**Федеральное государственное образовательное бюджетное учреждение**

**высшего образования**

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**(Финансовый университет)**

**Кафедра Информационная безопасность**

**Программа государственной итоговой аттестации**

для студентов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность

профиль: Безопасность автоматизированных систем в финансово-банковской сфере

*Одобрено заседанием кафедры «Информационная безопасность»*

*протокол № 5 от 25.11.2019г.*

**Москва 2019**

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

|  |  |
| --- | --- |
| Код и наименование компетенции | Форма государственной итоговой аттестации, в рамках которой проверяется сформированность компетенции |
| 1 | 2 |
| способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1) | Защита ВКР |
| способность использовать основы экономических знаний в различных сферах деятельности (ОК-2) | Государственный экзамен  Защита ВКР |
| способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3) | Государственный экзамен  Защита ВКР |
| способность использовать основы правовых знаний в различных сферах деятельности (ОК-4) | Государственный экзамен  Защита ВКР |
| способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5) | Защита ВКР |
| способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6) | Защита ВКР |
| способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7) | Защита ВКР |
| способность к самоорганизации и самообразованию (ОК-8) | Защита ВКР |
| способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9) | Защита ВКР |
| способность анализировать физические явления и процессы для решения профессиональных задач (ОПК-1); | Государственный экзамен  Защита ВКР |
| способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2); | Государственный экзамен  Защита ВКР |
| способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3) | Государственный экзамен |
| способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4) | Защита ВКР |
| способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5) | Государственный экзамен  Защита ВКР |
| способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6) | Защита ВКР |
| способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7) | Государственный экзамен  Защита ВКР |
| способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1) | Защита ВКР |
| способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2) | Защита ВКР |
| способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3) | Защита ВКР |
| способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4) | Государственный экзамен  Защита ВКР |
| способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5) | Защита ВКР |
| способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); | Защита ВКР |
| способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7) | Государственный экзамен  Защита ВКР |
| способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8) | Защита ВКР |
| способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9) | Государственный экзамен  Защита ВКР |
| способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10) | Государственный экзамен  Защита ВКР |
| способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11) | Защита ВКР |
| способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12) | Защита ВКР |
| способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13) | Государственный экзамен  Защита ВКР |
| способность организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14) | Защита ВКР |
| способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15). | Государственный экзамен  Защита ВКР |
| способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных финансово-банковских систем и противодействию технической разведке (ПКП-1) | Государственный экзамен  Защита ВКР |
| 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) | Государственный экзамен  Защита ВКР |
| способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных финансово-банковских систем (ПКП-3) | Защита ВКР |
| способность участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных финансово-банковских систем, контролировать события безопасности и действия пользователей автоматизированных систем (ПКП-4) | Защита ВКР |
| способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной финансово-банковской системы и документировать процедуры и результаты функционирования системы защиты информации автоматизированной системы(ПКП-5) | Государственный экзамен  Защита ВКР |
| способность проводить мониторинг защищенности информации автоматизированной финансово-банковской системы (ПКП-6) | Государственный экзамен  Защита ВКР |

**Федеральное государственное образовательное бюджетное учреждение**

**высшего образования**

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**(Финансовый университет)**

**Кафедра Информационная безопасность**

|  |
| --- |
| УТВЕРЖДАЮ  Ректор  \_\_\_\_\_\_\_\_\_\_\_\_ М.А. Эскиндаров  **17.12. 2019 г.** |

**Евсеев В.Л., Оладько В.С.**

**Программа государственного экзамена**

для студентов, обучающихся по направлению подготовки

10.03.01 Информационная безопасность

профиль: Безопасность автоматизированных систем в финансово-банковской сфере

*Рекомендовано Ученым советом факультета прикладной математики и информационных технологий*

*протокол №20 от 09.12.2019г.*

*Одобрено заседанием кафедры «Информационная безопасность»*

*протокол №5 от 25.11.2019 г.*

**Москва 2019**

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ………………………………..……………………………………… ……7](#_Toc532658686)

[1 Перечень вопросов, выносимых на государственный экзамен. Перечень рекомендуемой литературы для подготовки к государственному экзамену….…....8](#_Toc532658687)

[1.1 Вопросы на основе содержания общепрофессиональных и профессиональных дисциплин программы бакалавриата………………...………………………….…...8](#_Toc532658688)

[1.2 Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам общепрофессиональных и профессиональных дисциплин……………………………………………..…………………………..…..14](#_Toc532658689)

[1.3 Вопросы на основе содержания дисциплин профиля программы бакалавриата…………………………………………………………………………..16](#_Toc532658690)

[1.4 Перечень рекомендуемой литературы для подготовки к государственному экзамену по вопросам дисциплин профиля программы бакалавриата…….….…..20](#_Toc532658691)

[2 Примеры практико-ориентированных заданий………………….…………….....23](#_Toc532658692)

[3 Рекомендации обучающимся по подготовке к государственному экзамену…..26](#_Toc532658693)

[4 Критерии оценки результатов сдачи государственных экзаменов…………......27](#_Toc532658694)

# **ВВЕДЕНИЕ**

В соответствии с Федеральным государственным образовательным стандартом высшего образования подготовки бакалавров по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1515, государственный экзамен, как форма итоговой государственной аттестации, направлен на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВО.

Программа государственного экзамена по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) – бакалавр) 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».

