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

Кафедра информационной безопасности
Факультета информационных технологий и анализа больших данных

Программа государственной итоговой аттестации

для студентов, обучающихся по направлению подготовки
10.03.01 Информационная безопасность
ОП «Безопасность автоматизированных систем
в финансово-банковской сфере»,
профиль: «Безопасность автоматизированных систем
в финансово-банковской сфере»

Одобрено на заседании Кафедры информационной безопасности
протокол от «25» апреля 2024 г. № 3

Москва 2024

Перечень компетенций, подлежащих оценке в ходе государственной итоговой аттестации для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», ОП «Безопасность автоматизированных систем в финансово-банковской сфере», профиль «Безопасность автоматизированных систем в финансово-банковской сфере»

Код и наименование компетенции	Форма государственной итоговой аттестации, в рамках которой проверяется сформированность компетенции
УК-1. Способность к восприятию межкультурного разнообразия общества, в социально-историческом, этическом и философских контекстах, анализу и мировоззренческой оценке происходящих процессов и закономерностей	Государственный экзамен, выпускная квалификационная работа
УК-10. Способность осуществлять поиск, критически анализировать, обобщать и систематизировать информацию, использовать системный подход для решения поставленных задач	Государственный экзамен, выпускная квалификационная работа
УК-11. Способность к постановке целей и задач исследований, выбору оптимальных путей и методов их достижения	Государственный экзамен, выпускная квалификационная работа
УК-12. Способность использовать базовые дефектологические знания в социальной и профессиональной сферах	Государственный экзамен, выпускная квалификационная работа
УК-13. Способность принимать обоснованные экономические решения в различных областях жизнедеятельности	Государственный экзамен, выпускная квалификационная работа
УК-14. Способность формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению, попыткам фальсификации истории и противодействовать им в профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
УК-15. Способность релевантно решаемым задачам использовать информационные ресурсы и информационно-коммуникационные технологии для достижения целей, связанных с профессиональной деятельностью, обучением, участием в жизни общества и других сферах жизни	Государственный экзамен, выпускная квалификационная работа
УК-2. Способность применять нормы государственного языка Российской Федерации в устной и письменной речи в процессе личной и профессиональной коммуникаций	Государственный экзамен,

	выпускная квалификационная работа
УК-3. Способность применять знания иностранного языка на уровне, достаточном для межличностного общения, учебной и профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
УК-4. Способность использовать прикладное программное обеспечение при решении профессиональных задач	Государственный экзамен, выпускная квалификационная работа
УК-5. Способность использовать основы правовых знаний в различных сферах деятельности	Государственный экзамен, выпускная квалификационная работа
УК-6. Способность применять методы физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
УК-7. Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	Государственный экзамен, выпускная квалификационная работа
УК-8. Способность и готовность к самоорганизации, продолжению образования, к самообразованию на основе принципов образования в течение всей жизни	Государственный экзамен, выпускная квалификационная работа
УК-9. Способность к индивидуальной и командной работе, социальному взаимодействию, соблюдению этических норм в межличностном профессиональном общении	Государственный экзамен, выпускная квалификационная работа
ПКН-1. Способность понимать значение и роль информации, информационных технологий и информационной безопасности в современном обществе	Государственный экзамен, выпускная квалификационная работа
ПКН-10. Способность проводить подготовку исходных данных для проектирования систем информационной безопасности и для технико-экономического обоснования соответствующих проектных решений	Государственный экзамен, выпускная квалификационная работа
ПКН-11. Способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью на объекте защиты	Государственный экзамен,

	выпускная квалификационная работа
ПКН-12. Способность проводить эксперименты по заданной методике и обработку их результатов, в том числе оценку погрешности и достоверности	Государственный экзамен, выпускная квалификационная работа
ПКН-13. Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Государственный экзамен, выпускная квалификационная работа
ПКН-14. Способность принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Государственный экзамен, выпускная квалификационная работа
ПКН-2. Способность применять необходимый математический аппарат для решения задач профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
ПКН-3. Способность применять необходимые физические законы и модели, анализировать физические явления и процессы для решения задач профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа

