36

ПРИЛОЖЕНИЕ А. Форма заявления на выпускную квалификационную работу……. 39

ПРИЛОЖЕНИЕ Б. Форма плана-задания на выпускную квалификационную работу…..……. 40

ПРИЛОЖЕНИЕ В. Форма отзыва руководителя выпускной квалификационной работы…… 41

ПРИЛОЖЕНИЕ Г. Оформление титульного листа ……..... 43

## 1 Общие положения

1.1 Образовательная программа высшего образования – программа магистратуры, реализуемая Финансовым университетом по направлению подготовки 10.04.01 Информационная безопасность (далее – программа магистратуры), разрабатывается и реализуется в соответствии с основными положениями Федерального закона «Об образовании в Российской Федерации» (от 29.12.2012 № 273-ФЗ) [1] и на основе федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО, утвержден приказом Минобрнауки России от 1 декабря 2016 г. N 1513) [2] с учетом требований рынка труда.

1.2 В соответствии с ФГОС ВО выпускник, освоивший данную программу магистратуры, должен обладать следующими компетенциями:

– способность к абстрактному мышлению, анализу, синтезу (ОК-1);

– способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2);

– способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1);

– способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2);

– способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1);

– способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2);

– способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3);

– способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4);

– способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5);

– способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6);

– способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7);

– способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8);

– способность проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9);

– способность проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10);

– способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности (ПК-11);

– способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12);

– способностью организовать управление информационной безопасностью (ПК-13);

– способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14);

– способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15);

– способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации па системы и средства обеспечения информационной безопасности (ПК-16);

– способность разрабатывать модели угроз и оценивать возможности внешних и внутренних нарушителей безопасности автоматизированной системы финансово-кредитной организации (ДКН-1);

– способность классифицировать и оценивать угрозы информационной безопасности для объекта информатизации предприятий финансово-кредитной сферы (ДКН-2)

– способность осуществлять меры противодействия нарушениям сетей безопасности предприятий финансово-кредитной сферы с использованием различных программных и аппаратных средств защиты и принимать меры защиты информации при выявлении новых угроз безопасности информации (ДКН-3);

– способность формирования политик информационной безопасности организации предприятий финансово-кредитной сферы, с учетом порядка аттестации компьютерных систем на предмет их соответствия требованиям по информационной безопасности и выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний (ДКН-4);

## 2 Определение темы выпускной квалификационной работы

2.1 Примерный перечень тем ВКР ежегодно формируется департаментом совместно с представителями организаций – работодателей с учетом научных интересов департамента информационной безопасности, утверждается на заседании Совета департамента с последующим размещением на WEB - странице Департамента информационной безопасности сайта Финуниверситета в разделе «магистратура → информация по ВКР».

2.2 Обучающийся первого курса магистратуры должен или выбрать тему ВКР из размещенного на портале перечня тем ВКР, или сформулировать её самостоятельно, с последующим согласованием с предполагаемым руководителем ВКР, в срок не позднее 15 ноября первого года обучения, путем подачи письменного заявления о закреплении темы ВКР на имя руководителя образовательной программы магистратуры по соответствующей форме приложения А [4].

Закрепление тем и руководителей ВКР осуществляется приказом Финансового университета в установленном порядке не позднее 15 декабря первого года обучения.

2.3 Изменение темы ВКР в исключительных случаях возможно не позднее, чем за 1 месяц, а уточнение темы – не позднее, чем за 10 календарных дней до начала ГИА, определенной календарным учебным графиком, на основании согласованного с руководителем ВКР заявления обучающегося, составленного на имя руководителя департамента, с обоснованием причины корректировки. Изменение или уточнение темы оформляется приказом Финансового университета.

## 3 Руководство и контроль подготовки выпускной квалификационной работы

Руководство и контроль за ходом подготовки выпускной квалификационной работы обучаемым осуществляются руководителем ВКР, руководством Департамента информационной безопасности, консультантом с другой кафедры при необходимости.

3.1 В обязанности руководителя ВКР входит [4]:

— Оказание помощи обучающемуся при составлении плана ВКР, формирование и утверждение плана-задания на ВКР по утвержденной форме (приложение Б) [6];

— консультирование обучающегося по подбору литературы, информационного и фактического материала;

— содействие в выборе методики исследования;

— проведение систематических консультаций с обучающимся по проблематике работы, предоставление квалифицированных рекомендаций по содержанию ВКР;

— осуществление постоянного контроля за ходом подготовки ВКР в соответствии с графиком и планом ВКР;

— осуществление контроля за качеством подготовки ВКР и принятие решения о размещении обучающимся завершенной ВКР в электронном виде (далее - ЭВКР) на платформе org.fa.ru, входящей в электронную информационно-образовательную среду Финансового университета (далее - платформа);

— своевременное информирование служебной запиской руководителя департамента, а также руководство факультета в случае нарушения обучающимся графика подготовки ВКР или сроков размещения ВКР на платформе для применения мер дисциплинарного взыскания, предусмотренных Правилами внутреннего трудового и внутреннего распорядка обучающихся [9];

— проверка размещенной работы, в том числе анализ отчета системы «Антиплагиат.ВУЗ» на наличие заимствований, принятие решения о ее готовности, а также подготовка и своевременное размещение на платформе письменного отзыва о работе обучающегося в период подготовки ВКР по формам, установленным Департаментом;

— консультирование обучающегося при подготовке презентации и доклада для защиты ВКР;

— присутствие на защите ВКР, при условии его незанятости в аудиторной работе с обучающимися Финансового университета.