# **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. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Сущность и определение понятия защиты информации.
2. Место защиты информации в системе обеспечения безопасности Российской Федерации. Значение защиты информации для субъектов информационных отношений: государства, общества, личности.
3. Современные подходы к составу защищаемой информации. Основания и принципы отнесения информации к защищаемой, категории информации, подпадающие под эту основу. Критерии отнесения информации к защищаемой, необходимостью защиты информации от утраты и утечки.
4. Становление и современное определение понятия «государственная тайна». Основания отнесения информации к государственной тайне.
5. Современные подходы к защите служебной тайны. Понятие служебной тайны, границы и области ее действия. Распределение полномочий по отнесению сведений к служебной тайне.
6. Понятие угрозы информационной безопасности. Связь угрозы информации с уязвимостью информации. Признаки и источники угроз информационной безопасности организаций банковской сферы.
7. Каналы несанкционированного доступа к информации как составная часть угроз информации. Современные подходы к понятию канал несанкционированного доступа к информации.
8. Факторы, воздействующие на безопасность защищаемой информации. Каналы утечки информации ограниченного доступа. Условия и факторы, способствующие утечке информации ограниченного доступа.
9. Общая характеристика технических средств несанкционированного получения информации и технологий их применения. Виды моделей систем и процессов защиты информации. Основные организационные меры и направления инженерно-технической защиты информации
10. Категорирование и проведение специальных мероприятий по технической защите информации на объектах информатизации. Основные понятия и положения защиты информации в автоматизированных системах.
11. Нарушитель и информационной безопасности. Виды нарушителей. Модель нарушителя безопасности.
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.
26. Лицензирование деятельности в области технической защиты информации. Виды лицензируемой деятельности. Требования к лицензиату.
27. Аттестация объекта по требованиям безопасности. Аттестат соответствия. Программа и методика аттестационных испытаний. Специальные исследования. Специальные проверки. Специальные обследования.
28. Специальные технические средства подавления средств перехвата речевой информации: подавители диктофонов, широкополосные генераторы шума.
29. Системные вопросы и основные термины криптологии. Классификация шифров. Базовые протоколы секретной связи на основе симметричной и асимметричной криптосистем.
30. Система RSA. Проверка чисел на простоту. Метод пробных делений. Решето Эратосфена. Вероятностный тест Ферма. Детерминированные алгоритмы распознавания простоты. Генерация простых чисел.
31. Блочные шифры. SP-сети, шифры Фейстеля. Инволютивность алгоритма шифрования.
32. Алгоритмы DES, ГОСТ 28147-89, AES, их характеристики: длина блока число раундов шифрования, длина ключа.
33. Инфраструктура на основе криптографии с открытыми ключами (ИОК). Сертификаты. Управление сертификатами. Компоненты ИОК и их функции. Стандарты в области ИОК. Управление ключами.
34. Понятие электронной подписи. Федеральный закон N 63-ФЗ «Об электронной подписи». Задачи и области применения электронной подписи. Виды электронной подписи.
35. Ассиметричные криптографические алгоритмы, электронная подпись, хеширование (DSA, ГОСТ Р 34.10-2001, MD5, SHA1, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012).
36. Ключи криптосистемы: размер, случайность, секретность. Жизненный цикл ключей. Схемы разделения секрета, пороговые схемы. Ключевые протоколы: симметричные 2-х и 3-хсторонние, бесключевой протокол Шамира, асимметричные Диффи-Хеллмана, «станция-станция», Мэсси-Омуры.
37. Уязвимость. Характеристика уязвимостей системного и прикладного программного обеспечения. Средства поиска и анализа уязвимостей. Меры устранения уязвимостей.
38. Характеристика угроз безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия. Современные технологии обнаружения вторжений.
39. Вредоносное программное обеспечение. Понятие. Схема классификация вредоносного программного обеспечения. Признаки и способы проявления.
40. Технологии управления доступом к информации на основе дискретного и мандатного управления доступом.
41. Понятие «Политика информационной безопасности». Перечислите содержание политики ИБ. Перечислите политики ИБ, которые рекомендуется разрабатывать в соответствии с международными стандартами ИСО/МЭК.
42. Жизненный цикл информационной безопасности. Перечислите этапы жизненного цикла ИБ-услуг по ITIL. Опишите содержание деятельности в рамках каждого этапа.
43. Определите суть сервис-ориентированного подхода к управлению информационной безопасности, опишите содержание договора SLA, опишите содержание договора OLA. Определите суть процессного подхода к управлению ИБ. Перечислите процессы, поддерживающие управление ИБ в банковской организации.
44. Организационно-психологические аспекты работы с сотрудниками по защите информации ограниченного доступа. Создание в коллективе здорового психологического климата. Создание корпоративной культуры в организации.
45. Средства обеспечения защиты информации от угрозы НСД. Принципы функционирования. Задачи. Примеры современных средств защиты информации от НСД.
46. Факторы угроз информационной безопасности через СМИ и рекламу. Основные приемы психологического воздействия через СМИ.
47. Информационная сфера как сфера обращения информации и правового регулирования. Методы правового регулирования, принципы, субъекты и объекты информационного права.
48. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации по содержанию ФЗ РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
49. Сети и системы передачи данных. Классификация сетей. Уровни модели взаимодействия открытых систем (модель OSI). Требования по защите информации в сетях общего пользования.
50. Вторжения в сети передачи данных. Сетевые атаки и аномалии. Архитектура систем обнаружения вторжений в сети передачи данных. Профили систем обнаружения вторжений.
51. Межсетевое экранирование. Классификация межсетевых экранов. Уровни и правила фильтрации трафика. Особенности межсетевых экранов с DPI (NGFW). Демилитаризованная зона.
52. DLP-системы контроля утечек информации. Типовая архитектура. Принципы функционирования. Современные DLP-системы российского и международного производства.
53. SIEM-системы. Типовая архитектура. Принципы функционирования. Особенности сбора данные и корреляции событий безопасности. Современные SIEM российского и международного производства.
54. Критическая информационная инфраструктура (КИИ). Понятие. Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
55. Построение защищенных сетей с помощью технологии ViPNet. Инкапсуляция и шифрование трафика. Открытие защищенные и туннелируемые узлы. Функции ViPNet-Coordinator, ViPNet-Administrator, ViPNet-Client.
56. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Архитектура. Функции. Средства ГоcСОПКА.
57. Средства защиты программного обеспечения от несанкционированной загрузки. Программно-аппаратная защита программ от несанкционированного копирования, пароли и ключи.
58. Защита программ от изучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям.
59. Материально-вещественный канал утечки информации. Защита информации на машинных носителях. Методы и средства гарантированного уничтожения информации. Защита остатков информации.
60. Системы обнаружения вторжений. Уровни наблюдения систем обнаружения вторжений – характеристика, достоинства и недостатки. Методы обнаружения вторжений – характеристика, достоинства и недостатки.

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

**а) основная литература:**

1. Гришина, Н. В. Информационная безопасность предприятия: учебное пособие / Н. В. Гришина. — Москва: ФОРУМ, 2019. – 216 с. – ЭБС ZNANIUM.com. – URL: http://znanium.com/catalog/product/1017663 (дата обращения: 25.12.2019). - Текст: электронный

2. Нестеров, С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва: Юрайт, 2019. — 321 с. – ЭБС Юрайт. – URL: https://www.biblio-online.ru/bcode/434171 (дата обращения: 25.12.2019). – Текст: электронный.

**б) дополнительная литература:**

3. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. — Москва: Горячая линия-Телеком, 2013. —220 с. — ЭБС ZNANIUM.com. — URL: <http://znanium.com/catalog.php?bookinfo=421968>(дата обращения: 25.12.2019). – 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.com. — http://znanium.com/catalog.php?bookinfo=405000.(дата обращения 25.12.2019) — Текст: электронный

**в) нормативные акты**

1. Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации» (с дополнениями и изменениями).
2. [Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».](http://www.consultant.ru/document/cons_doc_LAW_220885/)
3. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ.
4. Стандарт ISO 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
5. 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).
6. [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)"](http://www.e-nigma.ru/stat/p090208/).
7. 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».
8. Приказ ФСТЭК № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методический документ. ФСТЭК России, 2008 г. (обновление 2013 г.).
10. [ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации](http://www.e-nigma.ru/stat/gost/).