ПКН-4. Способность использовать современные языки программирования и технологии разработки программного обеспечения для решения задач профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
ПКН-5. Способность осуществлять подбор, изучение и обобщение научной, научно-технической, правовой литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
ПКН-6. Способность на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессиональной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессиональных задач	Государственный экзамен, выпускная квалификационная работа
ПКН-7. Способность применять информационно-коммуникационные технологии, программные средства системного, прикладного и инструментального назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
ПКН-8. Способность применять правовые акты, нормативные и методические документы, регламентирующие деятельность в сфере профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
ПКН-9. Способность применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Государственный экзамен, выпускная квалификационная работа
ПКП-1. Способность участвовать в разработке и реализации политики информационной безопасности автоматизированных финансово-банковских систем и контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Государственный экзамен, выпускная квалификационная работа
ПКП-2. Способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных финансово-банковских систем	Государственный экзамен, выпускная квалификационная работа
ПКП-3. Способность участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных финансово-банковских систем, контролировать события безопасности и действия пользователей автоматизированных систем	Государственный экзамен, выпускная квалификационная работа
ДПКН-4.1. Способность администрировать операционные системы, системы управления базами данных, вычислительные сети	Государственный экзамен, выпускная квалификационная работа

ДПКН-4.2. Способность выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	Государственный экзамен, выпускная квалификационная работа
ДПКН-4.3. Способность осуществлять диагностику и мониторинг систем защиты автоматизированных систем	Государственный экзамен, выпускная квалификационная работа
ДПКН-4.4.Способность проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	Государственный экзамен, выпускная квалификационная работа

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

Кафедра информационной безопасности

Факультета информационных технологий и анализа больших данных

УТВЕРЖДАЮ

Проректор по учебной
и методической работе

_____ Е.А. Каменева

«28» мая 2024 г.

Селезнёв В.М., Коннова И.Г.

Программа государственного экзамена

для студентов, обучающихся по направлению подготовки
10.03.01 Информационная безопасность
ОП «Безопасность автоматизированных систем
в финансово-банковской сфере»
профиль «Безопасность автоматизированных систем
в финансово-банковской сфере»

Рекомендовано Ученым советом Факультета информационных технологий и анализа больших данных (протокол от «21» мая 2024 г. № 44)

Одобрено на заседании Кафедры информационной безопасности (протокол от «25» апреля 2024 г. № 3)

Москва 2024

СОДЕРЖАНИЕ

1	Перечень вопросов, выносимых на государственный экзамен. Перечень рекомендуемой литературы для подготовки к государственному экзамену	9
2.	Примеры практико-ориентированных заданий	19
3.	Рекомендации обучающимся по подготовке к государственному экзамену	21
4.	Критерии оценки результатов сдачи государственных экзаменов	22

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. Правовое регулирование информационной безопасности в системе российского информационного права.

2. Роль и место информационной составляющей в системе национальной безопасности Российской Федерации. Национальные интересы и угрозы их безопасности.

3. Цель и приоритетные направления государственной политики в области технической защиты информации.

4. Виды нормативных правовых актов в сфере защиты информации.

5. Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации .

6. Понятие и виды юридической ответственности в области обеспечения информационной безопасности.

7. Субъекты и объекты правоотношений в области обеспечения информационной безопасности.

8. Классификация угроз информационной безопасности при формировании информационного общества в условиях глобализации.

9. Уголовно-правовая ответственность за информационные преступления.

10. Понятие информации ограниченного доступа. Правовые режимы тайн в системе организационного и правового обеспечение безопасности информации ограниченного доступа.

11. Основные задачи защиты информации, решаемые с использованием криптографических методов. Примеры.

12. Утечка информации по техническому каналу. Перехват информации. Технический канал утечки информации. Схема технического канала утечки

информации. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники.

13. Причины образования технических каналов утечки информации, возникающих за счет наводок побочных электромагнитных излучений (электромагнитные ТКУИ).

14. Специально создаваемые технические каналы утечки информации, обрабатываемой СВТ. Схема технического канала утечки информации, создаваемого путем высокочастотного облучения СВТ.

15. Аппаратные закладные устройства. Классификация аппаратных закладок. Схема технического канала утечки информации создаваемого путем внедрения в СВТ электронных устройств перехвата информации (аппаратных закладок).

16. Реестр сертифицированных средств защиты информации. Структура и содержание реестра. Условия включения средств защиты информации в реестр. Операции над записями реестра.

17. Выделенное помещение организации банковской сферы (определение). Контролируемая зона объекта. Утечка информации по техническому каналу. Перехват информации. Технический канал утечки информации (определение). Классификация технических каналов утечки речевой информации и способов перехвата речевой информации.

18. Схема прямого технического канала утечки речевой информации. Способы перехвата речевой информации по прямому техническому каналу утечки речевой информации (схемы каналов перехвата информации).

19. Перехват речевой информации с использованием цифровых диктофонов. Типы цифровых диктофонов. Основные характеристики цифровых диктофонов. Виды и основные характеристики направленных микрофонов.

