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
10.04.01 «Информационная безопасность»,
направленность программы магистратуры -
«Информационная безопасность финансово-кредитных организаций»

Одобрено заседанием кафедры «Информационная безопасность»

протокол №5 от 25 ноября 2019г.

Москва 2019

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

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

методов, технических и программных средств обработки результатов эксперимента (ПК-7)	Защита ВКР
способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)	Защита ВКР
способность проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9)	Государственный экзамен Защита ВКР
способность проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10)	Государственный экзамен Защита ВКР
способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности (ПК-11)	Защита ВКР
способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)	Защита ВКР
способностью организовать управление информационной безопасностью (ПК-13)	Государственный экзамен Защита ВКР
способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)	Защита ВКР
способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15).	Государственный экзамен Защита ВКР
способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации па системы и средства обеспечения информационной безопасности (ПК-16)	Государственный экзамен Защита ВКР
способность разрабатывать модели угроз и оценивать возможности внешних и внутренних нарушителей безопасности автоматизированной системы финансово-кредитной организации (ДКН-1) 2019	Государственный экзамен Защита ВКР
способность применять математические модели, методы и алгоритмы решения типовых задач анализа информации в информационно-аналитических системах безопасности предприятий финансово-кредитной сферы, создавая соответствующее программное и математическое обеспечение, основанное на криптографических методах, алгоритмах, протоколах используемых для защиты информации в автоматизированных системах (ДКН- 1) 2018	Защита ВКР
способность применять математические модели, методы и алгоритмы решения типовых задач анализа информации в информационно-аналитических системах безопасности предприятий финансово-кредитной сферы, создавая соответствующее программное и математическое обеспечение (ДКМП-1) 2017	Защита ВКР

способность классифицировать и оценивать угрозы информационной безопасности для объекта информатизации предприятий финансово-кредитной сферы (ДКН-2) 2019, 2018, (ДКМП-2) 2017	Государственный экзамен Защита ВКР
способность осуществлять меры противодействия нарушениям сетей безопасности предприятий финансово-кредитной сферы с использованием различных программных и аппаратных средств защиты и принимать меры защиты информации при выявлении новых угроз безопасности информации (ДКН-3) 2019, 2018	Государственный экзамен Защита ВКР
способность осуществлять меры противодействия нарушениям сетей безопасности предприятий финансово-кредитной сферы с использованием различных программных и аппаратных средств защиты (ДКМП-3) 2017	Защита ВКР
способность формирования политик информационной безопасности организации предприятий финансово-кредитной сферы, с учетом порядка аттестации компьютерных систем на предмет их соответствия требованиям по информационной безопасности и выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний (ДКН-4) 2019, 2018	Государственный экзамен Защита ВКР
способность формирования политик информационной безопасности организации предприятий финансово-кредитной сферы, с учетом порядка аттестации компьютерных систем на предмет их соответствия требованиям по информационной безопасности (ДКМП-4) 2017	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

11.12. 2019 г.

Дворянкин С.В.

Программа государственного экзамена

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

Рекомендовано Ученым советом Факультета прикладной математики и информационных технологий
протокол №20 от 09 декабря 2019 г.

Одобрено кафедрой «Информационная безопасность»
протокол №5 от 25 ноября 2019 г.

Москва 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

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

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

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

1.1 Вопросы на основе содержания общепрофессиональных и профессиональных дисциплин направления подготовки

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

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

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

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

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

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

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

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

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

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

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

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

24. Содержание процессного подхода к управлению ИБ.

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

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

27. Дискретно-событийное моделирования для учета риска.

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

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

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

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

а) основная литература:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш . - Москва: РИОР, 2014. - 256 с. - Текст : непосредственный. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/1009606 (дата обращения: 30.01.2020). - Текст : электронный. *Может быть рекомендовано бакалаврам и магистрам.

2. Понятийный аппарат информационной безопасности финансово-экономических систем = The conceptual apparatus of the information security of financial and economic systems: Энциклопедический словарь / Финуниверситет, Каф. "Информационная безопасность" ; авт.-сост.: Г.О. Крылов, В.Л. Никитина. - Москва: Финуниверситет, 2016. - 255 с. – Текст : непосредственный. - То же. - ЭБ

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

б) дополнительная:

1. Башлы, П.Н. Информационная безопасность и защита информации: учебник/ П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва: РИОР, 2013. — 222 с. — ЭБС ZNANIUM.com. — URL: https://new.znanium.com/catalog/product/405000 (дата обращения: 30.01.2020). — Текст: электронный.
2. Гришина, Н. В. Основы информационной безопасности предприятия: учебное пособие / Н. В. Гришина. — Москва: ФОРУМ, 2019. – 216 с. – (Высшее образование: Бакалавриат). — ЭБС ZNANIUM.com. – URL: https://new.znanium.com/catalog/product/1017663 (дата обращения: 30.01.2020). - Текст : электронный.
3. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – Москва: Гор. линия – Телеком, 2013. – 220 с. - ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/421968 (дата обращения: 30.01.2020). - Текст : электронный.
4. Рассолов, И.М. Информационное право: учебник для магистров, обуч. по юридич. напр. и спец. / И.М. Рассолов. - Москва: Юрайт, 2015. - 448 с. – Текст : непосредственный. Рассолов, И. М. Информационное право : учебник и практикум / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 347 с. — (Бакалавр. Специалист. Магистр). — ЭБС Юрайт. — URL: https://www.biblio-online.ru/bcode/431833 (дата обращения: 30.01.2020). - Текст : электронный.

в) нормативно-правовые акты

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

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

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

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

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

8. Приказ ФСТЭК № 21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

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

10. Приказ Гостехкомиссии России N 187, 2002г. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1,2,3. Руководящий документ.

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

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

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

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

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

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

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

18. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

19. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.

20. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

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

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

г) ресурсы информационно-телекоммуникационной сети «Интернет»

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

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

27. Российская научная библиотека www.rsl.ru.

28. Код безопасности - www.securitycode.ru.

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

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

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

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

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

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

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

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

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

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

1.3 Вопросы на основе содержания дисциплин направленности программы магистратуры

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

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

15. Риск-ориентированный подход к обеспечению информационной безопасности.

16. Технологические меры защиты информации

17. Защита персональных данных.

18. Организационные меры защиты информации

19. Построение модели нарушителя

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

21. Федеральный закон «О государственной тайне».

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

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

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

25. Методы и модели разграничения доступа.

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

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

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

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

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

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

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

33. Основные способы заражения персонального компьютера вредоносным программным обеспечением.

34. Основные способы использования зараженного компьютера.

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

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

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

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

а) основная литература

1. Генкин, А. Блокчейн: Как это работает и что ждет нас завтра / А. Генкин, А. Михеев. — Москва: Альпина Паблишер, 2018. — 592 с. - ЭБС ZNANIUM.com. - URL: https://new.znanium.com/catalog/product/1002003 (дата обращения: 30.01.2020). - Текст: электронный.

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

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

б) дополнительная

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

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

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

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

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

9. Дербин, Е.А. Организационные основы обеспечения информационной безопасности предприятия: учебное пособие / Е.А. Дербин, С.М. Климов;

Финуниверситет, Каф. "Информационная безопасность" — Москва: Финуниверситет, 2013. — Информационно-образовательный портал Финуниверситета.—URL: http://http://portal.ufrf.ru/Content/Data/bfe5ac2d-d57d-4f4a-9929-3d440cab52cb/Elektr_uch._posobie_OOIB1.pdf (дата обращения: 30.01.2020) — Текст : электронный.

10. Муссель, К.М. Платежные технологии: системы и инструменты / К.М. Муссель. – Москва : КНОРУС : ЦИПСиР, 2015. – 288 с.– ЭБС Университетская библиотека online. – URL: http://biblioclub.ru/index.php?page=book&id=441393 (дата обращения: 30.01.2020). – Текст : электронный.

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

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

в) нормативно-правовые акты

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

2. Информация Банка России от 27.01.2014 "Об использовании при совершении сделок "виртуальных валют", в частности, Биткойн" Письмо ФНС России от 03.10.2016 № ОА-18-17/1027 [Электронный ресурс] // URL: http://www.finanz.ru/novosti/aktsii/minekonomrazvitiya-predlozhilorazrabatyvatzakony-o-kriptovalyute-na-osnove-opyta-pravovykh-pesochnic1003537455

3. Федеральный закон: Выпуск 12(520). О национальной платежной системе. — Москва: ИНФРА-М, 2011. — 55 с. — Режим доступа: http://znanium.com/catalog.php?bookinfo=237826

4. СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств».

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

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

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

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

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

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

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

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

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

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

15. ГОСТ Р 56045-2014 Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.

16. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

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

18. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

19. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

20. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

21. ГОСТ Р ИСО/МЭК ТО 15446-2008 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

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

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

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

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

26. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

27. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

28. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.

29. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

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

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

32. ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

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

34. ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

35. 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.

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

г) ресурсы информационно-телекоммуникационной сети «Интернет»

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

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

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

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

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

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

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

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

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

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

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

48. Российская научная библиотека www.rsl.ru.

49. Код безопасности - www.securitycode.ru.