— осуществляет разработку совместно с обучающимся индивидуального плана научно-исследовательской работы и контролирует его выполнение, оказывает помощь и дает рекомендаций по участию в научных конференциях, семинарах и других научных мероприятиях, а также при подготовке научных публикаций.

Формы задания на ВКР, плана и графика разработки и оформления ВКР размещены на странице Департамента разделе «Магистратура» [8].

При необходимости, по ходатайству руководителя ВКР, руководитель Департамента может привлекать для консультирования обучающихся консультантов из числа научно-педагогических работников другого департамента/кафедры

Финансового университета по согласованию с руководителем соответствующего департамента/заведующим соответствующей кафедры.

Консультант обязан:

— оказывать консультационную помощь обучающемуся в выборе методики исследования, в подборе источников и информационных баз данных, теоретического и практического материала в части консультируемого вопроса;

— давать квалифицированные рекомендации в части содержания консультируемого вопроса [4];

3.3 В процессе выполнения ВКР обучающийся обязан [4]:

— вести НИР в соответствии с ИПР, заданиями руководителя ВКР и руководителя научно-исследовательского семинара (НИС);

— своевременно заполнять и вести ИПР в личном кабинете на org.fa.ru;

— систематически работать над ВКР в соответствии с установленными сроками и требованиями, использовать методические рекомендации Департамента информационной безопасности;

— регулярно общаться с руководителем ВКР (и консультантом при наличии) и информировать его о проделанной работе;

— оформить ВКР в соответствии с установленными требованиями;

— загрузить (разместить) ВКР на платформу для проверки работы руководителем; информировать руководителя о размещении ВКР на платформе;

— пройти процедуру предзащиты ВКР (при установлении процедуры предзащиты руководителем департамента;

— разместить окончательную версию ВКР на платформе;

— подготовить доклад и (или) презентацию для защиты ВКР, согласовать их с научным руководителем.

Департамент в рамках своих полномочий:

— доводит до сведения обучающихся методические рекомендации, которые определяют правила подготовки к защите ВКР и критерии оценки ВКР;

— осуществляет контроль регулярности и качества взаимодействия обучающихся и руководителей ВКР, а также хода подготовки ВКР; в случае выявления нарушений установленных требований и норм принимает меры к их устранению и информирует о нарушениях декана факультета;

— утверждает форму отзыва руководителя (приложение В);

— вправе организовать и провести предварительную защиту ВКР.

## 4 Структура и содержание выпускной квалификационной работы

4.1 ВКР должна отвечать следующим требованиям:

— наличие в работе основных структурных элементов исследования: аналитической, теоретической и практической составляющих;

— использование обоснованного комплекса методов и средств, способствующих раскрытию сути и решению актуальной проблемы/задачи обеспечения информационной безопасности (ИБ) в предметной деятельности;

— наличие в работе материала, который может стать источником дальнейших исследований;

— достаточность и современность использованного библиографического материала.

4.2 Рекомендуемый объем составляет не менее 80 и не более 100 страниц без учета приложений (для коллективной ВКР 100 - 150 страниц без учета приложений).

4.3 ВКР должна включать следующие разделы:

— титульный лист (по форме согласно приложению Г);

— содержание;

— введение;

— основная часть, структурированная на главы и параграфы;

— заключение;

— список использованных источников;

— приложения (при наличии). [4]

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

4.3.2 Во введении обосновывается актуальность темы ВКР, степень её 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 ее центральной проблемой, при этом целью исследования в ВКР должно быть получение определенных результатов, а не сам процесс исследования.

Задачи вытекают из общей цели, их 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 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 ее 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.). [4].

Рекомендуется писать введение по завершении основных глав работы, перед заключением. В этом случае исключена возможность несоответствия «желаемого» и «действительного».

Таким образом, введение кратко раскрывает план выполнения выпускной работы, то, что обучающемуся необходимо сделать для решения выбранной задачи.

4.3.3 Основная часть ВКР включает разделы (главы) и подразделы в соответствии с логической структурой изложения. Название раздела (главы) не должно дублировать название темы, а название подразделов – названия разделов (глав). Формулировки должны быть лаконичными и отражать суть раздела (главы) и подраздела. Основная часть ВКР должна содержать, как правило, три раздела (главы).

4.3.4 Сведения, содержащиеся в первом разделе (главе), должны давать полное представление о состоянии и степени изученности поставленной проблемы/задачи на данный момент времени.

Написание первого раздела (главы) проводится на базе предварительно подобранных литературных источников, в которых освещаются вопросы, в той или иной степени раскрывающие тему ВКР.

Раздел (глава) должен иметь название, отражающее суть изложенного в нем материала. Не допускается выносить в качестве названия этого раздела заголовки «Теоретическая часть», «Обзор литературных источников» и т.д. [4].

Особое внимание следует обратить на законодательную, нормативную и специальную документацию, посвященную вопросам, связанным с предметом и объектом исследования.

В первом разделе (главе) приводится:

— анализ конкретного материала по избранной теме (на примере конкретной системы/подсистемы информационной безопасности организации, отрасли, региона, страны);

— анализ информационных ресурсов и актуальных для объекта уязвимостей, каналов утечки информации, включая сравнительный анализ с действующей практикой;

— разработка модели актуальных угроз и оценка рисков;

— анализ эффективности существующих на объекте системы защиты информации.