20. Перехват речевой информации с использованием закладных устройств с передачей информации по радиоканалу. Аналоговые и цифровые радиозакладки (основные характеристики). Радиозакладки, построенные на

базе средств сотовой связи (основные характеристики). Радиозакладки, использующие для передачи сложные сигналы (основные характеристики).

21. Эксплуатация подсистем безопасности информации в автоматизированных системах. Мероприятия по охране труда и технике безопасности в процессе эксплуатации и обслуживания средств защиты информации.

22. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

23. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации. Основные требования при установке системы пространственного зашумления на объекте информатизации.

24. Сертификация средств защиты информации. Структура и принципы взаимодействия участников в системе сертификации средств защиты.

25. Сертификат соответствия средства защиты требованиям безопасности. Знаки соответствия. Процедура получения знаков соответствия и маркирования средств защиты информации.

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

а) основная литература:

1. Информационная безопасность: учебник/ В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева; под ред. В. П. Мельникова. – Москва : Кнорус, 2022. – 371 с. – ЭБС BOOK.ru. - URL: https://www.book.ru/book/941809 (дата обращения: 14.05.2024). - Текст : электронный.

2. Информационная безопасность: практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. – Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ЭБС ZNANIUM. - URL:

https://znanium.com/catalog/product/1094244 (дата обращения: 14.05.2024). – Текст : электронный.

б) дополнительная литература:

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. - URL: http://znanium.com/catalog.php?bookinfo=421968 (дата обращения: 14.05.2024). – Текст : электронный.

4. 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. — URL: http://znanium.com/catalog.php?bookinfo=405000 (дата обращения: 14.05.2024). — Текст : электронный.

в) нормативные акты

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

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

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

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

9. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера». с изменениями п. 7 (Указ Президента РФ от 13.07.2015 N 357).

10. 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)» .

11. 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».

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

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

14. ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации.

15. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.

г) ресурсы информационно-телекоммуникационной сети «Интернет»

16. Официальный сайт ФСТЭК России. https://fstec.ru/

17. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/

18. (http://library.fa.ru/files/elibfa.pdf)

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

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

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

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

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

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

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

1.3 Вопросы на основе содержания дисциплин профиля программы бакалавриата

1. Современное состояние безопасности банковских автоматизированных систем. Защита информации в автоматизированных системах банков. Реализация политики безопасности в автоматизированных банковских системах.

2. Реквизиты сертификатов актуальных ключей электронной подписи Центрального Банка России Требования к электронной подписи Центрального Банка России.

3. Модель оценивания реализации процессов защиты информации финансовых организаций согласно ГОСТ Р 57580.2-2018. Уровни оценивания. Характеристика уровней.

4. Организационные методы защиты банковской информации. Обеспечение безопасности компьютерных банковских сетей. Обеспечение безопасности электронных платежей.

5. Классификация и характеристика угроз безопасности информации в организациях банковской сферы. Угрозы несанкционированного доступа к информации в автоматизированных банковских системах.

6. Технологии идентификации и аутентификации пользователей в организациях банковской сферы. Метки аутентификации. Однофакторная и многофакторная аутентификация.

7. Наиболее распространенные методы совершения преступлений, связанных с системами дистанционного банковского обслуживания: внутренний и внешний злоумышленник.

8. Раскройте сущность и содержание основных законодательных актов аудита информационной безопасности в РФ?

9. Основные направления построения системы информационной безопасности в банковских структурах. Особенности и виды нарушений безопасности банковских информационных систем. Классификация угроз информационной безопасности банков.

10. Особенности требований Стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС) как ведомственного нормативного документа.

11. Опишите этапы работ по проведению внешнего аудита ИБ. Какой из этих этапов является, по-вашему, наиболее важным? Приведите примеры.

12. Банковские устройства самообслуживания. Риски использования банковских устройств самообслуживания. Меры предосторожности при использовании банкоматов.

13. Дистанционное банковское обслуживание. Задачи обеспечения безопасности в системах дистанционного банковского обслуживания. Назовите и охарактеризуйте основные криптографические средства защиты информации в ДБО.

14. Раскройте основные цели, задачи соответствия требованиям стандарта PCI DSS. Какая из этих задач является, по-вашему, наиболее эффективной? Приведите примеры.

15. Мошенничество в системах дистанционного банковского обслуживания. Схемы мошенничества с использованием электронных денег. Фишинг.

16. Инцидент информационной безопасности. Основные требования к обнаружению и реагированию на инциденты безопасности дистанционного банковского обслуживания.

17. Банковские устройства самообслуживания. Виды устройств. Нормативные документы, направленных на обеспечение безопасности банкоматов. Их требования.

