Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе

_____Н.Г. Кузнецов
«01» июня 2018 г.

Программа государственной итоговой аттестации

по направлению (специальности) подготовки

10.03.01 «Информационная безопасность»

Профиль (специализация)
10.03.01.02 "Организация и технология защиты информации"

Уровень образования

бакалавриат

Ростов-на-Дону
2018

Составитель: к.т.н., доцент _____ Скляров А. В.

Рецензенты:

Генеральный директор ЗАО
«Универсальные Бизнес Технологии»
Тактаров А.С.
д.э.н., профессор кафедры ФиПМ Денисов М.Ю.

Программа государственной итоговой аттестации составлена в соответствии с ФГОС ВО по направлению подготовки *10.03.01 «Информационная безопасность»*, утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. N 1515.

Программа государственной итоговой аттестации утверждена на заседании кафедры Информационных технологий и защиты информации, протокол № 3 от «17» мая 2018 г.

Заведующий кафедрой _____ Тищенко Е.Н.
подпись

СОГЛАСОВАНО:

Отделом образовательных программ и планирования учебного процесса _____ Т.В.Торопова 30.05.18

Проректором по учебно-методической работе _____ В.М.Джуха 31.05.18

Оглавление

1. Общие положения

Организация и проведение государственной итоговой аттестации ФГБОУ ВО «РГЭУ (РИНХ)» определяется:

– Порядком проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утверждённым приказом Министерства образования и науки Российской Федерации от 29 июня 2015 г. № 636.

– Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утверждённым в РГЭУ (РИНХ) 29 декабря 2015 г.

К государственной итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план (индивидуальный учебный план).

2. Цели государственной итоговой аттестации

Целью проведения государственной итоговой аттестации является определение соответствия результатов освоения обучающимися образовательной программы соответствующим требованиям федерального государственного образовательного стандарта по направлению подготовки 10.03.01 «Информационная безопасность».

В частности, проверяется готовность выпускника к решению профессиональных задач в рамках следующих видов профессиональной деятельности, предусмотренными ФГОС:

- эксплуатационная;
- проектно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая.

3. Содержание государственной итоговой аттестации

3.1.Трудоемкость государственной итоговой аттестации составляет 9 зачетных единиц.

3.2.Государственная итоговая аттестация выпускников проводится в форме:

– государственного экзамена;

– защиты выпускной квалификационной работы (далее вместе – государственные аттестационные испытания).

3.3.В ГИА входит защита выпускной квалифицированной работы, включая подготовку к процедуре защиты и процедуру защиты, а также подготовка к сдаче и сдача государственного экзамена.

4. Фонд оценочных средств для государственной итоговой аттестации

Фонд оценочных средств для проведения государственной итоговой аттестации представлен в приложении 1 к программе государственной итоговой аттестации.

5. Содержание государственного экзамена

5.1 Форма проведения государственного экзамена: *устно*

5.2 Программа проведения государственного экзамена:

Наименование дисциплины, выносимой на государственный экзамен	Разделы (темы) дисциплины, выносимые на государственный экзамен
Защита информационных процессов и систем	Тема. Управление рисками. Модель безопасности с полным перекрытием Тема. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками Тема. Методики построения систем защиты информации Тема. Методики и программные продукты для оценки рисков. Тема. Проведение оценки рисков в соответствии с методикой Microsoft Тема. Технические мероприятия по снижению уровня риска Тема. Инфраструктура открытых ключей. Цифровые сертификаты
Техническая защита информации	Тема Классификация технологий обеспечения информационной безопасности объектов на различных этапах их жизненного цикла Тема Выбор методов защиты информации при проектировании объектов информатизации Тема Выбор методов защиты информации при эксплуатации объектов информатизации Тема Методы физической защиты объектов от несанкционированного доступа» Тема Методы криптографической защиты объектов информатизации Тема Технологии технической зашиты информации от утечки по техническим каналам