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

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

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

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

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

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

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

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

2 Примеры практико-ориентированных заданий

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22. Во время посещения отдела кадров на столе была обнаружена точка доступа. Сотрудник объяснил, что точка доступа приобретена для личных целей как

обеспечение соединения ноутбука с сетью для посещения web-сайтов и просмотра фильмов online в обеденное время. Задание: Укажите на нарушения, присвойте им степень, спланируйте меры устранения этих нарушений. В какие сроки и почему по данному инциденту будет установлена плановая или внеплановая проверка.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

38. Вы – руководитель отдела исследований и разработок в ПАО «Банк Уралсиб». Задание: Сформировать требования к составу ресурсов доступа (баз

данных, сетевых файловых ресурсов, виртуальных машин, ресурсов доступа, расположенных на серверах электронной почты, ресурсов доступа, расположенных на WEB-серверах информационно-телекоммуникационной сети Интранет, ресурсов доступа, расположенных на WEB-серверах информационно-телекоммуникационной сети Интернет), в соответствии с ГОСТ 34.601-90

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

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

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

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

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

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

3 Рекомендации обучающимся по подготовке к государственному экзамену

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

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

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

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

4 Критерии оценки результатов сдачи государственных экзаменов

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

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

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

Оценка «неудовлетворительно» (2 балла) выставляется в случае, если материал излагается непоследовательно, не аргументировано, бессистемно, ответы на вопросы выявили несоответствие уровня знаний выпускника требованиям ФГОС ВО 3+ в части формируемых компетенций, а также дополнительным компетенциям, установленным вузом.

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

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

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

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

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

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

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

Федеральное государственное образовательное бюджетное учреждение высшего образования

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

Кафедра «Информационная безопасность»

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

Москва 2019

Федеральное государственное образовательное бюджетное
учреждение высшего образования

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

Кафедра «Информационная безопасность»

Дворянкин С.В., Коннова И.Г.

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

Одобрено заседанием кафедры «Информационная безопасность»
Протокол от 26.09.2019 №3

Москва 2019

УДК 004.056
ББК 74.58В-

Методические рекомендации по подготовке и защите выпускной квалификационной работы по программе магистратуры направления подготовки 10.04.01 «Информационная безопасность», «Информационная безопасность финансово-кредитных организаций».
Составители: – Дворянкин С.В., Коннова И.Г. - М.: Финансовый университет, 2020 – 34с.

Учебное пособие
Дворянкин С.В.
Коннова И.Г.

Методические рекомендации по подготовке и защите выпускной квалификационной работы по программе магистратуры направления подготовки 10.04.01 «Информационная безопасность», «Информационная безопасность финансово-кредитных организаций».
Размещение на портале одобрено на заседании кафедры «Информационная безопасность», протокол от 26.09.2019 №3

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

Отпечатано в Финансовом университете

СОДЕРЖАНИЕ

1 Общие положения

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

– способность разрабатывать модели угроз и оценивать возможности внешних и внутренних нарушителей безопасности автоматизированной системы финансово-кредитной организации (ДКН-1) 2019;

– способность применять математические модели, методы и алгоритмы решения типовых задач анализа информации в информационно-аналитических системах безопасности предприятий финансово-кредитной сферы, создавая соответствующее программное и математическое обеспечение, основанное на криптографических методах, алгоритмах, протоколах, используемых для защиты информации в автоматизированных системах (ДКН- 1) 2018;

– способность применять математические модели, методы и алгоритмы решения типовых задач анализа информации в информационно-аналитических системах безопасности предприятий финансово-кредитной сферы, создавая соответствующее программное и математическое обеспечение (ДКМП-1) 2017;

– способность классифицировать и оценивать угрозы информационной безопасности для объекта информатизации предприятий финансово-кредитной сферы (ДКН-2) 2019, 2018, (ДКМП-2) 2017;

– способность осуществлять меры противодействия нарушениям сетей безопасности предприятий финансово-кредитной сферы с использованием различных программных и аппаратных средств защиты и принимать меры защиты информации при выявлении новых угроз безопасности информации (ДКН-3) 2019, 2018;

– способность осуществлять меры противодействия нарушениям сетей безопасности предприятий финансово-кредитной сферы с использованием различных программных и аппаратных средств защиты (ДКМП-3) 2017;

– способность формирования политик информационной безопасности организации предприятий финансово-кредитной сферы, с учетом порядка аттестации компьютерных систем на предмет их соответствия требованиям по информационной безопасности и выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний (ДКН-4) 2019, 2018;

– способность формирования политик информационной безопасности организации предприятий финансово-кредитной сферы, с учетом порядка аттестации компьютерных систем на предмет их соответствия требованиям по информационной безопасности (ДКМП-4) 2017. [1,2]