18. Система электронных платежей. Принципы функционирования и технологические процессы. Перечень потенциальных угроз безопасности системы электронных платежей.

19. Гражданско-правовые вопросы в случае осуществления операций по поддельным, утраченным картам, с использованием реквизитов карт в сети Интернет.

20. Опишите показатели, используемые для оценки соответствия защиты информации финансовой организации требованиям ГОСТ Р 57580.1.

21. Технологические платежные процессы. Общие требования по обеспечению информационной безопасности платежных технологических процессов.

22. Аудит информационной безопасности. Виды аудита информационной безопасности. Аудит организации обеспечения информационной безопасности при дистанционном банковском обслуживании.

23. Аудит информационной безопасности. Методы проведения аудита информационной безопасности. Методика проведения внутреннего аудита.

24. Риск информационной безопасности. Составляющие риска. Методика оценки риска информационной безопасности в банковской системе.

25. Жизненный цикл управления рисками. Управление рисками, краткая характеристика для банков.

1.4 Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам дисциплин профиля программы бакалавриата

а) основная литература

1. Шульц, В. Л. Безопасность предпринимательской деятельности : учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Юрайт, 2024. — 585 с. — (Высшее образование). — ЭБС Юрайт. — URL:

https://urait.ru/bcode/543152 (дата обращения: 14.05.2024). — Текст : электронный.

2. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2021. — 327 с. — (Высшее образование). - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/1189342 (дата обращения: 14.05.2024). — Текст : электронный.

б) дополнительная

3. 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: 14.05.2024). – Текст : электронный.

4. Вейнберг, Р. Р. Интеллектуальный анализ данных и систем управления бизнес-правилами в телекоммуникациях: Монография / Р. Р. Вейнберг. – Москва : НИЦ ИНФРА-М, 2016. - 173 с. (Научная мысль). - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/520998 (дата обращения: 14.05.2024). – Текст : электронный.

5. 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. — URL: http://znanium.com/catalog.php?bookinfo=405000 (дата обращения 14.05.2024). — Текст : электронный.

6. Сотов, А. И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография / А. И. Сотов. — Москва : Русайнс, 2020. — 128 с. — ЭБС BOOK.ru. — URL: https://www.book.ru/book/934740 (дата обращения: 14.05.2024). — Текст : электронный.

в) нормативные акты

7. СТО БР БФБО-1.0 -2014. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

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

9. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия

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

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

12. ГОСТ Р ИСО/МЭК 27006-2020 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

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

14. 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.

г) ресурсы информационно-телекоммуникационной сети «Интернет»

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

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

3. Суглобов А.Е. Защита коммерческой информации как основа безопасности компаний - участников внешнеэкономической деятельности / Суглобов А.Е., Савин В.Ю. // Аудиторские ведомости, 2018. – № 3-С.65-72 — <URL:http://elib.fa.ru/art2018/bv1548.pdf>.

4. Российская научная библиотека www.rsl.ru.

5. Код безопасности - www.securitycode.ru.

6. Центральный банк Российской Федерации. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦерт). http://www.cbr.ru/fincert/

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

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

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

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

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

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

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

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

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

2. Примеры практико-ориентированных заданий

1. Перечислите основные задачи, которые должна решать служба безопасности известного Вам объекта информатизации кредитно-финансовой сферы. Укажите функции отдела ИБ в составе службы безопасности.

2. Предложите типовые мероприятия по созданию системы защиты конфиденциальной информации и их краткое содержание. На какие нормативно-правовые акты следует опираться?

3. Составьте перечень основных угроз безопасности персональных данных и предложите механизмы противодействия этим угрозам. На какие нормативно-правовые акты следует опираться?

4. Составьте перечень факторов, влияющих на инциденты информационной безопасности, анализ условий их возникновения.

5. Составьте перечень лицензионных требований при осуществлении деятельности по разработке и (или) производству средств защиты конфиденциальной информации, лицензирование которых отнесено к компетенции ФСТЭК.

6. Разработайте Порядок проведения служебного расследования по инциденту ИБ.

7. Разработайте типовую Инструкцию пользователя в случае обнаружения атак.

8. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

9. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них? Приведите примеры.

10. Каковы основные принципы защиты целостности данных? В чем заключается суть каждого из них? Приведите примеры.

11. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным? Приведите примеры.

12. Цель, задачи и функции управления электронными подписями на объекте КИИ. Раскройте основное содержание алгоритма электронной подписи. Приведите примеры использования электронной подписи в банковской сфере.