	Тема Технологии зашиты информации от программно-математических воздействий
Основы управления информационной безопасностью	Тема Цели и задачи управления информационной безопасностью объекта Тема Основные концепции и архитектуры построения систем управления информационной безопасностью Тема Основы функционирования систем управления информационной безопасностью на объектах Тема Аудит и анализ состояния информационной безопасности на объектах информатизации Тема Организацию мониторинга состояния информационной безопасности объектов Тема Оценка эффективность проводимых мероприятий по совершенствованию системы управления информационной безопасностью Тема Основные существующие и перспективные продукты управления системами информационной безопасности
Комплексная система защиты информации на предприятии	Тема. Сущность, назначение КСЗИ автоматизированных информационных и телекоммуникационных систем. Тема. Методика выявления каналов несанкционированного доступа к информации. Тема. Методика выявления способов воздействия на информацию. Тема. Определение состава кадрового обеспечения функционирования КСЗИ. Тема. Планирование и контроль функционирования КСЗИ. Способы и методы планирования. Тема. Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем Тема. Методологические основы организации КСЗИ. Тема. Основные стадии создания КСЗИ. Характеристика основных стадий создания КСЗИ. Тема. Сущность процессов управления КСЗИ. Тема. Характеристика подходов к оценке эффективности систем защиты информации.

	Тема. Классификационная структура методов и моделей оценки эффективности комплексной системы защиты информации.
Организационное и правовое обеспечение информационной безопасности	Тема. Система защиты информации. Роль и место организационно-правовой защиты информации в структуре системы обеспечения информационной безопасности. Тема. Законодательно-правовые и организационные основы обеспечения информационной безопасности. Тема. Структура организационно-правовой защиты информации. Тема. Политика безопасности предприятия. Организационное управление защитой информации. Тема. Оформление запроса на лицензирование по видам деятельности Тема. Проведения аттестации объектов информатизации и оформление ее результатов. Тема. Разработка политики безопасности предприятия Тема. Организация и принципы допускной работы. Тема. Организация пропускного и внутриобъектового режимов.

Перечень вопросов, выносимых на государственный экзамен представлен в приложении 1 к программе ГИА.

6. Требования к выпускной квалификационной работе обучающегося

6.1. Вид выпускной квалификационной работы: *бакалаврская работа.*

6.2. Примерная тематика выпускных квалификационных работ

1. Методы защищенной передачи информации в радиоканалах систем управления
2. Методы оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования
3. Методы прогнозирования информационных угроз

4. Метод формирования электронной цифровой подписи на основе открытого коллективного ключа для электронного документооборота предприятия

5. Методика аудита информационной безопасности объектов электронной коммерции

6. Методика защиты информации в беспроводных сетях на основе динамической маршрутизации трафика

7. Методика обработки рисков нарушения безопасности информации в объектно-ориентированных сетях хранения данных

8. Методики защиты цифровых видеодоказательств

9. Методы и программные средства исследования моделей логического разграничения доступа на предмет выполнения требований по безопасности

10. Методы и средства автоматизированного обнаружения уязвимостей в программах на языке С

11. Методы оценки информационной безопасности предприятия на основе процессного подхода

12. Модели и алгоритмы оценки эффективности программных систем защиты информации

13. Модели и методики поиска источников внутренних угроз безопасности предприятия

14. Модели и средства выявления угроз нарушения информационной безопасности штатных механизмов обнаружения скрытых информационных воздействий

15. Модели и алгоритмы обнаружения компьютерных атак в локальных вычислительных сетях органов государственного и муниципального управления

16. Разграничение доступа в IP-сетях на основе моделей состояния виртуальных соединений

17. Разграничение доступа в компьютерных сетях на основе классификации и приоритетной обработки пакетного трафика

18. Разработка и исследование алгоритмов и методик идентификации цифровых устройств записи

19. Разработка системы поддержки принятия решений для обеспечения физической безопасности объектов

20. Исследование и развитие методического обеспечения оценки и управления рисками информационных систем

21. Исследование процессов передачи и обработки информации в конфиденциальном хранилище электронных документов

22. Исследование способов выявления сетевых узлов, участвующих в несанкционированной рассылке сообщений электронной почты

23. Комплексная методика моделирования рисков информационной безопасности открытых систем

24. Методика оценки рисков при построении системы защиты

25. Методика оценки рисков в платёжной системе банковских карт

26. Методы аутентификации информации и обеспечения защищенности документов от подделки

27. Методы защиты цифровой видеоинформации при ее передаче в распределенных компьютерных сетях