2 Определение темы выпускной квалификационной работы

2.1 Примерный перечень тем ВКР с контактами (ФИО, электронная почта) предполагаемых научных руководителей (далее руководитель ВКР), разрабатывается совместно с представителями организаций – работодателей с учетом научных интересов кафедры «Информационная безопасность», ежегодно формируется руководителем образовательной программы магистратуры до 15 мая и утверждается на заседании кафедры до 30 июня т.г. с последующим размещением на WEB-странице кафедры «Информационная безопасность» сайта Финуниверситета в разделе «магистратура → информация по ВКР». [3]

2.2 Обучающийся первого курса магистратуры должен или выбрать тему ВКР из размещенного на портале перечня тем ВКР, или сформулировать её самостоятельно, с последующим согласованием с предполагаемым руководителем ВКР, в срок не позднее 30 октября т.г., путем подачи письменного заявления о закреплении темы ВКР на имя руководителя образовательной программы магистратуры по соответствующей форме приложения А [4].

Закрепление тем и руководителей ВКР осуществляется приказом Финансового университета в установленном порядке не позднее 10 декабря т.г.

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

3 Руководство и контроль подготовки выпускной квалификационной работы

Руководство и контроль за ходом подготовки выпускной квалификационной работы обучаемым осуществляются руководителем ВКР, руководством кафедры «Информационная безопасность», консультантом с другой кафедры при необходимости.

3.1 В обязанности руководителя ВКР входит [4]:

– консультирование обучающегося в соответствии с графиком подготовки ВКР;

– выдача задания на подготовку ВКР по форме согласно приложению Б не позднее одного месяца с даты издания приказа о закреплении тем и руководителей ВКР за обучающимися;

– консультирование обучающегося по подготовке в соответствии с выданным заданием выполнения ВКР, подбору источников и информационных баз данных, выбору теоретического и практического материала, методики исследования;

– оказание помощи при составлении и заполнении индивидуального плана (ИПР) обучающегося на информационно-образовательном портале (ИОП), контроль выполнения пунктов заданий ИПР и проставление баллов за их выполнение на ИОП;

– мотивация обучаемого к участию в научных конференциях, семинарах и других научных мероприятиях;

– 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 № 1335/о от 15.07.2013;

– осуществление постоянного контроля за ходом подготовки ВКР в соответствии с ИПР обучающихся;

– принятие решения о готовности ВКР и размещения её обучающимся на ИОП;

– информирование служебной запиской заведующего кафедрой о неготовности ВКР, в том числе и к размещению на ИОП;

– представление письменного отзыва о работе обучающегося в период подготовки ВКР по форме согласно приложению В (в случае выполнения одной ВКР несколькими обучающимися руководитель ВКР составляет письменный отзыв об их совместной работе в период подготовки ВКР);

– размещение отзыва на ИОП;

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

– присутствие на защите ВКР, при условии его незанятости в аудиторной работе со студентами.

Формы задания на ВКР и оформления ВКР размещены на странице кафедры «Информационная безопасность» сайта Финуниверситета в разделе «магистратура → информация по ВКР». Задание на ВКР оформляется в трех экземплярах: один хранится на кафедре (ком. 904), второй у руководителя ВКР, третий у студента.

3.2 При необходимости, по ходатайству руководителя ВКР, заведующий кафедрой может привлекать для консультирования обучающихся консультантов из числа научно-педагогических работников другого департамента/кафедры Финансового университета по согласованию с руководителем соответствующего департамента/заведующим соответствующей кафедры.

Консультант может:

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

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

3.3 В процессе выполнения ВКР обучающийся обязан [4]:

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

— своевременно заполнять и вести ИПР в личном кабинете на ИОП;

— систематически работать над ВКР в соответствии с установленными кафедрой и руководителем 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 изложены в приложении В данных методических рекомендаций.

4 Структура и содержание выпускной квалификационной работы

4.1 Руководитель ВКР совместно с обучающимся первого курса магистратуры определяют перечень исходных данных, включая статистические и библиографические источники, обязательных к изучению при подготовке ВКР.

4.2 ВКР должна отвечать следующим требованиям:

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

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

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

— достаточность и современность использованного библиографического материала.

4.3 ВКР должна включать следующие разделы: титульный лист (по форме согласно приложению Г); оглавление; введение; основная часть, структурированная

на главы и параграфы; заключение; список использованных источников; приложения. [4]

4.3.1 Во введении раскрывается актуальность выбранной темы, степень ее научной разработанности, очерчивается круг найденных научных противоречий (проблемных ситуаций) в сфере ИБ, формулируется научная задача/проблема по их разрешению, определяющая цель, задачи, объект и предмет исследования. Также указывается гипотеза исследования (при наличии), выбираются информационная база и методы научного исследования, обязательно отражается теоретическая и практическая значимость работы.

Таким образом во введении в сжатой форме описываются все основные положения, обоснованию которых и посвящена ВКР.