13. Проведите анализ возможных решений по защите объектов информационных систем финансово-кредитной организации от преднамеренных угроз

14. Проведите анализ возможных решений для защиты информационных систем финансово-кредитной организации от угроз безопасности, возникающих на этапе доступа пользователей или программ к ресурсам информационных систем финансово-кредитной организации

15. Проведите анализ возможных решений по защите информационных систем финансово-кредитной организации от внешних угроз информационной безопасности

16. Проведите анализ возможных решений для защиты информационных систем финансово-кредитной организации от внутренних угроз информационной безопасности

17. Проведите анализ возможных угроз при подключении локальной или корпоративной сети финансово-кредитной организации к глобальным сетям

18. Проведите анализ наиболее распространенных видов вредоносных программ

19. Проведите анализ возможных угроз безопасности и уязвимости в беспроводных сетях финансово-кредитной организации

20. Проведите анализ угроз безопасности, связанных с развитием Интернета вещей (IoT), а также услугами в облаке.

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 и опытом, полученным в период прохождения практики.

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

4 Критерии оценки результатов сдачи государственных экзаменов

Максимальное количество баллов (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.

«Удовлетворительно» (3 балла) за ответ на теоретический вопрос экзаменационного билета ставится, если студент не раскрывает основных моментов вопроса, логика изложения нарушена, ответы не всегда конкретны.

Оценка «неудовлетворительно» (2 балла) выставляется в случае, если материал излагается непоследовательно, не аргументировано, бессистемно, ответы на вопросы выявили несоответствие уровня знаний выпускника требованиям ОС ВО ФУ в части формируемых компетенций, а также дополнительным компетенциям, установленным вузом.

Критерии оценки умений выпускников в ходе решения практико-ориентированных заданий.

Максимальное количество баллов (5 баллов) ставится, если выпускник полностью справился с выполнением практико-ориентированного задания, обосновал полученные результаты.

Количество баллов снижается, если практико-ориентированное задание выполнено, но допускаются неточности в обосновании результатов.

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

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

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

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

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

Кафедра информационной безопасности
Факультета информационных технологий и анализа больших данных

Селезнёв В.М., Коннова И.Г.

Методические рекомендации по подготовке и защите выпускных квалификационных работ студентами

для студентов, обучающихся по направлению подготовки 10.03.01
Информационная безопасность
ОП «Безопасность автоматизированных систем в финансово-банковской сфере»
Профиль «Безопасность автоматизированных систем в финансово-банковской сфере»

Одобрено на заседании Кафедры информационной безопасности Факультета информационных технологий и анализа больших данных

(протокол № 3 от «25» апреля 2024 г.*)*

Москва 2024

1. Общие положения

1.1. Методические рекомендации разработаны для направления подготовки 10.03.01 «Информационная безопасность», ОП «Безопасность автоматизированных систем в финансово-банковской сфере», профиль «Безопасность автоматизированных систем в финансово-банковской сфере».

1.2. Перечень планируемых результатов освоения ОП в соответствии с ФГОС ВО, подлежащих оценке в ходе защиты ВКР:

Универсальные компетенции:

УК-1. Способность к восприятию межкультурного разнообразия общества, в социально-историческом, этическом и философских контекстах, анализу и мировоззренческой оценке происходящих процессов и закономерностей

УК-10. Способность осуществлять поиск, критически анализировать, обобщать и систематизировать информацию, использовать системный подход для решения поставленных задач

УК-11. Способность к постановке целей и задач исследований, выбору оптимальных путей и методов их достижения

УК-12. Способность использовать базовые дефектологические знания в социальной и профессиональной сферах

УК-13. Способность принимать обоснованные экономические решения в различных областях жизнедеятельности

УК-14. Способность формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению, попыткам фальсификации истории и противодействовать им в профессиональной деятельности

УК-15. Способность релевантно решаемым задачам использовать информационные ресурсы и информационно-коммуникационные технологии для достижения целей, связанных с профессиональной деятельностью, обучением, участием в жизни общества и других сферах жизни

УК-2. Способность применять нормы государственного языка Российской Федерации в устной и письменной речи в процессе личной и профессиональной коммуникаций

УК-3. Способность применять знания иностранного языка на уровне, достаточном для межличностного общения, учебной и профессиональной деятельности

УК-4. Способность использовать прикладное программное обеспечение при решении профессиональных задач

УК-5. Способность использовать основы правовых знаний в различных сферах деятельности

УК-6. Способность применять методы физической культуры для обеспечения полноценной социальной и профессиональной деятельности

УК-7. Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов

УК-8. Способность и готовность к самоорганизации, продолжению образования, к самообразованию на основе принципов образования в течение всей жизни