28. Методы контроля эквивалентности информационных технологий в системах защиты информации

29. Многоуровневая многоагентная система фильтрации спама в организации

30. Модели и алгоритмы повышения защищенности информации в интегрированных системах безопасности на основе оптимизации временных ресурсов

6.3. Методические указания по оформлению и содержанию выпускной квалификационной работы

Методические указания по оформлению и содержанию ВКР представлены в приложении 2 к программе государственной итоговой аттестации

7. Перечень основной и дополнительной литературы, необходимой для подготовки к государственной итоговой аттестации

7.1. Основная литература

№	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), с указанием наличия в библиотеке; перечень учебно-методического обеспечения	
	Основная литература	
1	Аверченков В. И. , Рытов М. Ю. , Кондрашин Г. В. , Рудановский М. В. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс]: учебное пособие для вузов / Аверченков В. И. , Рытов М. Ю. , Кондрашин Г. В. , Рудановский М. В. - М.: Флинта, 2016. – 224 с. - ISBN: 978-5-9765-1274-0 - http://biblioclub.ru/index.php?page=book_red&id=93351&sr=1	Неограниченный доступ для зарегистрированных пользователей
2	Аверченков В. И. , Рытов М. Ю. Служба защиты информации : организация и управление [Электронный ресурс]: учебное пособие для вузов / Аверченков В. И. , Рытов М. Ю. - М.: Флинта, 2016. – 186 с. - ISBN: 978-5-9765-1271-9 - http://biblioclub.ru/index.php?page=book_red&id=93356&sr=1	Неограниченный доступ для зарегистрированных пользователей
3	Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Загинайлов Ю. Н. - М., Берлин: Директ-Медиа, 2015. – 253 с. - ISBN: 978-5-4475-3946-7 - http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1	Неограниченный доступ для зарегистрированных пользователей
4	Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс]: учебное пособие / Сердюк В. А. – М.: Издательский дом Высшей школы экономики, 2015. - ISBN: 978-5-7598-0698-1 - http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1	Неограниченный доступ для зарегистрированных

		пользователей
5	Петренко В. И. Теоретические основы защиты информации [Электронный ресурс]: учебное пособие / Петренко В. И. - Ставрополь: СКФУ, 2015.- 222 с. - http://biblioclub.ru/index.php?page=book_red&id=458204&sr=1	Неограниченный доступ для зарегистрированных пользователей
6	Долозов Н. Л. , Гультяева Т. А. Программные средства защиты информации [Электронный ресурс]: конспект лекций / Долозов Н. Л. , Гультяева Т. А. - Новосибирск: НГТУ, 2015. – 63 с. - ISBN: 978-5-7782-2753-8 – http://biblioclub.ru/index.php?page=book_red&id=438307&sr=1	Неограниченный доступ для зарегистрированных пользователей
7	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / Прохорова О. В. - Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – ISBN: 978-5-9585-0603-3 – http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1	Неограниченный доступ для зарегистрированных пользователей
8	Сагдеев К. М. , Петренко В. И. , Чипига А. Ф. Физические основы защиты информации [Электронный ресурс]: учебное пособие / Сагдеев К. М. , Петренко В. И. , Чипига А. Ф. – Ставрополь: СКФУ, 2015. – 394 с. – http://biblioclub.ru/index.php?page=book_red&id=458285&sr=1	Неограниченный доступ для зарегистрированных пользователей
9	Новожилов О.П. Электротехника и электроника [Текст] : учеб. для бакалавров : учеб. для студентов вузов, обучающихся по напр. подгот. 230100 (654600) "Информатика и вычислит. техника" / О. П. Новожилов ; Моск. гос. индустр. ун-т. - 2-е изд., испр. и доп. - М. : Юрайт, 2013. - 653 с.	65
10	Шейдаков, Николай Евгеньевич. Физические основы защиты информации [Текст] : учеб. пособие / Н. Е. Шейдаков, Е. Н. Тищенко ; Рост. гос. экон. ун-т (РИНХ). - Ростов н/Д : Изд-во РГЭУ (РИНХ), 2013. - 188 с.	66