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

1. Официальный сайт ФСТЭК России. https://fstec.ru/
2. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
3. (http://library.fa.ru/files/elibfa.pdf)
4. Электронно-библиотечная система BOOK.RU http://www.book.ru
5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
6. Электронно-библиотечная система Znanium http://www.znanium.com
7. «Деловая онлайн библиотека» издательства «Альпина Паблишер» http://lib.alpinadigital.ru/en/library
8. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com/
9. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/
10. 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: инсайд, внешний злоумышленник.
8. Становление и современное определение коммерческой тайны. Место коммерческой тайны в системе банковской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Функции государства в сфере защиты коммерческой тайны. Тенденция и определяющие факторы защиты коммерческой тайны.
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. Электронные заместители денежных средств. Противодействие социальным мошенническим схемам в сфере электронных денег.
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. Безопасность банковских карт. Основные способы защиты, которыми пользуются владельцы банковских карт, их эффективность.
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. Понятие атаки злоумышленника. Атаки на держателей пластиковых карт. Способы противодействия атакам на держателей карт.
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.
26. Автоматизированная банковская система. Активы организации банковской системы Российской Федерации. Ценность активов.
27. События безопасности. Мониторинг событий и инцидентов в организациях банковской системы РФ. Программные средства проведения мониторинга событий и инцидентов безопасности.
28. Радикальное изменение способов и условий осуществления банковской деятельности при применении кредитными организациями технологий ДБО или, иначе, «электронного банкинга».
29. Основные виды противоправной деятельности в области предоставления финансовых услуг. Этапы организации противодействия противоправной деятельности (ППД) в области предоставления финансовых услуг.
30. Методики оценки соответствия ИТ-инфраструктуры финансовой организации требованиям по безопасности информации и разработка плана мероприятий по обеспечению соответствия. Анализ защищенности финансовых систем.
31. Планирование непрерывности бизнеса. Превентивные меры. Стратегии восстановления. Восстановление бизнес-процессов.

# **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 в 2 ч. Часть 1: учебник для академического бакалавриата / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко; под ред. В. Л. Шульца. — Москва: Юрайт, 2019. — 288 с. — ЭБС Юрайт.— URL: <https://www.biblio-online.ru/book/bezopasnost-predprinimatelskoy-deyatelnosti-v-2-ch-chast-1-432979> (дата обращения 25.12.2019) —Текст : электронный.
2. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. — Москва: Форум: ИНФРА-М, 2019. — 352 с. — ЭБС ZNANIUM.com. — URL: http://znanium.com/catalog/product/1025261(дата обращения 25.12.2019) —Текст: электронный.

**б) дополнительная**

1. Муссель, К. М. Платежные технологии: системы и инструменты: научно-популярное издание / К.М. Муссель. — Москва: Центр Исследований Платежных Систем и Расчетов (ЦИПСиР), 2015. — 288 с. — ЭБС ZNANIUM.com. —URL: http://znanium.com/go.php?id=556619. (дата обращения 25.12.2019) —Текст: электронный.
2. Вейнберг, Р.Р. Интеллектуальный анализ данных и систем управления бизнес-правилами в телекоммуникациях: монография/ Р.Р. Вейнберг. — Москва: НИЦ ИНФРА-М, 2016. — 173 с. — ЭБС ZNANIUM.com URL: http://znanium.com/catalog.php?bookinfo=520998. (дата обращения 25.12.2019) — Текст: электронный
3. 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. — http://znanium.com/catalog.php?bookinfo=405000.(дата обращения 25.12.2019) — Текст: электронный
4. Сотов, А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография / А.И. Сотов. — Москва: Русайнс, 2017. — 127с. — ЭБС BOOK.ru. — URL: <https://www.book.ru/book/920258>. (дата обращения 25.12.2019) —Текст: электронный.

**в) нормативные акты**

1. СТО БР БФБО-1.0. -2014. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.
2. СТО БР БФБО-1.5.-2018. Стандарт Банка России. Безопасность финансовых (банковских) операций управления инцидентами информационной безопасности.
3. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия
4. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
5. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
6. ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.
7. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.
8. 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](http://www.rsl.ru).
5. Код безопасности - [www.securitycode.ru](http://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

# **Примеры практико-ориентированных заданий**

1. При техногенной аварии были потеряны все необходимые для возобновления банковских 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.

2. В организации финансово-банковской сферы, имеющей несколько территориально-распределённых объектов (филиалы 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.

4. Во время посещения отдела кадров финансовой организации 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.

5. Имеется филиал финансово-банковской организации, предоставляющей банковские услуги физическим лица и имеющей в смежным с основным залом помещении зоны 24ч. с банкоматами. Задание: Предложите перечень мероприятий, которые должны осуществляться для защиты информации при работе с посетителями на объекте.

6. Имеется банковская организация, расположенная в отдельном здании с собственной огороженной территорией и парковкой для посетителей и сотрудников, предоставляющая услуги кредитования физическим и юридическим лицам. Задание: Предложите мер и инженерно-технических средств защиты информации, которые должны войти в состав интегрированной системы безопасности объекта информатизации кредитно-финансовой сферы.

7. Определите эффект от применения межсетевого экрана (МСЭ), если вероятность реализации угрозы заражения вредоносным ПО до применения МСЭ один раз в 10 дней, размер ущерба – 150 000 рублей, после применения МСЭ вероятность снизилась в 10 раз, а размер возможного ущерба не изменился.

8. Оцените риск заражения информационной системы вирусом, если вероятность угрозы составляет 90%, вероятность наличия уязвимости – 20%. Размер ущерба составит 100 000 рублей.

9. В ИСПДн обрабатываются персональные данные: фио, национальность, год рождения, банковские счета. Для ИСПДн актуальны угрозы ошибок в коде системы и наличие процедур, приводящих к нарушению целостности данных. Определите уровень защищенности ИСПДн. Обоснуйте свое решение.

10. Рассчитать коэффициент возврата инвестиций IDS системы на периоде 3 года. Лицензия на IDS-систему составляет 14 000 доллларов. Аппаратное и системное программное обеспечение составляет 10 000 долларов сша. Обучение сотрудников 2 000 долларов сша. Поддержка IDS системы составляет 3 000 долларов в год. Ущерб от каждого вторжения составляет 10 000 долларов. Частота атаки 10 раз в год. Вероятность наличия уязвимости 50%.

11. Имеется организация, чья деятельность связана с финансово-кредитной сферой. Организации необходимо привлечь клиентов посредством рекламы своих услуг. Задание: Сформулируйте правила, которые следует соблюдать для обеспечения безопасности конфиденциальной информации при подготовке рекламно-выставочных материалов на объекте кредитно-финансовой сферы.

12. Имеется организация, чья деятельность связана с финансово-кредитной сферой и предоставлении услуг физическим лицам и индивидуальным предпринимателям. Задание: Перечислите этапы и принципы, которые должен содержать процесс увольнения сотрудника, допущенного к конфиденциальной информации данной организации кредитно-финансовой сферы.

13. Имеется банковская организация, расположенная в отдельном здании с собственной огороженной территорией и парковкой для посетителей и сотрудников, предоставляющая услуги кредитования физическим и юридическим лицам. Задание: Предложите, какие функции должно обеспечивать автоматизированное рабочее места оператора службы безопасности банковской организации.