УК-9. Способность к индивидуальной и командной работе, социальному взаимодействию, соблюдению этических норм в межличностном профессиональном общении

Профессиональные компетенции направления:

ПКН-1. Способность понимать значение и роль информации, информационных технологий и информационной безопасности в современном обществе

ПКН-10. Способность проводить подготовку исходных данных для проектирования систем информационной безопасности и для технико-экономического обоснования соответствующих проектных решений

ПКН-11. Способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью на объекте защиты

ПКН-12. Способность проводить эксперименты по заданной методике и обработку их результатов, в том числе оценку погрешности и достоверности

ПКН-13. Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ПКН-14. Способность принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ПКН-2. Способность применять необходимый математический аппарат для решения задач профессиональной деятельности

ПКН-3. Способность применять необходимые физические законы и модели, анализировать физические явления и процессы для решения задач профессиональной деятельности

ПКН-4. Способность использовать современные языки программирования и технологии разработки программного обеспечения для решения задач профессиональной деятельности

ПКН-5. Способность осуществлять подбор, изучение и обобщение научной, научно-технической, правовой литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

ПКН-6. Способность на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессиональной деятельности, базирующиеся на гражданской

позиции, патриотизме, ответственном отношении к выполнению профессиональных зада

ПКН-7. Способность применять информационно-коммуникационные технологии, программные средства системного, прикладного и инструментального назначения, в том числе отечественного производства, для решения задач профессиональной деятельности

ПКН-8. Способность применять правовые акты, нормативные и методические документы, регламентирующие деятельность в сфере профессиональной деятельности

ПКН-9. Способность применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

Дополнительные профессиональные компетенции направления:

ДПКН-4.1. Способность администрировать операционные системы, системы управления базами данных, вычислительные сети

ДПКН-4.2. Способность выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем

ДПКН-4.3. Способность осуществлять диагностику и мониторинг систем защиты автоматизированных систем

ДПКН-4.4. Способность проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах

Профессиональные компетенции профиля:

ПКП-1. Способность участвовать в разработке и реализации политики информационной безопасности автоматизированных финансово-банковских систем и контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

ПКП-2. Способность участвовать в проектировании, эксплуатации и

совершенствовании системы управления информационной безопасностью автоматизированных финансово-банковских систем

ПКП-3. Способность участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных финансово-банковских систем, контролировать события безопасности и действия пользователей автоматизированных систем

Перечень знаний и умений, которые выпускник должен продемонстрировать для подтверждения освоенных компетенций:

знать: способы формирования комплекса мер по информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; виды информации и современные угрозы безопасности информации и возможные пути их реализации; принципы, методы и технологии проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; современные криптографические методы защиты, области эффективного применения различных классов методов защиты информации в информационно-технологических системах; основные нормативные и методические документы, используемые в оформлении рабочей технической документации; комплекс мер (по установке, настройке и обслуживанию) технических средств защиты информации.

уметь: формировать комплекс мер по информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; анализировать структуры и содержание информационных процессов и особенности функционирования объектов защиты с целью определения угроз безопасности информации и путей их реализации; проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; определять место криптографических средств в общей системе защиты информации в информационно-

технологической системе, применять методы защиты информации, оценивать эффективность криптографических систем защиты информации; использовать основные нормативные и методические документы для оформления рабочей технической документации; формировать и эффективно применять комплекс мер (по установке, настройке и обслуживанию) технических средств защиты информации.

2. Правила подготовки к защите ВКР

2.1. Требования к содержанию и продолжительности доклада по ВКР.

Для программ бакалавриата доклад 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.

На доклад обучающемуся отводится не более 10 минут.

2.2. Требования к презентации ВКР.

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

Требования к содержанию презентации.

На первом слайде должны быть: логотип и полное название Финансового университета, название факультета, кафедры, 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.

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 слайда.

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.

Кафедра организует и проводит предварительную защиту ВКР по утвержденному графику.

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

3. Критерии оценки ВКР

Перечень знаний и умений, которые выпускник по направлению подготовки 10.03.01 «Информационная безопасность» профиль: Информационная безопасность автоматизированных систем в финансово-банковской сфере систем должен продемонстрировать для подтверждения освоенных компетенций приведен в разделе 1 «Общие положения» настоящих Методических рекомендаций.

При формировании критериев оценки члены ГЭК используют перечень знаний и умений, которые выпускник должен продемонстрировать для подтверждения освоенных программ бакалавриата.