Первичным, как более широкое понятие предметной деятельности по обеспечению информационной безопасности, защите информации, указывается объект исследования. Вторичным – предмет исследования, в котором выделяется определенная автором проблемная ситуация в сере ИБ. Предмет исследования чаще всего совпадает с названием темы или очень близок к ней.

К числу задач, решаемых в выпускной работе, можно отнести следующие:

— текущий анализ предметной области и выявление недостатков существующей системы информационной безопасности, определяющих необходимость разработки данного проекта;

— постановку задачи;

— обоснование выбора основных проектных решений в области обеспечения информационной безопасности, защиты информации;

— разработку и исследование методов, моделей, алгоритмов и средств разрешения проблемной ситуации в области обеспечения ИБ в предметной деятельности;

— разработку организационно-технических мер 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 создаваемой системы обеспечения ИБ, защиты информации;

— обоснование результативности/экономической эффективности проекта.

В качестве апробации результатов исследования указываются:

— участие обучающегося в НИР, включая гранты, конкурсы, выполнение НИР в рамках государственного задания или по договорам с организациями и т.п.;

— выступления на конференциях, круглых столах и иных научных мероприятиях;

— имеющиеся научные публикации по теме исследования.

Введение должно быть кратким (2 – 3 стр.) [4].

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

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

4.2.2 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 Сведения, содержащиеся в первой главе, должны давать полное представление о состоянии и степени изученности поставленной проблемы/задачи на данный момент времени.

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

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. [4].

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

В первой главе приводится:

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

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

— разработка модели актуальных угроз и оценка рисков;

— анализ эффективности существующих на объекте системы защиты информации.

Примерная структура первой главы представлена на рисунке 1.

Глава 1. Анализ условий функционирования автоматизированных банковских систем как объектов преднамеренных деструктивных воздействий.

1.1. Структура типовой автоматизированной банковской системы и классификация ее элементов.

1.2. Анализ существующих средств защиты от преднамеренных деструктивных воздействий.

1.3. Модель угроз и классификация преднамеренных деструктивных воздействий.

1.4. Состояние проблемы обеспечения безопасного функционирования автоматизированных систем в условиях преднамеренных деструктивных воздействий.

1.5. Постановка научной задачи.

Выводы по главе 1.

Рисунок 1 – Пример структуры первой главы

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

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

4.2.4 Глава 2 посвящена разработке и исследованию предлагаемых автором моделей, методов и алгоритмов защиты информации, необходимых для решения поставленной научной задачи. Вторая глава может опираться на результаты анализа и обработки практического материала, собранного во время подготовки и написания первой главы и-или производственной практики.

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

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

Примерная структура второй главы представлена на рисунке 2.

Глава 2. Разработка научно-методического аппарата защиты автоматизированных банковских систем от преднамеренных деструктивных воздействий.

2.1. Концептуальная модель системы предупреждения и обнаружения преднамеренных деструктивных воздействий на информационные ресурсы автоматизированных систем

2.2. Совершенствование математической модели активной защиты информационных ресурсов автоматизированных систем от преднамеренных деструктивных воздействий.

2.3. Алгоритмизация задач защиты информационных ресурсов автоматизированных систем от преднамеренных деструктивных воздействий.

2.4. Разработка методики синтеза многоагентных систем предупреждения и обнаружения преднамеренных деструктивных воздействий на информационные ресурсы автоматизированных банковских систем.

2.5. Разработка способа защиты информационных ресурсов автоматизированных систем от преднамеренных деструктивных воздействий.

Выводы по главе 2.

Рисунок 2 – Примерная структура второй главы

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

4.2.5 В третьей главе рассматриваются и обосновываются пути решения исследуемой проблемы/задачи, оценивается возможность их практической

реализации, предлагаются конкретные практические рекомендации и предложения по использованию и дальнейшему совершенствованию разработанных методов, моделей и алгоритмов защиты. В данной главе должны быть сделаны самостоятельные выводы, разработаны рекомендации, при необходимости представлены экономические расчеты.

Примерная структура третьей главы представлена на рисунке 3.

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

Глава 3. Организационно-технические предложения по повышению защищенности информационных ресурсов автоматизированных банковских систем от преднамеренных деструктивных воздействий.

3.1. Программно-технические решения по моделированию параметров реальных процессов функционирования автоматизированных систем.

3.2. Технические решения по параметрической оценке закона распределения потоков сообщений.

3.3. Технические решения для обслуживания разноприоритетных запросов абонентов автоматизированной системы.

3.4 Экспериментальное тестирование предложенного способа защиты информационных ресурсов автоматизированных систем от преднамеренных деструктивных воздействий.

3.5 Предложения и рекомендации по информационному обеспечению задач оценки состояния информационной безопасности автоматизированных банковских систем.

Выводы по главе 3.