14. В результате проведенного моделирования, актуальной угрозой безопасности информации связанной с услугами доступа к Интернету для сотрудников компании, являются вирусные атаки и внедрение вредоносных программ. Нарушаемое свойства безопасности активов: целостность, управление доступом, аутентификация. Задание: Провести анализ мер и средств контроля и управления безопасности для сценария доступа сотрудников к Интернету при актуальной угрозе - вирусные атаки и внедрение вредоносных программ.

15. В результате проведенного моделирования, актуальной угрозой безопасности информации, связанной с услугами бизнес-клиент, является фальсификация информационного наполнения транзакций. Нарушаемое свойства безопасности активов: неотказуемость. Провести анализ мер и средств контроля и управления безопасности для сценария услуг бизнес-клиент при актуальной угрозе - фальсификация информационного наполнения транзакций.

16. Разработайте документ «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

17. Проведенный аудит информационной системы предприятия показал наличие возможности группе пользователей устанавливать на рабочие станции дополнительное программное обеспечение. Докажите, что данная процедура может быть небезопасна, и предложите решение по устранению данной проблемы.

18. Используя ресурсы операционной системы Windows, докажите незащищенность от «троянских» программ. Задание: опишите как данное вредоносное ПО может маскироваться и предложите решения по повышению защищённости.

19. Проходя практику по информационной безопасности в медицинском учреждении, Вы убеждаетесь в серьезности проблемы обеспечения информационной безопасности, но специалистов в данной области нет. Выйдя из метро на работу, Вы сталкиваетесь с главным врачом и понимаете, что это шанс объяснить ему о необходимости применения средств защиты информации. У Вас есть только 5 минут, чтоб добиться результата.

20. Опишите процедуру проведения специального исследования на выявление попыток НСД в АС. Дайте рекомендации по устранению возможности обхода загрузки операционной системы, обрабатывающей персональные данные.

21. В результате обследования информационных ресурсов объекта информатизации (организации) выявлено, что в базу данных одной из функциональных АИС включены данные, составляющие сведения о кассовых и банковских операциях, остатки на счетах, займы и обязательства. Возможно и следует ли их отнести к информационным объектам ограниченного доступа? Предложите обоснование.

22. На объекте информатизации проводится комплексное обследование информационных ресурсов, средств и процессов обработки информации с целью выявления уязвимостей и решения вопросов по конфигурации СОВ. Предложите организационную схему проведения обследования и роли специалистов по безопасности, ИТ-специалистов и уполномоченных руководства различного уровня.

# **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.

# **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)**

**Информационная безопасность**

Оладько В.С., Козьминых С.И., Коннова И.Г.

**Методические рекомендации по подготовке и защите выпускных квалификационных работ студентами**

для студентов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность

профиль: Безопасность автоматизированных систем в финансово-банковской сфере

*Одобрено заседанием кафедры «Информационная безопасность»*

*протокол №3 от 26.09.2019 г.*

**Москва 2019**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Образовательная программа высшего образования – программа бакалавриата, реализуемая Финансовым университетом по направлению подготовки 10.03.01 Информационная безопасность (далее – программа бакалавриата), 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 1515) [2] с учетом требований рынка труда.

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

* способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
* способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
* способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);
* способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
* способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
* способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
* способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);
* способностью к самоорганизации и самообразованию (ОК-8);
* способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).
* способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);
* способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);
* способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);
* способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
* способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);
* способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);
* способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
* способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
* способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);
* способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
* способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);
* способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);
* способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);
* способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
* способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);
* способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);
* способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);
* способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);
* способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);
* способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);
* способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);
* способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных финансово-банковских систем и противодействию технической разведке (ПКП-1);
* способностью 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);
* способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных финансово-банковских систем (ПКП-3);
* способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных финансово-банковских систем, контролировать события безопасности и действия пользователей автоматизированных систем (ПКП-4);
* способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной финансово-банковской системы и документировать процедуры и результаты функционирования системы защиты информации автоматизированной системы(ПКП-5);
* способностью проводить мониторинг защищенности информации автоматизированной финансово-банковской системы (ПКП-6)

Общекультурные, общепрофессиональные и профессиональные компетенции формируются, в основном, дисциплинами базовой части образовательной программы. Вариативная часть образовательной программы формирует, в основном, профессиональные компетенции профиля обучающихся (установлены Финансовым университетом совместно с работодателями) с учетом профиля программы бакалавриата и содержатся в общей характеристике образовательной программы, которая представлена отдельным документом.

2. ОПРЕДЕЛЕНИЕ ТЕМЫ ВКР

2.1. Примерный перечень тем ВКР, разработанный совместно с представителями организаций-работодателей, а также с учетом научных интересов кафедры «Информационная безопасность» ежегодно обновляется и размещается до 15 сентября на странице кафедры «Информационная безопасность» сайта Финуниверситета в разделе «бакалавриат → информация по ВКР».

2.2. Обучающийся обязан выбрать тему ВКР до 15 октября учебного года, завершающего обучение. Закрепление тем и руководителей ВКР за обучающимися (при необходимости консультантов) осуществляется приказом Финансового университета в установленном порядке не позднее 30 октября текущего учебного года. После выхода приказа о закреплении тем ВКР студенты и руководители ВКР обязаны в установленной кафедрой «Информационная безопасность» срок ознакомиться с приказом.

2.3. Изменение темы ВКР в исключительных случаях возможно не позднее, чем за 2 месяца, а уточнение темы – не позднее, чем за 1 месяц до предполагаемой даты защиты ВКР, на основании согласованного с руководителем ВКР личного заявления обучающегося, составленного на имя руководителя заведующего кафедрой, с обоснованием причины корректировки. Изменение или уточнение темы оформляется приказом Финансового университета.

3. РУКОВОДСТВО И КОНТРОЛЬ ПОДГОТОВКИ ВКР

3.1. В обязанности руководителя ВКР входит [3]:

* консультирование обучающегося в соответствии с графиком подготовки ВКР;
* разработка задания на ВКР;
* оказание помощи в подготовке плана ВКР;
* консультирование обучающегося в соответствии с графиком подготовки ВКР;
* консультирование обучающегося по подбору литературы 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 завершенной ВКР обучающимся на информационно-образовательном портале (далее – ИОП);
* информирование служебной запиской заведующего кафедрой, а также руководства факультета в случае несоблюдения обучающимся графика подготовки ВКР для применения мер воздействия, предусмотренных Правилами внутреннего трудового и внутреннего распорядка обучающихся, утвержденными приказом Финансового университета от 15.07.2013 № 1335/о;
* информирование служебной запиской заведующего кафедрой о неготовности ВКР, в том числе и к размещению на ИОП;
* консультирование обучающегося при подготовке презентации и доклада для защиты ВКР;
* представление письменного отзыва о работе обучающегося в период подготовки ВКР.
* в случае выполнения одной ВКР несколькими обучающимися руководитель ВКР составляет письменный отзыв об их совместной работе в период подготовки ВКР;
* размещение отзыва на ИОП;
* присутствие на защите ВКР, при условии его незанятости в аудиторной работе со студентами.