7.2. Дополнительная литература

Перечень дополнительной учебной литературы		
1	Свинарев Н. А. , Ланкин О. В. , Данилкин А. П. , Потехецкий С. В. , Перетокин О. И. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие / Свинарев Н. А. , Ланкин О. В. , Данилкин А. П. , Потехецкий С. В. , Перетокин О. И. - Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с. - ISBN: 978-5-00032-018-1 – http://biblioclub.ru/index.php?page=book_red&id=255905&sr=1	Неограниченный доступ для зарегистрированных пользователей
2	Руденков Н. А. , Пролетарский А. В. , Смирнова Е. В. , Суровов А. М. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Руденков Н. А. , Пролетарский А. В. , Смирнова Е. В. , Суровов А. М. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. - http://biblioclub.ru/index.php?page=book_red&id=428820&sr=1	Неограниченный доступ для зарегистрированных пользователей
3	Шубович В. Г. , Капитанчук В. В. , Знаенко Н. С. , Титаренко Ю. И. Разработка моделей криптографической защиты информации [Электронный ресурс]: монография / Шубович В. Г. , Капитанчук В. В. , Знаенко Н. С. , Титаренко Ю. И. – Ульяновск: УлГПУ, 2013. – 128 с. – ISBN: 978-5-86045-640-2 – http://biblioclub.ru/index.php?page=book_red&id=278070&sr=1	Неограниченный доступ для зарегистрированных

		пользователей
4	Петренко В. И. Защита персональных данных в информационных системах информации [Электронный ресурс]: учебное пособие / Петренко В. И. – Ставрополь: СКФУ, 2016. – 201 с. – http://biblioclub.ru/index.php?page=book_red&id=459205&sr=1	Неограниченный доступ для зарегистрированных пользователей
5	Гуляев В. П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации [Электронный ресурс]: учебно-методический комплекс / Гуляев В. П. - Екатеринбург: Издательство Уральского университета, 2014. – 163 с. – http://biblioclub.ru/index.php?page=book_red&id=275706&sr=1	Неограниченный доступ для зарегистрированных пользователей
6	Аверченков В. И. , Рытов М. Ю. , Кувыклин А. В. , Рудановский М. В. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс]: учебное пособие / Аверченков В. И. , Рытов М. Ю. , Кувыклин А. В. , Рудановский М. В. – М.: Флинта, 2016. – 100 с. – ISBN: 978-5-9765-1277-1 – http://biblioclub.ru/index.php?page=book_red&id=93259&sr=1	Неограниченный доступ для зарегистрированных пользователей
7	Аверченков В. И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / Аверченков В. И. – М.: Флинта, 2016 – 269 с. – ISBN: 978-5-9765-1256-6 – http://biblioclub.ru/index.php?page=book_red&id=93245&sr=1	Неограниченный доступ для зарегистрированных пользователей
8	Ефремов И. В. , Солопова В. А. Информационные технологии в сфере безопасности [Электронный ресурс]: учебное пособие / Ефремов И. В. , Солопова В. А. – Оренбург: ОГУ, 2013 – 116 с. – http://biblioclub.ru/index.php?page=book_red&id=259178&sr=1	Неограниченный доступ для зарегистрированных пользователей
9	Громов Ю. Ю. , Мартемьянов Ю. Ф. , Букурако Ю. К. , Иванова О. Г. , Однолько В. Г. Организация безопасной работы информационных систем [Электронный ресурс]: учебное пособие / Громов Ю. Ю. , Мартемьянов Ю. Ф. , Букурако Ю. К. , Иванова О. Г. , Однолько В. Г. – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014 – 132 с. – http://biblioclub.ru/index.php?page=book_red&id=277794&sr=1	Неограниченный доступ для зарегистрированных пользователей
10	Тищенко Евгений Николаевич (РГЭУ (РИНХ)). Инструментальные методы анализа потребительского качества защищенных информационных систем [Текст] : учеб. пособие / Е. Н. Тищенко ; Рост. гос. экон. ун-т (РИНХ). - Ростов н/Д : Изд-во РГЭУ (РИНХ), 2016. - 126 с. - ISBN 978-5-7972-2204-0	68
11	Шейдаков Николай Евгеньевич (РГЭУ (РИНХ)). Физические основы защиты информации [Текст] : учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность" / Н. Е. Шейдаков, О. В. Серпенинов, Е. Н. Тищенко ; Рост. гос. экон. ун-т (РИНХ). - М. : РИОР : ИНФРА-М, 2016. - 204 с. - ISBN 978-5-369-01603-9	110
12	Хорев Павел Борисович Программно-аппаратная защита информации [Текст] : учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. "Информац. безопасность" / П. Б. Хорев. - 2-е изд. испр. и доп. - М. : ФОРУМ : ИНФРА-М, 2015. - 352 с. – ISBN 978-5-00091-004-7 (ФОРУМ).	25
13	Попова Людмила Константиновна (РГЭУ (РИНХ)). Информатика [Текст] : лаборатор. практикум / Л. К. Попова ; Рост. гос. экон. ун-т (РИНХ). - Ростов н/Д : Изд-во РГЭУ (РИНХ), 2014. - 95 с. - ISBN 978-5-7972-1993-4	68
14	Савельева Наталья Григорьевна (РГЭУ (РИНХ)). Информатика и программирование	63