В качестве основы оценки ВКР принимаются следующие базовые критерии:

— «Отлично» – работа имеет исследовательский характер, грамотно изложенную теоретическую часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. При ее защите обучающийся 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. В целом, работа и защита демонстрируют высокий уровень освоения компетенций обучающимся.

— «Хорошо» – работа имеет исследовательский характер, грамотно изложенную теоретическую часть, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными предложениями. При ее защите обучающийся 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. В целом, работа и защита демонстрируют средний уровень освоения компетенций обучающимся.

— «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 обучающийся 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. В целом, работа и защита демонстрируют базовый уровень освоения компетенций обучающимся.

— «Неудовлетворительно» – работа не носит исследовательского характера, в ней отсутствуют выводы, или они носят декларативный характер. При защите работы обучающийся затрудняется отвечать на поставленные вопросы, при этом допускает существенные ошибки. В отзыве руководителя имеются критические замечания. Работа и защита не демонстрируют освоения ряда компетенций обучающимися.

4. Структура и содержание ВКР

4.1 Выпускная квалификационная работа должна отвечать следующим требованиям:

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

— использование в аналитической части исследования статистической информации, обоснованного комплекса методов и методик, способствующих раскрытию сути проблемы;

— целостность работы, которая проявляется в связанности теоретической и практической его частей;

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

— достаточность и современность использованного библиографического материала.

4.2 ВКР должна включать следующие разделы:

— титульный лист;

— содержание;

— введение;

— основная часть, структурированная на главы и параграфы;

— заключение;

— список использованных источников;

— приложения (при наличии).

4.3 Рекомендуемый объем ВКР для обучающихся по программам бакалавриата составляет не менее 60 и не более 80 страниц без учета приложений. При выполнении коллективной ВКР объем работы может быть увеличен до 80-120 страниц без учета приложений.

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.).

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

Сведения, содержащиеся в этой главе, должны давать полное представление о состоянии и степени изученности поставленной проблемы. В рамках главы, в частности, обобщается и систематизируется понятийный аппарат, дается критическая оценка имеющихся понятий и их уточнение, приводятся классификации основных понятий по различным критериальным признакам, описываются теоретические концепции и эволюция взглядов научного сообщества по предмету исследования, а также имеющиеся средства и методы измерения и решения рассматриваемой проблемы; характеризуется степень проработанности проблемы в России и за рубежом и др.

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

Завершается первая глава обоснованием необходимости проведения аналитической части работы.

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

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

4.3.5 В ней содержится:

— анализ конкретного материала по избранной теме (на примере конкретной организации, отрасли, региона, страны, сферы) желательно за период не менее 3-х лет;

— сравнительный анализ с действующей практикой (на примере ряда организаций, отрасли (отраслей), региона (регионов), страны;

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

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

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

Практическая часть работы должна содержать самостоятельно проведенные обучающимся расчеты, составленный иллюстративный материал:

рисунки (графики, диаграммы, схемы), таблицы. Весь иллюстративный материал должен быть проанализирован и использован для подтверждения выводов по исследуемой проблеме.

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

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

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

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

Объем заключения, должен составлять, как правило, до 5-ти страниц. Заключение является основой доклада, обучающегося на защите ВКР.

4.3.8 Список использованных источников должен содержать сведения об источниках, которые использовались или были изучены при подготовке ВКР (не менее 40 наименований для программ бакалавриата) и характеризует осведомленность обучающегося по изучаемой проблеме.

4.3.9 Список использованных источников располагается в следующем порядке:

— законы Российской Федерации (в прямой хронологической последовательности);

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

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

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

— авторефераты диссертаций (в алфавитном порядке);

— научные статьи (в алфавитном порядке);

— литература на иностранном языке (в алфавитном порядке);

— интернет-источники [13].

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

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

5. Требования к оформлению ВКР

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

Оформление ВКР должно производиться по общим правилам, изложенным в ГОСТ 7.32-2017 «Отчет о научно-исследовательской работе. Структура и правила оформления». [13]

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» [14];

ГОСТ 7.80-2000 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Заголовок. Общие требования и правила составления» [15];

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» [16];

ГОСТ 7.11-2004 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на иностранных европейских языках» [17].

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] [18], 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.

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

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

Заголовки, подзаголовки и подстрочные сноски (состоящие из нескольких

[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.

строк) печатаются через одинарный интервал.

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

Нумерация 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.

7.1 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.

7.2 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. Иллюстрации, за

исключением иллюстраций приложений, следует нумеровать арабскими цифрами сквозной нумерацией (то есть по всему тексту) - 1,2,3, и т.д., либо внутри каждой главы - 1.1,1.2, и т.д. Наименование рисунка располагается посредине, без точки в конце.