Формы задания на ВКР, плана и графика исполнения ВКР размещены на странице кафедры «Информационная безопасность» сайта Финуниверситета в разделе «бакалавриат → информация по ВКР». График, задание на ВКР, план ВКР оформляются в трех экземплярах, один хранится на кафедре (ком. 904), второй у руководителя ВКР, третий у студента.

3.2. Консультант обязан:

* оказывать консультационную помощь обучающемуся в выборе методики исследования, в подборе литературы и фактического материала в части содержания консультируемого вопроса; давать квалифицированные рекомендации в части содержания консультируемого вопроса;
* контролировать ход выполнения ВКР в части содержания консультируемого вопроса. [3]

3.3. Обучающийся обязан [3]:

* разработать и согласовать с руководителем план подготовки ВКР;
* систематически работать над ВКР в соответствии с установленными сроками и требованиями, использовать методические рекомендации кафедры «Информационная безопасность»;
* регулярно общаться с руководителем ВКР (и консультантом при наличии) и информировать его о проделанной работе;
* представить ВКР в установленные сроки.

3.4. Требования к отзыву руководителя ВКР представлены в [3].

4. СТРУКТУРА И СОДЕРЖАНИЕ ВКР

4.1. ВКР должна отвечать следующим требованиям:

* наличие в работе всех структурных элементов исследования: теоретической, аналитической и практической составляющих;
* использование в аналитической части исследования обоснованного комплекса методов, методик и средств обеспечения информационной безопасности, способствующих раскрытию сути проблемы;
* 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; оглавление; введение; основная часть, структурированная на главы и параграфы; заключение; список использованных источников; приложения. [3]

4.2.1. Введение содержит: актуальность выбранной темы; степень её разработанности; цель, задачи, объект и предмет исследования; круг рассматриваемых проблем и в сжатой форме все основные положения, обоснованию которых посвящена ВКР. Первичным является объект исследования (более широкое понятие), вторичным – предмет исследования, в котором выделяется определенная проблемная ситуация. Предмет исследования чаще всего совпадает с определением ее темы или очень близок к ней. Введение должно быть кратким (2 – 3 стр.). [3] К числу задач, решаемых в выпускной работе можно отнести:

* изучение предметной области и выявление недостатков существующей системы информационной безопасности, определяющих необходимость разработки данного проекта;
* разработку постановки задачи;
* обоснование выбора основных проектных решений в области защиты информации;
* разработку технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ России, ФСТЭК России, Центрального Банка России;
* обработка и анализ результатов экспериментальных исследований системы защиты информации;
* обоснование результативности/экономической эффективности проекта.

Во введении необходимо также перечислить вопросы, которые будут рассмотрены в проекте, выделив вопросы, которые предполагается решить практически. Рекомендуется писать введение по завершении основных глав работы, перед заключением. В этом случае исключена возможность несоответствия «желаемого» и «действительного». Введение кратко раскрывает план выполнения выпускной работы, то что обучающемуся необходимо сделать для решения выбранной задачи.

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

4.2.3. Первая глава содержит исторические, теоретические и методические аспекты исследуемой проблемы. В ней содержится обзор используемых источников информации по теме ВКР, описание объекта и предмета исследования, различные теоретические концепции, принятые понятия и их классификация, а также своя аргументированная позиция по данному вопросу. Сведения, содержащиеся в этой главе, должны давать полное представление о состоянии и степени изученности поставленной проблемы. Написание первой главы проводится на базе предварительно подобранных литературных источников, в которых освещаются вопросы, в той или иной степени раскрывающие тему ВКР. Особое внимание следует обратить на законодательную, нормативную и специальную документацию, посвященную вопросам, связанным с предметом и объектом исследования. Объем этой главы должен составлять 30 – 35 % от всего объема ВКР. Завершается первая глава обоснованием необходимости проведения аналитической части работы. Глава должна иметь название, отражающее суть изложенного в нем материала. Не допускается выносить в качестве названия этой главы заголовки «Теоретическая часть», «Обзор литературных источников» и т.д. [3]. Примерная структура первой главы:

Глава 1. Специфика предприятий кредитно-финансовой деятельности в части обеспечения информационной безопасности.

1.1 Организационное обеспечение информационной безопасности кредитно-финансовой организации.

1.2 Анализ киберпреступлений в кредитно-финансовой сфере.

* 1. Аудит информационной безопасности. Стандарты. Модели. Методы. Механизмы выявления аномалий в ДБО.
  2. Выводы.

4.2.4. 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 практики. В ней содержится:

* анализ конкретного материала по избранной теме (на примере конкретной подсистемы информационной безопасности, организации, отрасли, региона, страны) желательно за период не менее 2-х лет;
* сравнительный анализ с действующей практикой;
* анализ информационных ресурсов и актуальных для объекта уязвимостей, каналов утечки информации;
* разработка модели актуальных угроз и оценка рисков;
* анализ эффективности существующих на объекте системы защиты информации.

В ходе анализа используются аналитические таблицы, расчеты, формулы, схемы, диаграммы и графики. Объем второй главы должен составлять, как правило, 20 - 40 % от всего объема ВКР. [3]

Примерная структура второй главы:

Глава 2. Биометрические системы идентификации клиентов как перспективный способ противодействия мошенничеству

2.1 Анализ уязвимостей дистанционного банковского обслуживания

2.2 Анализ применения биометрических систем идентификации в системах ДБО как инструмента противодействия мошенничеству

2.3 Построение модели угроз для типовой биометрической системы идентификации клиента

2.4 Вывод по главе 2

4.2.5. 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. В данной главе должны быть сделаны самостоятельные выводы, разработаны методики или модели, представлены экономические расчеты. Объем третьей главы должен составлять, как правило, 15-25 % от всего объема ВКР. [3]

Примерная структура третьей главы:

Глава 3. Разработка решения по совершенствованию технологии надлежащей проверки клиентов

3.1 Разработка методики проведения надлежащей проверки клиентов

3.2 Перечень открытых информационных ресурсов способных помочь в сборе дополнительных сведений о клиентах

3.3 Разработка алгоритма методики надлежащей проверки клиентов

3.4 Оценка результативности предложенного решения

3.5 Выводы

После расчета срока окупаемости проекта, все показатели эффективности должны быть проиллюстрированы диаграммами (например, круговыми или столбчатыми).