Рисунок 3 – Примерная Структура третьей главы

4.2.6 В заключении, являющимся завершающей частью ВКР, рекомендуется отметить, какие задачи были решены в ходе выполнения выпускной работы, определить пути внедрения и направления дальнейшего совершенствования разработанных решений по обеспечению информационной безопасности объекта информатизации; отразить основные проектные решения, разработанные методики и модели, используемые классификаторы, входные и выходные документы, показатели экономической эффективности и другие существенные показатели. Заключение содержит выводы и предложения из всех трех глав ВКР с их кратким обоснованием в соответствии с поставленной целью и задачами, раскрывает значимость полученных

результатов. При этом выводы общего порядка, не вытекающие из результатов и содержания ВКР, не допускаются. Выводы также не могут подменяться механическим повторением выводов по отдельным главам. Объем заключения, должен составлять, как правило, до 5-ти страниц. Заключение является основой доклада студента на защите ВКР. [4]

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

— законы Российской Федерации (в прямой хронологической последовательности);

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

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

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

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

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

— авторефераты диссертаций (в алфавитном порядке);

— научные статьи (в алфавитном порядке);

— литература на иностранном языке (в алфавитном порядке);

— интернет-источники [4].

4.2.8 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. [4]. Приложения должны располагаться в логической последовательности появления ссылок на них из основной части выпускной квалификационной работы. Каждое приложение должно

обязательно иметь обозначение и наименование, характеризующее его содержание. В одном приложении нельзя размещать различные по смыслу таблицы или рисунки. Не допускается дублирование в приложении материала, размещенного в основной части выпускной работы.

4.3 ВКР должна быть распечатана и переплетена. Рекомендуемый объем составляет не менее 80 и не более 100 страниц без учета приложений (для коллективной ВКР 150 - 200 страниц без учета приложений).

5 Порядок подготовки выпускной квалификационной работы

5.1 Сроки составления задания на ВКР, утверждения задания на ВКР в соответствии с приказом Финуниверситета «Об утверждении формы индивидуального плана работы студента, обучающегося по программе магистратуры» на текущий год, размещаются на странице кафедры в разделе «магистратура→ информация по ВКР».

5.2 Сроки предоставления каждой главы ВКР, в соответствии с приказом Финуниверситета «Об утверждении формы индивидуального плана работы студента, обучающегося по программе магистратуры» [6].

5.3 Руководитель ВКР в обязательном порядке проверяет ВКР в системе «Антиплагиат. ВУЗ» на корректность оформления заимствований, выявленных в результате проверки. 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 [4].

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 [4].

Алгоритм размещения ВКР на ИОП описан в [3].

5.5 К защите ВКР допускаются обучающиеся, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по программе магистратуры, успешно сдавшие государственный экзамен [4,5].

6 Требования к оформлению выпускной квалификационной работы

6.1 ВКР оформляется в соответствии с ГОСТ Р 7.0.5-2008 Библиографическая ссылка; ГОСТ 7.32-2017 Отчет о научно-исследовательской работе. Структура и правила оформления; 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. 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 - 15 мм, верхнее и нижнее - 20 мм, левое - 30 мм. Абзацный отступ 1,25 см по всему документу.

6.4 ВКР состоит из следующих структурных элементов: введение, 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, с прописной буквы, полужирным шрифтом, не подчеркиваются, без точки в конце. Если заголовок включает несколько предложений их разделяют точками. Переносы слов в заголовках не допускаются.

«ОГЛАВЛЕНИЕ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ» 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 При необходимости дополнительного пояснения допускается использовать примечание, оформленное в виде сноски. Знак сноски ставят без пробела непосредственно после того слова, числа, символа, предложения, к которому дается пояснение. Знак сноски указывается надстрочно арабскими цифрами, соблюдая сквозную нумерацию по всему тексту.

Сноску располагают с абзацного отступа в конце страницы, на которой приведено поясняемое слово (или данные). Сноску отделяют от текста короткой сплошной тонкой горизонтальной линией с левой стороны страницы. Для сносок шрифт выбирается Times New Roman, черного цвета, размер 12, через одинарный интервал.

6.8 Иллюстрации (графики, схемы, диаграммы) располагаются в ВКР непосредственно после текста, где они упоминаются впервые, или на следующей странице. На все иллюстрации должны быть ссылки. При ссылке необходимо писать

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

Пример - Рисунок 1 – Схема прибора

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

6.9 Таблицы в ВКР располагаются непосредственно после текста, в котором она упоминается впервые, или на следующей странице. На все таблицы должны быть ссылки. При ссылке следует печатать слово «таблица» с указанием её номера.