В этой главе ВКР выявляются особенности объекта защиты, а также освещаются практические аспекты и условия функционирования объекта информатизации, влияющие на уровень его защищенности от угроз. Объем этой главы должен составлять 30 – 35 % от всего объема ВКР.

Завершается первая глава как правило постановкой научной задачи и обоснованием необходимости проведения исследовательской части работы.

4.3.5 Вторая глава посвящена разработке и исследованию предлагаемых автором моделей, методов и алгоритмов защиты информации, необходимых для решения поставленной научной задачи. Вторая глава может опираться на результаты анализа и обработки практического материала, собранного во время подготовки и написания первой главы и-или производственной практики.

В этой главе приводятся результаты разработки научно-методического аппарата методологии и моделирования безопасного развития систем и процессов, совершенствования и уточнения концептуальных и частных моделей защиты объекта информатизации от выявленных ранее информационных угроз и сценариев действий нарушителя, предлагаются варианты конкретных способов, технологий, решений по защите значимых информационных ресурсов.

В ходе подготовки главы могут использоваться аналитические таблицы, расчеты, формулы, схемы, диаграммы и графики.

Объем второй главы должен составлять, как правило, 20 - 40 % от всего объема ВКР [4].

4.3.6 В третьей главе рассматриваются и обосновываются пути решения исследуемой проблемы/задачи, оценивается возможность их практической реализации, предлагаются конкретные практические рекомендации и предложения по использованию и дальнейшему совершенствованию разработанных методов, моделей и алгоритмов защиты. В данной главе должны быть сделаны самостоятельные выводы, разработаны рекомендации, при необходимости представлены экономические расчеты.

Объем третьей главы должен составлять, как правило, 15-25 % от всего объема ВКР [4].

4.3.7 В заключении, являющимся завершающей частью ВКР, рекомендуется отметить, какие задачи были решены в ходе выполнения выпускной работы, определить пути внедрения и направления дальнейшего совершенствования разработанных решений по обеспечению информационной безопасности объекта информатизации; отразить основные проектные решения, разработанные методики и модели, используемые классификаторы, входные и выходные документы, показатели экономической эффективности и другие существенные показатели. Заключение содержит выводы и предложения из всех трех 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 5-ти страниц. Заключение является основой доклада студента на защите ВКР. [4]

4.3.8 Список использованных источников должен содержать сведения об источниках, которые использовались при подготовке ВКР (не менее 60) и располагаться в следующем порядке:

— законы Российской Федерации (в прямой хронологической последовательности);

— указы Президента Российской Федерации (в прямой хронологической последовательности);

— постановления Правительства Российской Федерации (в прямой хронологической последовательности);

— нормативные акты, инструкции (в прямой хронологической последовательности);

— 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 [4].

4.3.9 Приложения включают дополнительные справочные материалы, необходимые для полноты исследования, но имеющие вспомогательное значение, например, копии документов, выдержки из отчетных материалов, статистические данные, схемы, таблицы, диаграммы, программы, положения и т.п. [4]. Приложения должны располагаться в логической последовательности появления ссылок на них из основной части выпускной квалификационной работы. Каждое приложение должно обязательно иметь обозначение и наименование, характеризующее его содержание. В одном приложении нельзя размещать различные по смыслу таблицы или рисунки. Не допускается дублирование в приложении материала, размещенного в основной части выпускной работы.

4.4 Руководитель ВКР в обязательном порядке проводит анализ отчета ВКР сформированный системой «Антиплагиат.ВУЗ». В случае выявления заимствований (без учета цитирования) в объеме **более 15% руководитель ВКР проводит анализ текста на соблюдение норм правомерного заимствования** и принимает решение о правомерности использования заимствованного текста в ВКР. При необходимости руководитель вправе дополнительно проверить работу на наличие заимствований. В случае выявления факта неправомерного заимствования при подготовке ВКР работа возвращается руководителем ВКР обучающемуся на доработку.

4.5 При невыполнении требований руководителя по доработке ВКР и размещении работы, отчет по которой **повторно** показывает **более 15% заимствований (без учета цитирования)**, руководитель, как правило, готовит и размещает **отрицательный отзыв на работу**. Экспертная оценка уровня заимствований в ВКР отражается в отзыве руководителя ВКР.

4.6 Обучающийся **обязан разместить** полностью законченную, оформленную в соответствии с требованиями, а также согласованную с руководителем ВКР в электронном виде на платформе, **не позднее 10-ти календарных дней до начала ГИА согласно календарному графику**, ежегодно утверждаемому приказом об организации учебного процесса.

4.7 Размещение ЭВКР и дальнейшее ее рецензирование и допуск осуществляется в соответствии с Регламентом размещения, хранения и списания курсовых проектов (работ) и выпускных квалификационных работ [3].

4.8 Загрузка обучающимся ЭВКР на платформе из личного кабинета означает подтверждение самостоятельности выполненной работы, аналогично собственноручной подписи на титуле, а также подтверждает согласие на обработку персональных данных, размещение и хранение ВКР.

4.9 Если обучающийся **не разместил на платформе ЭВКР в сроки**, указанные в пункте 4.6., руководитель департамента служебной запиской информирует декана факультета о нарушении сроков представления ВКР и необходимости подготовки **приказа об отчислении** обучающегося из Финансового университета как не выполнившего обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана, включая подготовку ВКР.

## 5 Порядок подготовки к защите и защита выпускной квалификационной работы

5.1. После размещения на платформе полностью законченной, оформленной в соответствии с требованиями ЭВКР, руководитель составляет письменный отзыв о работе обучающегося в период подготовки ВКР и размещает его на платформе.