4.2.6. В заключении, являющимся завершающей частью ВКР, рекомендуется определить, какие задачи были решены в ходе выполнения выпускной работы, определить пути внедрения и направления дальнейшего совершенствования разработанных решений по обеспечению информационной безопасности объекта; 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. [3]

4.2.7. Список использованных источников должен содержать сведения об источниках, которые использовались при подготовке ВКР (не менее 40) и располагаться в следующем порядке:

* законы Российской Федерации (в прямой хронологической последовательности);
* указы Президента Российской Федерации (в той же последовательности); постановления Правительства Российской Федерации (в той же очередности);
* нормативные акты, инструкции (в той же очередности); иные официальные материалы (резолюции-рекомендации международных организаций и конференций, официальные доклады, официальные отчеты, материалы судебной практики и др.);
* монографии, учебники, учебные пособия (в алфавитном порядке); авторефераты диссертаций (в алфавитном порядке); научные статьи (в алфавитном порядке);
* литература на иностранном языке (в алфавитном порядке); интернет-источники. [3]

4.2.8. 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. [3]. Приложения должны располагаться в логической последовательности появления ссылок на них из основной части ВКР. Каждое приложение должно обязательно иметь номер и название, 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.

4.3. ВКР должна быть распечатана и переплетена. Рекомендуемый объем составляет не менее 60 и не более 80 страниц без учета приложений (для коллективной ВКР 120 - 160 страниц без учета приложений).

5. ПОРЯДОК ПОДГОТОВКИ ВКР

5.1. Сроки составления плана и задания на ВКР, утверждения задания на ВКР в соответствии с приказом Финуниверситета «О проведении практики, подготовке ВКР» на текущий год, размещаются на странице кафедры в разделе «бакалавриат → информация по ВКР» до 15 сентября текущего учебного года.

5.2. Сроки предоставления каждой главы ВКР, в соответствии с приказом Финуниверситета «О проведении практики, подготовке ВКР» на текущий год, размещаются на странице кафедры в разделе «бакалавриат → информация по ВКР» до 15 сентября текущего учебного года.

5.3. Руководитель ВКР в обязательном порядке проверяет ВКР в системе «Антиплагиат. ВУЗ». В случае выявления заимствований в объеме более 15% руководитель ВКР проводит анализ текста на соблюдение норм правомерного заимствования и принимает решение о правомерности использования заимствованного текста в ВКР. Экспертная оценка уровня авторского текста в ВКР отражается в отзыве руководителя ВКР. В случае выявления факта неправомерного заимствования при подготовке ВКР работа возвращается руководителем ВКР обучающемуся на доработку. [3]

5.4. Обучающийся обязан разместить с разрешения руководителя законченную и оформленную в соответствии с методическими рекомендациями кафедры «Информационная безопасность» ВКР в электронном виде (далее – ЭВКР) на ИОП не позднее 10-ти календарных дней до начала ГИА согласно календарному графику, ежегодно утверждаемому приказом об организации учебного процесса. ВКР в распечатанном и переплетенном виде, соответствующем электронной версии, размещенной на ИОП, подписывается обучающимся, руководителем ВКР, консультантом (при наличии) и представляется обучающимся вместе с письменным разрешением обучающегося на размещение ВКР на ИОП, отзывом руководителя ВКР и отчетом о проверке на заимствования по системе «Антиплагиат. ВУЗ»на кафедру не позднее 5-ти календарных дней до даты защиты ВКР [3]. Алгоритм размещения ВКР на ИОП описан в Регламенте размещения на информационно-образовательном портале Финансового университета курсовых работ (проектов) и выпускных квалификационных работ, порядок хранения и списания, утверждённом приказом Финуниверситета от 12.11.2015 №2372/о.

5.5. 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 – программе бакалавриата, успешно сдавшие государственный экзамен или отсутствовавшие на государственном экзамене по уважительной причине [3].

6. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ВКР

6.1. ВКР оформляется в соответствии с ГОСТ Р 7.0.5-2008 (Библиографическая ссылка); ГОСТ 7.1-2003 (Библиографическая запись. Библиографическое описание. Общие требования и правила составления); ГОСТ 7.82-2001 Библиографическая запись. Библиографическое описание электронных ресурсов; ГОСТ 7.012-2011 Библиографическая запись. Сокращение слов на русском языке. Общие требования и правила.

6.2. К защите принимаются только сброшюрованные ВКР. ВКР оформляется с использованием компьютера. Работа должна быть напечатана на стандартных листах бумаги формата А4 белого цвета, на одной стороне (без оборота), через полтора межстрочных интервала. Шрифт выбирается Times New Roman, чёрного цвета, размер 14, без применения полужирного начертания.

6.3. Текст ВКР следует печатать, соблюдая следующие размеры полей: правое - не менее 10 мм, верхнее и нижнее - не менее 20 мм, левое - не менее 30 мм.

6.4. ВКР состоит из следующих структурных элементов: ведение, заключение, список использованных источников, приложение. Слова «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ», «ПРИЛОЖЕНИЕ» являются заголовками структурных элементов работы. Заголовки структурных элементов следует располагать по середине текстового поля и печатать прописными буквами без кавычек, без подчеркивания и без проставления точки в конце заголовка.

6.5. Главы ВКР должны быть пронумерованы арабскими цифрами в пределах всей работы и записываться с абзацного отступа. После цифры ставится точка и пишется название главы, прописными буквами или начиная с прописной буквы. Введение и заключение как главы не нумеруются.

6.6. Параграфы следует нумеровать арабскими цифрами в пределах каждой главы. Номер параграфа должен состоять из номера главы и номера параграфа, разделенных точкой. Заголовки параграфов печатаются строчными буквами, начиная с прописной.

6.7. Для сносок шрифт выбирается Times New Roman, черного цвета, размер № 12, через одинарный интервал. Сноски следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту.

6.8. Графики, схемы, диаграммы располагаются в ВКР непосредственно после текста, имеющего на них ссылку, и выравниваются по центру страницы. Название графиков, схем, диаграмм помещается под ними, пишется без кавычек и содержит слово «Рисунок» без кавычек и указание на порядковый номер рисунка, без знака №. Например: Рисунок 1 - Название рисунка.

6.9. Таблицы в ВКР располагаются непосредственно после текста, имеющего на них ссылку (выравнивание по центру страницы). Таблицы нумеруются арабскими цифрами сквозной нумерацией в пределах всей работы (Таблица 1- Название).

6.10. Приложения должны начинаться с новой страницы, располагаться и нумероваться в порядке появления ссылок на них в тексте. Приложения должны иметь заголовок с указанием слова «Приложение», его обозначения и названия.

6.11. Страницы ВКР следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту. Номер страницы проставляют, начиная со второй, по середине нижнего поля листа. Титульный лист включается в общую нумерацию страниц отчета, но номер страницы на титульном листе не проставляется. Каждую главу работы следует начинать печатать с новой страницы. Параграфы на составные части не подразделяются. Приложения не входят в установленный объем выпускной квалификационной работы, при этом нумерация страниц их охватывает.

6.12. Законченная работа подписывается студентом: на титульном листе; после заключения записывается следующее:

«Данная работа выполнена мною самостоятельно» «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (дата сдачи работы – заполняется от руки) (подпись автора)»

ВКР представляется на кафедру в печатном виде в твердом переплете, а также размещается в электронном виде на информационно-образовательном портале Финуниверситета. [3]

7. ПРАВИЛА ПОДГОТОВКИ К ЗАЩИТЕ ВКР

7.1. Требования к содержанию и продолжительности доклада по ВКР.