Наименование таблицы следует помещать над таблицей слева, без абзацного отступа в следующем формате: Таблица Номер таблицы – Наименование таблицы. Наименование таблицы приводят с прописной буквы без точки в конце.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицу с большим количеством строк допускается переносить на другую страницу. При переносе части таблицы на другую страницу слово «Таблица», её номер и наименование указывают один раз слева над первой частью таблицы, а над другими частями также пишут слова «Продолжение таблицы» и указывают номер таблицы.

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

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они представлены в формуле. Значение каждого символа и числового коэффициента

необходимо приводить с новой строки. Первую строку пояснения начинают со слова «где» без двоеточия с абзаца.

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

Пример-

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

где А- площадь круга, мм^2;

π – число Пи (3,14);

r – радиус круга, мм.

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

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

6.11 Приложения могут включать: графический материал, таблицы, расчеты, описания алгоритмов и программ. Приложение оформляют как продолжение ВКР на последующих листах. В тексте отчета на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте ВКР. Каждое приложение следует размещать с новой страницы с указанием в центре верхней части страницы слова «ПРИЛОЖЕНИЕ». Приложение должно иметь заголовок, который записывают с прописной буквы, полужирным шрифтом, отдельной строкой по центру без точки в конце.

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

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

6.12 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.

6.13 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. [4]

7 Правила подготовки к защите выпускной квалификационной работы

7.1 Требования к содержанию 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 финансово-кредитной сфере.

7.2 Требования к презентации ВКР

7.2.1 Требования к содержанию презентации

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».

На слайде должны быть: логотип и полное название Финансового университета, название факультета, кафедры, название работы, данные автора и научного руководителя, как показано на рисунке 4.

Федеральное государственное образовательное
бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

«Разработка многоагентных комплексов защиты автоматизированных банковских систем от преднамеренных деструктивных воздействий»

Выполнил:
студент группы ИБ 18-1м
Иванов Иван Иванович

Научный руководитель:
доктор технических наук, профессор,
Петров Петр Петрович

Москва, 2020

Рисунок 4 - Пример оформления первого слайда презентации

На следующем слайде приводится актуальность темы исследования, обозначаются цель работы, объект и предмет исследования.

Объект исследования – эта та часть проблемы/задачи, которую Вы собираетесь исследовать, предмет – это метод, которым вы будете решать свою часть проблемы.

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

Основное время доклада должно быть отведено методу решения указанной в задании проблемы/задачи, на то, что выполнено в работе студентом, и к каким результатам это привело.

В докладе и в презентации необходимо продемонстрировать владение математическим аппаратом для проведения исследования, различными методами

моделирования, обработки, статистики, построения алгоритмов и программированием. Для этого на слайдах должны быть представлены математические выкладки, графики, алгоритмы, модели.

На последнем слайде должны быть представлены выводы по работе.

В выводах кратко отражается, что главное сделано в работе, какой результат достигнут, в чем заключается самостоятельная часть работы и к каким результатам приведет внедрение исследований на объекте информатизации финансово-кредитной сферы.

7.2.2 Требования к оформлению презентации

Количество слайдов – 12-18 с учетом трех слайдов, отводимых на титульный лист, введение и заключение.

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

Слайды необходимо оформлять в строгом стиле.

В левом верхнем углу должен быть номер слайда.

Содержание слайда должно быть максимально информативно и понятно (рисунок 5).

8

Трёхмерная модель состояния информационной безопасности объекта защиты

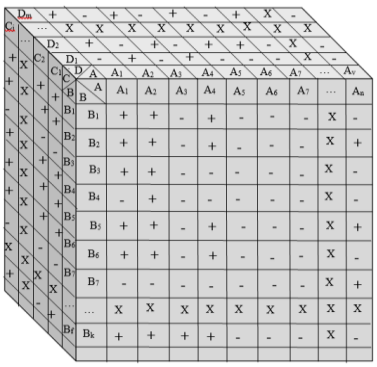

Рисунок 4- Трехмерная модель защищенности объекта кредитно-финансовой сферы (создано автором)

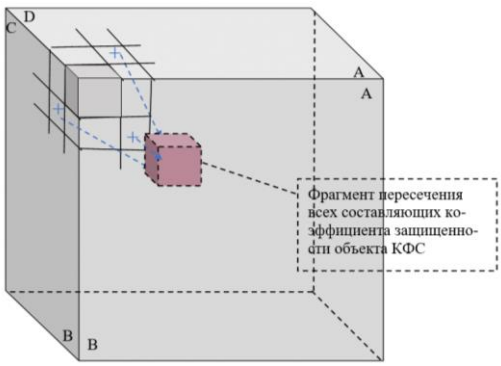

Рисунок 5- Фрагмент трехмерной модели коэффициента защищенности объекта информатизации КФС (создано автором)

Рисунок 5 – Пример оформления слайда презентации к докладу на защите ВКР

Пояснения на слайде должны быть краткими, но емкими.