5.2. В случае удовлетворения ЭВКР всем требованиям, при отсутствии замечаний, которые не позволяют допустить работу к защите, руководитель

осуществляет допуск ВКР к защите, устанавливая статус «Допущен (-а) к защите». Статус «Допущен (-а) к защите» устанавливается руководителем ВКР и в случае написанного им отрицательного отзыва руководителя, а также при невыполнении отдельных требований к оформлению или содержанию работы и невозможности ее исправить (например, из-за окончания срока размещения работы). Указанные несоответствия отражаются в отзыве руководителя до установления статуса. Установление статуса исключает внесение обучающимся или руководителем изменений в ВКР, а также загрузку новых версий файлов.

Размещение отзыва руководителя и установление им статуса «Допущен (-а) к защите» аналогично собственноручной подписи руководителя на работе и осуществляется не позднее чем за пять календарных дней до даты защиты ВКР.

5.3. ВКР обучающихся подлежит обязательному рецензированию. Для проведения рецензирования ВКР направляется департаментом одному или нескольким рецензентам.

Рецензия должна быть загружена на платформу до установления руководителем статуса «Допущена к защите» не позднее чем за 5 календарных дней до даты защиты, для ознакомления обучающегося с рецензией.

5.4. Получение отрицательного отзыва руководителя, отрицательной рецензии или статуса «Не соответствует требованиям» не является препятствием к представлению ВКР на защиту, однако в обязательном порядке озвучивается в ходе защиты работы.

5.5. С целью контроля готовности обучающегося к защите ВКР, департамент вправе организовать и провести предварительную защиту ВКР. Порядок и сроки проведения предзащиты ВКР определяются департаментом.

5.6. Завершающим этапом подготовки ВКР является ее защита.

К защите ВКР допускаются обучающиеся, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по соответствующей образовательной программе высшего образования, своевременно разместившие ВКР на платформе, успешно сдавшие государственный экзамен или отсутствовавшие на государственном экзамене по уважительной причине.

5.7. Ответственный сотрудник департамента направляет ЭВКР вместе с письменным отзывом руководителя ВКР, а также иными документами (дополнительными приложениями, отчетом системы плагиат и др., при наличии) секретарю государственной экзаменационной комиссии (далее – ГЭК) не позднее, чем за два календарных дня до дня защиты ВКР.

5.8. Защита ВКР проводится в установленное расписанием проведения государственных аттестационных испытаний время на заседании ГЭК по соответствующему направлению подготовки.

5.9. Защита ВКР производится в очном формате. Процедура защиты в этом случае определяется Регламентом проведения в Финансовом университете государственной итоговой аттестации [5].

5.10. Процедура защиты ВКР включает в себя:

— открытие заседания ГЭК (председатель);

— доклады обучающихся, максимальная продолжительность которых **не более 15 минут**. Конкретное максимальное время для доклада по ВКР озвучивается председателем ГЭК перед началом работы ГЭК;

— вопросы членов комиссии по ВКР и докладу обучающегося, а также смежной тематике. При ответах на вопросы обучающийся имеет право пользоваться своей работой;

— выступление руководителя ВКР либо, в случае его отсутствия, заслушивание текста отзыва с обязательным отражением замечаний и мнения руководителя о возможности рекомендации ВКР к защите;

— выступление рецензента(-ов) ВКР либо, в случае его (их) отсутствия, заслушивание текста рецензии(-й);

— заключительное слово обучающегося, включающее в себя ответы на замечания руководителя ВКР и рецензента.

5.10.1. Доклад обучающегося по теме ВКР должен включать в себя:

— обоснование избранной темы;

— описание цели и задач работы;

— круг рассматриваемых проблем и методы их решения;

— результаты анализа практического материала и их интерпретация;

— конкретные рекомендации по совершенствованию разрабатываемой темы.

В заключительной части доклада характеризуется значимость полученных результатов и даются общие выводы.

5.10.2. Доклад должен сопровождаться презентацией, иллюстрирующей основные положения работы с использованием мультимедийных средств. Количество слайдов — 10-15.

5.10.3. Требования к содержанию презентации.

На первом слайде должны быть: логотип и полное название Финансового университета, название факультета, департамента, название работы, данные автора и научного руководителя.

На следующем слайде указывают актуальность темы исследования, обозначают цель работы, объект и предмет исследования.

Далее необходимо обозначить задачи (3-4), которые поставлены и решены в работе (задачи должны соответствовать содержанию работы, с указанием результата решения).

В докладе и в презентации необходимо продемонстрировать свободное владение освоенными в рамках программы компетенциями. Для этого на слайдах могут быть представлены математические выкладки, графики, алгоритмы, схемы, модели, фрагменты программного кода, пользовательского интерфейса.

На последнем слайде должны быть представлены выводы по работе.

5.10.4. Требования к оформлению презентации. Рекомендуется использовать шаблон презентации, размещенный на главной странице сайта Финуниверситета, вкладка «размещение презентаций».

Фон слайда должен быть однотонный. Все надписи и рисунки выполняются темным цветом на светлом фоне, должны быть крупными и разборчивыми (размер шрифта - не менее 28, шрифт заголовков - не менее 36), занимать все пространство слайда. Слайд презентации должен состоять из двух частей – заголовка и содержательной части. Заголовок слайда располагается в верхней части и должен как можно более подробно обозначать, что изображено на слайде.

Слайды необходимо оформлять в строгом стиле.