Цель доклада и презентации: довести до членов Государственной Аттестационной Комиссии в краткой форме смысл и результаты выполненной работы. Доклад строится в форме отчета о проделанной работе от третьего лица (было сделано, построено, получено, достигнуто). В докладе должно быть четко определено:

* что сделано в главе, в параграфе, в целом в работе;
* с помощью чего, как это сделано (какие использовались методы анализа, классификации, статистика, модели, алгоритмы);
* зачем это сделано (в целях повышения защиты информации в электронном банкинге);
* что на основании сделанного будет сделано далее, в какой степени и как это повлияет на обеспечение информационной безопасности в банковской сфере.

Рекомендуется употреблять следующие обороты:

1. В первом параграфе работы была проведена классификация и анализ нормативно-правовых документов, который позволил сделать вывод, что в области проведения аудита информационной безопасности в банковской сфере неопределенны следующие аспекты…

2. Далее в работе была построена модель …

3. Во второй главе работы проведен анализ объекта информатизации КФС, который позволил выявить…

4. В заключении следует отметить, что построенная модель позволила…

В начале доклада следует представиться комиссии сообщить тему своего доклада, и данные научного руководителя, например: «Уважаемые члены Государственной Аттестационной Комиссии Вашему вниманию представляется выпускная квалификационная работа студента Иванова Петра Васильевича на тему: «Применение облачных хранилищ персональных данных в целях повышения уровня информационной безопасности в банковской сфере», выполненная на кафедре «Информационная безопасность». Научный руководитель: профессор кафедры, доктор технических наук Козьминых Сергей Игоревич.

7.2. Требования к презентации ВКР. Доклад должен сопровождаться презентацией, иллюстрирующей основные положения работы с использованием мультимедийных средств, выполненной в программе PowerPoint с использованием шаблона презентации, размещенного на главной странице сайта Финуниверситета, вкладка «размещение презентаций». Количество слайдов – 12-18 с учетом трех слайдов, отводимых на титульный лист, введение и заключение.

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



Следующий слайд обычно посвящен актуальности темы исследования, проблеме, в решение которой вы планируете внести свой вклад. Далее обозначают цель работы, объект и предмет исследования. Объект исследования – эта та часть проблемы, которую вы хотите исследовать, предмет – это метод, которым вы будете решать свою часть проблемы.

Далее вы должны обозначить задачи, которые поставлены и решены в работе (задачи должны соответствовать содержанию работы). Для бакалавров 3-4 задачи. Для бакалавров достаточно обозначить к чему приведет решение поставленных задач. Например: значительно повысит уровень информационной безопасности при хранении персональных данных на объекте защиты.

Основное время доклада должно быть отведено методу решения той части проблемы, за которую вы взялись. На то, что лично вами сделано в работе, и к каким результатам это привело.

В ходе доклада вы должны показать свою компетентность в той области исследования, которую выбрали. Для этого в докладе и в презентации вы должны показать, что свободно владеете математическим аппаратом для проведения исследования, различными методами моделирования, обработки статистики, методами построения алгоритмов и программированием. Для этого на слайдах должны быть математические выкладки, графики, алгоритмы, модели, которые вы использовали в ходе своей работы.

На последнем слайде должны быть представлены выводы по работе. В выводах очень кратко отражается, что главное сделано в работе, какой результат достигнут, в чем заключается самостоятельная часть работы и к каким результатам приведет внедрение ваших исследований на объекте информатизации кредитно-финансовой сферы.

Например:

«В заключении следует отметить, что в результате построения трехмерной модели и расчета коэффициента защищенности появляется возможность оценки существующего уровня защиты информации на объекте КФС. Кроме того, появляется возможность оптимизации выбора комплекса технических средств и методов защиты информации.

Таким образом, можно сделать вывод, что разработанный метод математического моделирования позволяет не только оценить текущий уровень информационной безопасности в любой организации кредитно-финансовой сферы, но и создавать эффективные системы защиты информации, а также оптимизировать затраты на их создание».

Количество слайдов определяется объемом работы, количеством необходимой для доклада информации, а главное временем, которое дается на доклад.

Слайды должны быть сформированы так, чтобы они хорошо читались на расстоянии членами комиссии, находящимися в аудитории. Для этого, как правило, все надписи и рисунки должны быть выполнены темным цветом на светлом фоне, быть крупными и разборчивыми, занимать все пространство слайда. Слайды лучше оформлять в строгом стиле, чтобы не вызывать критику членов комиссии.

Слайд презентации должен состоять из двух частей – заголовка и содержательной части. Заголовок слайда располагается в верхней части, пишется крупными буквами и должен как можно более подробно обозначать, что изображено на слайде.

В левом верхнем углу должен быть номер слайда, хорошо видный издалека, чтобы члены комиссии могли его рассмотреть и после доклада к нему вернуться.

Содержание слайда должно быть максимально информативно и понятно, для того, чтобы сократить текст доклада.

Например:



Пояснения на слайде должны быть краткими, но емкими, это также позволяет сократить текст доклада.

При расположении на слайде математических формул необходимо их нумеровать справа в круглых скобках. Формулы должны быть выполнены в соответствии с требованиями, хорошо читаться, иметь правильные математические знаки и соответствовать правилам математики. На этом же слайде необходимо представить расшифровку, составляющих формулы. Заголовок слайда должен подробно отражать, что это за формула и к чему она относится.

При расположении на слайдах скриншотов программных закладок желательно чтобы все, что на нем изображено было в хорошем качестве и хорошо читалось членами комиссии. Заголовок слайда должен четко отражать, что показано на слайде. Не увлекайтесь большим количеством таких слайдов, это утомляет комиссию и затягивает доклад. Покажите только те скриншоты, которые отражают суть работы.

При расположении на сладах алгоритмов и функциональных схем, не забывайте об обратных связях, вариантах исхода событий, которые должны быть обозначены красивыми стрелками.

При размещении на слайде статистических данных, не забывайте указывать какие значения статистики на графиках, каким показателям соответствуют, так чтобы это было видно и понятно.

**Не рекомендуется:**

1. Располагать на слайде большое количество текста и тем более читать его со слайда. Это производит очень плохое впечатление. Информацию лучше представлять в формализованном виде. В виде функциональных схем, алгоритмов, графиков, моделей с пояснениями.

2. Не рекомендуется загромождать слайды большим количеством таблиц. Если вы хотите представить на слайде модель или расчет, выполненный в виде таблиц, то совсем не обязательно приводить всю таблицу, которая как правило, не помешается на слайде, можете привести главную часть таблицы, обозначить разрыв волнистой линией и далее показать ее результаты. Дать пояснение в докладе.

3. Не рекомендуется представлять на слайдах абстрактные (креативные) картинки, на которых не понятно, что из чего вытекает, что за чем следует, какие связи и что связывают. Это вызывает лишние вопросы.