При расположении на слайде математических формул необходимо их оформлять в соответствии с п. 6.10.

Изображение скриншотов программных закладок должно быть выполнено в хорошем качестве. В презентацию должны быть включены только те скриншоты, которые отражают суть работы и которые имеются в основном теле и приложениях ВКР.

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 [4,5].

7.4 Порядок повторной защиты ВКР, определенный пунктом 5.4 [5].

7.5 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. [4,5]

7.6 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 [4,5].

8 Критерии оценки выпускной квалификационной работы

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

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

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

Критерии оценок:

«Отлично» – работа имеет исследовательский характер, грамотно изложенную теоретическую часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. При ее защите студент свободно оперирует данными исследования, вносит обоснованные предложения, свободно ориентируется в вопросах тематики исследования, правильно применяет эти знания при изложении материала, легко отвечает на поставленные вопросы. На работу имеется положительный отзыв руководителя.

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

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

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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ.

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

3 Регламент размещения на информационно-образовательном портале Финансового университета курсовых работ (проектов) и выпускных квалификационных работ, порядок хранения и списания (утв. приказом Финуниверситета от 12.11.2015 №2372/о).

4 Положение о выпускной квалификационной работе по программе магистратуры в Финансовом университете (утв. приказом Финуниверситета от 17.10.2017 № 1819/о).

5 Порядок проведения государственной итоговой аттестации по программам бакалавриата и магистратуры в Финансовом университете (утв. приказом Финуниверситета от 14.10 2016 № 1988/о.)

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

ПРИЛОЖЕНИЕ А

Форма заявления на выпускную квалификационную работу

ФИНУНИВЕРСИТЕТ

Кафедра «Информационная безопасность»
(наименование департамента/кафедры)

СОГЛАСЕН

_____ _____
(дата) (подпись)

Руководителю магистерской программы

С.В. Дворянкину, д.т.н., профессору
(И.О. Фамилия, уч.степень, уч.звание)

_____
(Фамилия И.О. обучающегося)

_____
(наименование факультета)

_____
(№ учебной группы)

Тел. Обучающегося: _____

E-mail обучающегося: _____

ЗАЯВЛЕНИЕ

Прошу закрепить за мной тему ВКР «*Название*» и назначить руководителем И.О. Фамилия, уч.степень, уч.звание.

«_____» _____ 20___г. _____
(подпись обучающегося)

Согласовано:

Руководитель ВКР

_____ _____
(подпись) (И.О. Фамилия)

«_____» _____ 20___г.

ПРИЛОЖЕНИЕ Б

Форма задания на выпускную квалификационную работу

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
КАФЕДРА ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УТВЕРЖДАЮ
Руководитель выпускной квалификационной работы
_____
(ученая степень ,ученое звание, должность)
_____(И.О. Фамилия)

ЗАДАНИЕ

на выпускную квалификационную работу

студенту _____
(фамилия, имя, отчество)

Тема выпускной квалификационной работы:

_____

закреплена приказом ректора Финуниверситета от «___» _____20__г. № _____

Целевая установка: разработка предложений по использованию результатов работы
_____
_____

Основные вопросы, подлежащие разработке (исследованию):

_____
_____
_____

Основная литература указывается в Приложении к заданию
Срок представления законченной работы_____
Дата выдачи задания _____

Руководитель: _____
(должность, подпись, фамилия)

Задание получил: _____
(подпись, фамилия студента)

ПРИЛОЖЕНИЕ В

Форма отзыва руководителя выпускной квалификационной работы

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

ОТЗЫВ РУКОВОДИТЕЛЯ

о работе обучающегося в период подготовки выпускной квалификационной работы

по программе магистратуры

Обучающийся _____
(фамилия, имя, отчество)

Факультет _____

Кафедра_____

Направление подготовки _____
Направленность_____
Наименование темы_____
Руководитель_____
(фамилия, имя, отчество, должность, ученое звание, степень)

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

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

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

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

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

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

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

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

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

(Ф.И.О. руководителя, полностью)

(подпись руководителя)

«___» _____ 20_ г.

ПРИЛОЖЕНИЕ Г

Оформление титульного листа

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Факультет Прикладная математика и информационные технологии
Кафедра «Информационная безопасность»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: «*Название согласно приказу*»

Направление подготовки 10.04.01 «Информационная безопасность»

Направленность программы магистратуры: «Информационная безопасность финансово-кредитных организаций»

Выполнил студент группы ____
_____
(ФИО полностью) (подпись)
Руководитель _____
ученая степень, ученое звание, должность
_____
(ФИО полностью) (подпись)

ВКР соответствует предъявленным требованиям
Заведующий кафедрой
_____
(ученая степень, ученое звание)
_____ _____
(Подпись) (И.О.Фамилия)
«___» _____ 20__ г.

Москва 20__