В левом верхнем углу должен быть номер слайда.

Содержание слайда должно быть максимально информативно и понятно.

Пояснения на слайде должны быть краткими, но емкими.

Изображение скриншотов программных закладок должно быть выполнено в хорошем качестве. В презентацию должны быть включены только те скриншоты, которые отражают суть работы.

5.11. Особенности проведения защиты ВКР обучающихся с ограниченными возможностями здоровья определены разделом 6 Порядка проведения государственной итоговой аттестации по программам бакалавриата и магистратуры в Финансовом университете [5].

5.12. ГЭК при определении результата защиты ВКР принимает во внимание:

— индивидуальную оценку членами ГЭК содержания работы, её защиты, включая доклад, ответы на вопросы членов ГЭК;

— наличие практической значимости и обоснованности выводов и рекомендаций, сделанных обучающимся в результате проведенного исследования;

— оценку руководителем ВКР работы обучающегося в период подготовки ВКР, степени ее соответствия требованиям, предъявляемым к ВКР, количество и серьезность замечаний;

— оценку рецензента за работу в целом, учитывая наличие научных результатов;

— наличие по теме ВКР опубликованных работ в научных изданиях; наличие подтверждения апробации результатов исследования в виде справки о внедрении, участия с докладами на научных мероприятиях.

В случае возникновения спорной ситуации при равном числе голосов председатель обладает правом решающего голоса.

5.13. Результат защиты ВКР обучающимся определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и заносится в протокол заседания ГЭК.

5.14. По результатам защиты ВКР обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению,

установленной процедуры проведения защиты ВКР. Апелляция подается лично обучающимся в апелляционную комиссию **не позднее следующего рабочего дня** после объявления результата защиты ВКР. Форма заявления в апелляционную комиссию, а также порядок проведения апелляции определен в Порядком проведения ГИА [5].

5.15. Обучающиеся, не прошедшие государственное аттестационное испытание в форме защиты ВКР в связи с неявкой по неуважительной причине или в связи с получением оценки «неудовлетворительно», отчисляются из Финансового университета с выдачей справки об обучении как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана.

5.16. Обучающиеся, не прошедшие государственное аттестационное испытание в форме защиты ВКР в связи с неявкой по уважительной причине (временная нетрудоспособность, исполнение государственных, общественных или служебных обязанностей, вызов в суд, транспортные проблемы (отмена или существенная задержка рейса)), вправе пройти ее в течение 6-ти месяцев после завершения ГИА. Обучающийся должен не позднее 2-х дней после того как отпали причины неявки представить документ, подтверждающий причину его отсутствия.

5.17. Подготовка, выполнение и защита Коллективной ВКР осуществляется в соответствии с пунктом 6 Положения о ВКР [4].

## 6 Требования к оформлению выпускной квалификационной работы

6.1 На титульном листе выпускной квалификационной работы указывается наименование факультета, департамента, группы, название темы выпускной квалификационной работы, фамилия и инициалы автора работы и руководителя, год написания работы. Образец титульного листа приведен в ПРИЛОЖЕНИИ А.

6.2 Оформление ВКР должно производиться по общим правилам, изложенным в ГОСТ 7.32-2017 «Отчет о научно-исследовательской работе. Структура и правила оформления». [9]

6.3 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» [10];

ГОСТ 7.80-2000 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Заголовок. Общие требования и правила составления» [11];

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» [12];

ГОСТ 7.11-2004 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на иностранных европейских языках» [13].

6.4 ВКР оформляется в текстовом редакторе на листах бумаги формата А4 и содержит примерно 1800 знаков на странице (включая пробелы и знаки препинания). Текст следует набирать через 1,5 интервала, шрифт соответствующий требованиям ГОСТ Р 7.0.97-2016[1] [14], размер шрифта 14 pt, в таблицах – размер шрифта 12 pt, в подстрочных сносках – размер шрифта 10 pt. Подчеркивание слов и выделение их курсивом не допускается.

6.5Страницы, 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.

6.6 Названия структурных элементов «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ИНТЕРНЕТ- РЕСУРСОВ», «ПРИЛОЖЕНИЕ» являющиеся заголовками, печатаются прописными буквами, а названия параграфов (подзаголовки) - строчными буквами (кроме первой прописной).

[1] Внимание! Шрифт Times New Roman не соответствует ГОСТ Р 7.0.97-2016, рекомендуется использовать его полный лицензионно-чистый импортозаместительный аналог PT Astra Serif.

Заголовки и подзаголовки при печатании текста письменной работы на принтере выделяются полужирным шрифтом.

6.7Заголовки, подзаголовки и подстрочные сноски (состоящие из нескольких строк) печатаются через одинарный интервал.

6.8Абзацный отступ должен соответствовать 1,25 см и быть одинаковым по всей работе.

6.9Нумерация разделов и подразделов 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 его не нужно.

6.10 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 на нем не ставится.

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

Каждую главу работы следует начинать с нового листа.

Параграф начинать с нового листа не следует.

6.11 Иллюстрации и таблицы

Если в работе имеются схемы, таблицы, графики, диаграммы, рисунки, то их следует располагать непосредственно после текста, в котором они упоминаются впервые, или на следующей странице.

На все иллюстрации должны быть ссылки. При ссылке необходимо писать слово «рисунок» и его номер, например: «в соответствии с рисунком 2». Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией. Слово «Рисунок», его номер, и через тире наименование, располагают в центре под рисунком без точки в конце. Если рисунок один, то он обозначается: Рисунок 1.