4. Не рекомендуется размещать на слайде для украшения ненужные картинки, злоупотреблять анимацией при показе слайдов, это приводит к задержке времени доклада.

7.3. Процедура защиты ВКР включает в себя:

* открытие заседания ГЭК (председатель);
* доклады обучающихся (предусматривается не более 10 минут на доклад обучающегося);
* вопросы членов комиссии по ВКР и докладу обучающегося (при ответах на вопросы обучающийся имеет право пользоваться своей работой);
* выступление руководителя ВКР либо, в случае его отсутствия, заслушивание текста отзыва [3].

Практика показывает, что доклад на 10 минут должен быть не более 7 страниц текста 14 кегелем единичным интервалом.

7.4. 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, ответы на вопросы членов ГЭК. В случае возникновения спорной ситуации при равном числе голосов председательствующий обладает правом решающего голоса. [3]

7.5. Порядок повторной защиты ВКР, определенный пунктом 5.4 Порядка проведения государственной итоговой аттестации по программам бакалавриата и магистратуры в Финансовом университете, утвержденного приказом Финуниверситета от 14.10 2016 № 1988/о. [3]

7.6. 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 рейса, отсутствие билетов, погодные условия), вправе пройти ее в течение 6-ти месяцев после завершения ГИА. Обучающийся должен в течение 7-ми календарных дней после установленной даты защиты ВКР представить документ, подтверждающий причину его отсутствия. [3]

7.7. 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. [3]

8. КРИТЕРИИ ОЦЕНКИ ВКР

При формировании критериев оценки следует использовать перечень знаний, умений, владений, которые выпускник должен продемонстрировать для подтверждения освоенных программ бакалавриата.

«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.

Приложение № 1

к Положению

**Форма заявления о закреплении темы ВКР**

|  |  |
| --- | --- |
| ФИНУНИВЕРСИТЕТ | Руководителю департамента/ заведующему кафедрой |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (наименование департамента/кафедры) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (И.О. Фамилия, уч. степень, уч.звание) |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Фамилия И.О. обучающегося) |
| **СОГЛАСЕН** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | (наименование факультета) |
| \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (дата) (подпись) | (№ учебной группы) |
|  | Тел. обучающегося\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  E-mail обучающегося\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |

**ЗАЯВЛЕНИЕ**

Прошу закрепить за мной тему ВКР «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_».

« » 20\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись обучающегося)

Согласовано:

Руководитель ВКР

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (И.О. Фамилия)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Руководитель департамента/

Руководитель департамента/

заведующий кафедрой

\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

(подпись)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 г. Приложение № 2

к Положению

Ф**орма задания на ВКР**

УТВЕРЖДАЮ

Руководитель выпускной квалификационной работы

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (И.О. Фамилия)

« » \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

|  |  |
| --- | --- |
| Руководитель департамента/ кафедры |  |
|  | |

|  |
| --- |
| ФИНУНИВЕРСИТЕТ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (наименование департамента/кафедры) |

**ЗАДАНИЕ**

**на выпускную квалификационную работу**

обучающемуся\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество )

Тема выпускной квалификационной работы «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

закреплена приказом Финуниверситета от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_

Целевая установка: разработка предложений по использованию результатов работы[[1]](#footnote-1) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Основные вопросы, подлежащие разработке (исследованию):

1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Основная литература указывается в Приложении к заданию*

Дата выдачи задания «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Задание получил:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, Фамилия И.О. обучающегося)

Приложение № 3

к Положению

**Форма отзыва руководителя о работе обучающегося в период подготовки ВКР**

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 бакалавриата**

Обучающийся\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (фамилия, имя, отчество)

Факультет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_

Департамент/кафедра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Направление подготовки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Профиль\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование темы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (имя, отчество, фамилия, должность, ученое звание, ученая степень)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Соответствие заявленных целей и задач теме ВКР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Соответствие полученных результатов заявленным целям и задачам:\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Умение проводить исследование в профессиональной деятельности (умение анализировать, владеть методами исследования и представления результатов):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Характеристика использования в работе инструментария математики, математического моделирования, расчетов, статистических методов, пакетов специальных прикладных программ и т.п.:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_5. Наличие конкретных предложений и рекомендаций, сформулированных в ВКР, ценность полученных результатов:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Степень самостоятельности при работе над ВКР (самостоятельность изложения и обобщения материала, самостоятельная интерпретация полученных результатов, обоснованность выводов):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Сформированность компетенций в ходе работы над ВКР: компетенции, предусмотренные Программой государственной итоговой аттестации и подлежащие оценке в ходе выполнения ВКР, сформированы (не сформированы):\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Доля (%) заимствований в ВКР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. Недостатки в работе обучающегося в период подготовки ВКР: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. ВКР соответствует (не соответствует) требованиям, предъявляемым к ВКР, и может (не может) быть рекомендована к защите на заседании ГЭК:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
|  |
| (И.О.Фамилия руководителя) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись руководителя)

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение № 7

к Положению

**Форма отзыва руководителя о совместной работе обучающихся в период подготовки коллективной ВКР**

Федеральное государственное образовательное бюджетное

учреждение высшего образования

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

**(Финансовый университет)**

**ОТЗЫВ РУКОВОДИТЕЛЯ**

**о совместной работе обучающихся в период подготовки коллективной выпускной квалификационной работы по программе бакалавриата[[2]](#footnote-2)**

Коллектив обучающихся:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

Факультет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_

Департамент/кафедра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Направление подготовки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Профиль\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование темы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (имя, отчество, фамилия, должность, ученое звание, ученая степень)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Соответствие заявленных целей и задач теме ВКР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Соответствие полученных результатов заявленным целям и задачам:\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Умение проводить исследование в профессиональной деятельности (умение анализировать, владеть методами исследования и представления результатов):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Характеристика использования в работе инструментария математики, математического моделирования, расчетов, статистических методов, пакетов специальных прикладных программ и т.п.:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_5. Наличие конкретных предложений и рекомендаций, сформулированных в ВКР, ценность полученных результатов:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Степень самостоятельности при работе над ВКР (самостоятельность изложения и обобщения материала, самостоятельная интерпретация полученных результатов, обоснованность выводов):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Сформированность компетенций в ходе работы над ВКР: компетенции, предусмотренные Программой государственной итоговой аттестации и подлежащие оценке в ходе выполнения ВКР, сформированы (не сформированы):\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Доля (%) заимствований в ВКР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. Недостатки в работе обучающегося в период подготовки ВКР: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. ВКР соответствует (не соответствует) требованиям, предъявляемым к ВКР, и может (не может) быть рекомендована к защите на заседании ГЭК:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
|  |
| (И.О. Фамилия руководителя) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись руководителя)

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

1. Руководитель ВКР конкретизирует целевую установку ВКР, исходя из темы ВКР [↑](#footnote-ref-1)
2. В пунктах 3-7 и 9 необходимо оценить каждого обучающегося индивидуально [↑](#footnote-ref-2)