Пример



Рисунок 1 – Модель атаки «один к одному»

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например – Рисунок А.2.

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».

Пример

Таблица 1.1 – Результаты расчетов

Шаг	ω, Гц	$\frac{\lvert U_1(j\omega)\rvert}{Ut_и}$	$\lvert H(j\omega)\rvert$	$\frac{\lvert U_2(j\omega)\rvert}{Ut_и}$
0,2	2590	0,780485598	0,37021511	0,288947561

…	…	…	…	…
4	51800	0,041056634	1,02954421	0,04226962

7.3 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;

π – 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: (А.1)

7.4 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.

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.

7.5 Список литературы (использованных источников) и интернет-ресурсов

После заключения, начиная с новой страницы, необходимо поместить список использованных источников и интернет-ресурсов.

Список 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.

7.6 Образцы библиографических описаний документов в списках литературы представлены в [19].

7.7 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.

Формы всей необходимой отчетности по ВКР образовательной программы

бакалавриата (включая заявление на выбор темы ВКР, титульный лист ВКР, план-задание, отзыв научного руководителя, отзыв научного руководителя для коллективной ВКР, рецензию, разрешение на размещение ВКР), адаптированные к текущему учебному году, размещены на странице Кафедры информационной безопасности по ссылке http://www.fa.ru/org/chair/is/Pages/bak.aspx [7].

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. Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность: Приказ Министерства науки и высшего образования РФ от 17 ноября 2020 г. N 1427 [Электронный ресурс]. – URL: https://fgosvo.ru/uploadfiles/FGOS%20VO%203++/Bak/100301_B_3_19022021.pdf

3. Образовательные стандарты высшего образования ФГОБУ «Финансовый университет при Правительстве Российской Федерации». – Режим доступа: http://www.fa.ru/sveden/pages/os-finuniver.aspx

4. 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

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 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%B

C%D0%B0%D0%B3%20%D0%BE%D1%82%2018.10.2021.pdf

7. Портал Финансового университета. Структура. Кафедры. Кафедра информационной безопасности. Бакалавриат. – Режим доступа: http:// http://www.fa.ru/org/chair/is/Pages/bak.aspx

8. Об утверждении регламента подготовки и защиты выпускной квалификационной работы, выполненной в виде Start Up проекта: Приказ Финуниверситета от 05.10.2021 №2085/о. [Электронный ресурс]. – URL: http://www.fa.ru/org/dep/is/Documents/%D0%9F%D1%80%D0%B8%D0%BA%D0%B0%D0%B7%20%E2%84%96%202085_%D0%BE%20%D0%BE%D1%82%2005.10.2021.PDF

9. Об утверждении правил внутреннего трудового и внутреннего распорядка обучающихся: Приказ Финуниверситета от 15.07.2013 №1335/о. – URL:
http://www.fa.ru/sveden/Documents/Sveden/2017/Prikaz_1335o_15072013.pdf

10. 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

11. Об утверждении Порядка проведения государственной итоговой

аттестации по программам бакалавриата и магистратуры в Финансовом университете, утвержденного приказом Финуниверситета от 14.10.2016 № 1988/0 – URL: http://www.fa.ru/univer/DocLib/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F%20%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%B0/%D0%9D%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D0%B5%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B%20%D0%BF%D0%BE%20%D0%B3%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B8%D1%82%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D0%B9%20%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D0%B8%20(%D0%92%D0%9A%D0%A0,%20%D0%93%D0%AD%D0%9A)/%D0%9F%D1%80%D0%B8%D0%BA%D0%B0%D0%B7%20%E2%84%961988%D0%BE%20%D0%BE%D1%82%2014.10.2016.PDF

12. Образовательная программа высшего образования – программа бакалавриата. Направление подготовки: 10.03.01 Информационная безопасность. Профиль: «Безопасность автоматизированных систем в финансово-банковской сфере»: Утверждено Ректором Финансового Университета 25 января 2022 – URL: http://www.fa.ru/org/div/umoop/Documents/Obraz_Progs/%D0%91%D0%B0%D0%BA%D0%B0%D0%BB%D0%B0%D0%B2%D1%80%D0%B8%D0%B0%D1%82_2022/%D0%9E%D0%B1%D1%89_%D0%A5%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80_%D0%91%D0%B0%D0%BA_2022/%D0%98%D0%91_%D0%9E%D0%9F%20%D0%91%D0%90%D0%A1%D0%B2%D0%A4%D0%91%D0%A1_%D0%B1%D0%B0%D0%BA%2022.pdf

13. 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

14. 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

15. 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

16. 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

17. 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 .

18. 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/

19. 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.