***Пример - Рисунок 1 – Схема прибора***

Если наименование рисунка состоит из нескольких строк, то его следует записывать через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки на конце. Перенос слов в наименовании графического материала не допускается.

При наличии в работе таблицы ее 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, за исключением таблиц приложений, следует нумеровать сквозной нумерацией арабскими цифрами по всему тексту или в рамках главы (2.1 и т.д.).

Если таблица имеет заголовок, то он 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».

6.12 Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы должно быть оставлено не менее одной свободной строки.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они

представлены в формуле. Значение каждого символа и числового коэффициента необходимо приводить с новой строки. Первую строку пояснения начинают со слова «где» без двоеточия с абзаца.

Формулы следует располагать посередине строки и обозначать порядковой нумерацией в пределах всего документа арабскими цифрами в круглых скобках в крайнем правом положении на строке.

***Пример***

$$A = \pi r^2, \qquad (1)$$

где А- площадь круга, мм$^2$;

$\pi$ – число Пи (3,14);

r – радиус круга, мм.

Ссылки на порядковые номера формул приводятся в скобках: в формуле (1).

Формулы, помещаемые в приложениях, нумеруются арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения (например: А.1)

6.13 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 он 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 ее 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» [19].

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 ее общий индекс».[1]

[1.] Бушуев В.В. Финансовые кризисы и волантильность 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 мая 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. рисунок 2.5., результаты приведены в таблице 3.1 и т.д.

6.14 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.

6.15 Образцы библиографических описаний документов в списках литературы

**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).

**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.

**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).

**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.

**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.]).

**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. (17-18 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.

**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 №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. № 273-ФЗ: [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.

**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 № 1-В2017.

**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.

**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: 19.01.2021). — 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: 18.01.2021).

— 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: 10.12.2020). — 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: 10.12.2020).

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/l_1/pdf_190537.pdf — Дата публикации: 31.10.2019.

6.16 Общие требования к приложениям

Приложения - дополнительные к основному тексту материалы. Приложения могут включать: графический материал, таблицы, расчеты, описания алгоритмов и программ. Приложение оформляют как продолжение ВКР на последующих листах. В тексте отчета на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте ВКР. Каждое приложение следует размещать с новой страницы с указанием в центре верхней части страницы слова

«ПРИЛОЖЕНИЕ». Приложение должно иметь заголовок, который записывают с прописной буквы, полужирным шрифтом, отдельной строкой по центру без точки в конце.

Приложения обозначают прописными буквами кириллического алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ъ, Ы, Ь.

Приложения должны иметь общую с остальной частью отчета сквозную нумерацию страниц.

Приложения размещаются в конце работы, после списка использованных источников в порядке их упоминания в тексте. Если приложение представляет собой отдельный рисунок или таблицу, то оно оформляется в соответствии с требованиями, предъявляемыми к иллюстрациям, таблицам.

Иллюстрации и таблицы нумеруются в пределах каждого приложения в отдельности.

Например: рисунок А.3 (третий рисунок первого приложения), таблица А.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.

## 7 Критерии оценки выпускной квалификационной работы

Государственная экзаменационная комиссия (ГЭК) при определении результата защиты ВКР принимает во внимание: оценку руководителем ВКР работы обучающегося в период подготовки ВКР, степени ее соответствия требованиям, предъявляемым к ВКР; наличие практической значимости и обоснованности выводов и рекомендаций, сделанных обучающимся в результате проведенного исследования; общую оценку членами ГЭК содержания работы, её защиты, включая доклад: качество, содержание вступительного слова, отражающего основные итоги проделанной работы; ответы на вопросы членов ГЭК; свободу обращения с основными теоретическими понятиями, терминами, особенно имеющими отношение к теме исследования; знание основных научных источников, истории вопроса, умение в ответах определить позиции ученых и обосновать свою; доказательность выводов, практических результатов исследования; соответствие оформления работы предъявляемым требованиям.

Общую оценку за выпускную квалификационную работу члены государственной экзаменационной комиссии выводят на коллегиальной основе с учетом соответствия содержания заявленной теме, глубины ее раскрытия, соответствия оформления принятым стандартам, проявленной во время защиты способности обучающегося демонстрировать собственное видение проблемы и умение мотивированно его отстаивать, владения теоретическим материалом, способности грамотно его излагать и аргументированно отвечать на поставленные вопросы. Оценки выпускным квалификационным работам даются членами экзаменационной комиссии на закрытом заседании и объявляются студентам-выпускникам в тот же день после подписания соответствующего протокола заседания комиссии.

В случае возникновения спорной ситуации при равном числе голосов председательствующий обладает правом решающего голоса. [4,5]

Критерии оценок:

«Отлично» – работа имеет исследовательский характер, грамотно изложенную теоретическую часть, логичное, последовательное изложение материала с

соответствующими выводами и обоснованными предложениями. При ее защите студент свободно оперирует данными исследования, вносит обоснованные предложения, свободно ориентируется в вопросах тематики исследования, правильно применяет эти знания при изложении материала, легко отвечает на поставленные вопросы. На работу имеется положительный отзыв руководителя.

«Хорошо» – работа имеет исследовательский характер, грамотно изложенную теоретическую часть, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными предложениями. При ее защите студент показывает знание вопросов темы, оперирует данными исследования, вносит предложения, ориентируется в вопросах тематики исследования, применяет эти знания при изложении материала, но имеются замечания при ответах на поставленные вопросы. На работу имеется положительный отзыв руководителя.

«Удовлетворительно» – работа имеет исследовательский характер, содержит теоретическую часть, базируется на практическом материале, но анализ выполнен поверхностно, просматривается непоследовательность изложения материала, представлены необоснованные предложения. При защите работы студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полного аргументированного ответа на заданные вопросы. В отзыве руководителя имеются замечания по содержанию работы и/или методике анализа.

«Неудовлетворительно» – работа не носит исследовательского характера, в ней отсутствуют выводы, или они носят декларативный характер. При защите работы студент затрудняется отвечать на поставленные вопросы, при этом допускает существенные ошибки. В отзыве руководителя имеются критические замечания. При формировании критериев оценки следует использовать перечень знаний, умений, владений, которые выпускник должен продемонстрировать для подтверждения освоенных компетенций.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Об образовании в Российской Федерации: федеральный закон от 29.12.2012 № 273-ФЗ (с изменениями на 30 декабря 2021 года) (в редакции, действующая с 1 марта 2022 года) [Электронный ресурс]. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102162745

2 Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.04.01 «Информационная безопасность» (уровень магистратуры) (утв. приказом Министерства образования и науки РФ от 1 декабря 2016 г. № 1513).

3 Об утверждении Регламента размещения, хранения и списания курсовых проектов (работ) и выпускных квалификационных работ обучающихся в электронном виде в информационно-образовательной среде Финуниверситета: Приказ Финуниверситета от 13.09.2021 № 1853/о. – URL: http://www.fa.ru/fil/vladik/about/base/SiteAssets/Pages/oup/%d0%9f%d1%80%d0%b8%d0%ba%d0%b0%d0%b7%20%e2%84%96%201853_%d0%be%20%d0%be%d1%82%2013.09.2021%20%d0%9e%d0%b1%20%d1%83%d1%82%d0%b2%d0%b5%d1%80%d0%b6%d0%b4%d0%b5%d0%bd%d0%b8%d0%b8%20%d0%a0%d0%b5%d0%b3%d0%bb%d0%b0%d0%bc%d0%b5%d0%bd%d1%82%d0%b0%20%d1%80%d0%b0%d0%b7%d0%bc%d0%b5%d1%89%d0%b5%d0%bd%d0%b8%d1%8f%2c%20%d1%85%d1%80%d0%b0%d0%bd%d0%b5%d0%bd%d0%b8%d1%8f%20%d0%b8%20%d1%81%d0%bf%d0%b8%d1%81%d0%b0%d0%bd%d0%b8%d1%8f%20%d0%ba%d1%83%d1%80%d1%81%d0%be%d0%b2%d1%8b%d1%85%20%d0%bf%d1%80%d0%be%d0%b5%d0%ba%d1%82%20%282901653%20v1%29.pdf

4 Об утверждении Положения о выпускной квалификационной работе по программам бакалавриата и магистратуры в Финансовом университете: Приказ 18 октября 2021 2203/о. [Электронный ресурс]. – URL: http://www.fa.ru/org/dep/eo/SiteAssets/Pages/bak/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BE%20%D0%92%D0%9A%D0%A0%20%D0%B1%D0%B0%D0%BA%20%D0%B8%20%D0%BC%D0%B0%D0%B3%20%D0%BE%D1%82%2018.10.2021.pdf

5 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры»: Приказ Министерства образования и науки РФ от 29 июня 2015 г. N 636 (с изменениями и дополнениями 9 февраля, 28 апреля 2016 г., 27 марта 2020 г.) [Электронный ресурс]. – URL: https://base.garant.ru/71145690/53f89421bbdaf741eb2d1ecc4ddb4c33/

6 «Об утверждении формы индивидуального плана работы студента, обучающегося по программе магистратуры» (утв. Приказом Финуниверситета от 15.09.2015 №1804/о)

7 Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»: приказ Министерства труда и социальной защиты российской федерации от 15 сентября 2016 года N 522н [Электронный ресурс]. – URL: https://docs.cntd.ru/document/420377328

8 Портал Финансового университета. Структура. Учебно-научные департаменты. Департамент информационной безопасности. Бакалавриат. – Режим доступа: http://www.fa.ru/org/dep/is/Pages/bak.aspx

9 ГОСТ 7.32-2017. Отчет о научно-исследовательской работе. Структура и правила оформления. Межгосударственный стандарт: Принят Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 25 сентября 2017 г. N 103-П. Введен 2018.07.01 – URL: https://docs.cntd.ru/document/1200157208

10 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 от 3 декабря 2018 года№ 1050-ст – URL: https://docs.cntd.ru/document/1200161674

11 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 от 06.10.2000 № 253-ст – URL: https://docs.cntd.ru/document/1200006960

12 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 от 13 декабря 2011 года № 813-ст – URL: https://docs.cntd.ru/document/1200093114

13 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 5 декабря 2003 года) – URL: https://docs.cntd.ru/document/1200039536 .

14 ГОСТ Р 7.0.97-2016. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов: Утвержден Приказом Росстандарта от 08.12.2016 N 2004-ст, в ред. От 14.05.2018 – URL: http://www.consultant.ru/document/cons_doc_LAW_216461/

15 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 апреля 2008 г. № 95-ст – URL: https://docs.cntd.ru/document/1200063713.

## ПРИЛОЖЕНИЕ А

### Форма заявления на выпускную квалификационную работу

ФИНУНИВЕРСИТЕТ

Департамент информационной безопасности
(наименование департамента)

**СОГЛАСОВАНО**

_____ _____
(подпись) (и.о. фамилия)
«_____» _____ 202_ г.

Руководителю департамента информационной безопасности

А.В. Осипов к.ф.-м.н
(и.о. фамилия, уч. степень, уч.звание)

_____
(фамилия и.о. обучающегося)
_____
(наименование факультета)
_____
(№ учебной группы)
Тел. _____
E-mail _____

**ЗАЯВЛЕНИЕ**[2]

Прошу закрепить за мной тему ВКР «_____».

С Положением о выпускной квалификационной работе по программам бакалавариата и магистратуры в Финансовом университете, графиком выполнения ВКР, а также Регламентом размещения, хранения и списания курсовых проектов (работ) и выпускных квалификационных работ обучающихся в электронном виде в информационно-образовательной среде Финуниверситета ознакомлен (а).

«____» _____ 202___г. _____ _____
подпись обучающегося И.О. Фамилия

Согласовано:
Руководитель ВКР

_____ _____
(подпись) (И.О. Фамилия)
«____» _____ 202__г.

Согласовано:
Руководитель образовательной программы

_____ _____
(подпись) (И.О. Фамилия)
«____» _____ 202__г.

[2] Заявление может быть оформлено и передано в департамент (кафедру) в электронном виде по электронной почте при условии отправки с корпоративной почты обучающегося (name@edu.fa.ru) и обязательным отражением факта и даты согласования заявления потенциальным руководителем ВКР

## ПРИЛОЖЕНИЕ Б

### Форма плана-задания на выпускную квалификационную работу

ФИНУНИВЕРСИТЕТ

Департамент информационной безопасности
(наименование департамента (кафедры))

УТВЕРЖДАЮ

Руководитель ВКР

_____
(должность, уч. степень, уч.звание)

_____ _____
(подпись) (И.О. Фамилия)

«____» _____202_ г.

**ПЛАН – ЗАДАНИЕ**
**на выпускную квалификационную работу[3]**

обучающегося_____
(фамилия, имя, отчество)

Тема выпускной квалификационной работы «_____»

закреплена приказом Финуниверситета от «___»_____202__г. №_____.

Целевая установка:[4]_____

План ВКР (основные вопросы, подлежащие исследованию и разработке):

1. _____
1.1._____
1.2. _____
2._____
2.1. _____
2.2. _____
3._____
3.1. _____
3.2. _____

Дополнительные рекомендации руководителя ВКР по проведению исследования:_____

_____ _____
подпись обучающегося И.О. Фамилия обучающегося

[3] План-задание согласовывается руководителем с обучающимся и размещается обучающимся в личном кабинете на платформе не позднее 15 календарных дней с даты издания приказа о закреплении темы ВКР.

[4] Руководитель ВКР совместно с обучающимся может конкретизировать целевую установку задачами.

## ПРИЛОЖЕНИЕ В

**Форма отзыва руководителя выпускной квалификационной работы**

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

ОТЗЫВ РУКОВОДИТЕЛЯ

о работе обучающегося в период подготовки выпускной квалификационной работы по программе магистратуры

Обучающийся _____

*(фамилия, имя, отчество)*

Факультет _____

Департамент _____

Направление подготовки _____

Направленность_____

Наименование темы_____

Руководитель_____

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

1. Актуальность темы, полнота обзора отечественной и зарубежной научной литературы по теме исследования: _____
_____
_____
_____

2. Оценка законченности и полноты проведенного исследования, достоверности полученных результатов, их соответствие поставленным целям и задачам: _____
_____
_____

3. Характеристика использования в работе современных методов научных исследований, математического и статистического инструментария, моделирования, расчетов, пакетов специальных прикладных программ, баз данных и т.п.: _____
_____
_____

4. Степень самостоятельности (доля (%) заимствований в ВКР и корректность оформления заимствованного текста): _____
_____
_____
_____

5. Оригинальность идей и практическая значимость полученных результатов (наличие научных выводов, теоретический и практический вклад автора в решение проблемной ситуации): _____
_____
_____
_____

6. Апробация основных положений и результатов работы, в т.ч. подготовка научных публикаций по теме исследования, участие с докладом в научной/научно-практической конференции, наличие справки о внедрении, участие студента в рантах, Госзадании и проч.:_____
_____
_____

7. Уровень (пороговый, продвинутый, высокий) сформированности компетенций, продемонстрированный в ходе работы над ВКР (перечень компетенций установлен методическими рекомендациями по выполнению ВКР в соответствии с ФГОС ВО или ОС ФУ): _____
_____
_____
_____

8.Недостатки в работе обучающегося в период подготовки ВКР:_____
_____
_____

9.ВКР соответствует (не соответствует) требованиям, предъявляемым к ВКР, и может (не может) быть рекомендована к защите на заседании ГЭК: _____

*(Ф.И.О. руководителя, полностью)*

(подпись руководителя)

«___» _____ 20_ г.

## ПРИЛОЖЕНИЕ Г

### Оформление титульного листа

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

Факультет информационных технологий и анализа больших данных
(наименование факультета)
Департамент информационной безопасности
(наименование департамента/кафедры)

Выпускная квалификационная работа

на тему «_____»
(наименование темы выпускной квалификационной работы)
Направление подготовки _____
(код и наименование направления подготовки)
_____
(наименование профиля /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 Департамента
к.ф.-м.н.
(ученая степень, ученое звание)
А.В. Осипов
(И.О. Фамилия)
«_____» _____ 202_ г.

Москва – 202_г.