	[Текст] : учеб. пособие / Н. Г. Савельева, Е. Г. Веретенникова ; Рост. гос. экон. ун-т (РИНХ). - Ростов н/Д : Изд-во РГЭУ (РИНХ), 2016. - 140 с. - ISBN 978-5-7972-2215-6	
15	Калугян Каринэ Хачересовна (РГЭУ (РИНХ)). Теория систем и системный анализ [Текст] : учеб. пособие / К. Х. Калугян, Г. Н. Хубаев ; Рост. гос. экон. ун-т (РИНХ). - Ростов н/Д : Изд-во РГЭУ (РИНХ), 2016. - 76 с. - ISBN 978-5-7972-2245-3	63

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Федеральная служба по техническому и экспортному контролю (ФСТЭК РФ)/ http://fstec.ru

Приложение 1
к программе ГИА

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры ИТиЗИ
Протокол № 8 от «28» марта 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки / специальность

10.03.01 «Информационная безопасность»

Профиль (специализация)
10.03.01.02 "Организация и технология защиты информации"

Уровень образования
бакалавриат

Составитель _____ Скляров А. В., к.т.н., доцент

Ростов-на-Дону, 2018

Оглавление

1. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы

В рамках проведения государственной итоговой аттестации проверяется степень освоения выпускником следующих компетенций:

√ ОК-1 способность использовать основы философских знаний для формирования мировоззренческой позиции

√ ОК-2 способность использовать основы экономических знаний в различных сферах деятельности

√ ОК-3 способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма

√ ОК-4 способность использовать основы правовых знаний в различных сферах деятельности

√ ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

√ ОК-6 способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия

√ ОК-7 способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности

√ ОК-8 способность к самоорганизации и самообразованию

√ ОК-9 способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности

√ ОПК-1 способность анализировать физические явления и процессы для решения профессиональных задач

√ ОПК-2 способность применять соответствующий математический аппарат для решения профессиональных задач

√ ОПК-3 способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач

√ ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации

√ ОПК-5 способность использовать нормативные правовые акты в профессиональной деятельности

√ ОПК-6 способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности

√ ОПК-7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

√ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

√ ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

√ПК-3 способность администрировать подсистемы информационной безопасности объекта защиты

√ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

√ ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

√ ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

√ ПК-7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

√ ПК-8 способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

√ ПК-9 способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

√ ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

√ ПК-11 способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

√ ПК-12 способность принимать участие в проведении экспериментальных исследований системы защиты информации

√ ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

√ ПК-14 способность организовывать работу малого коллектива исполнителей в профессиональной деятельности

ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ПСК-2.1 способность проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз информационной безопасности, вероятности их реализации и размера ущерба

ПСК-2.2способность формировать рекомендации по оптимизации функционального процесса объекта информатизации и разрабатывать комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты, с осуществлением его технико-экономического обоснования

ПСК-2.3 способность организовать и принимать участие в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты, с последующим его сопровождением

ПСК-2.4 способность организовать контроль защищенности объекта информатизации в соответствии с нормативными документами

2. Показатели и критерии оценивания компетенций

Код компетенции	Наименование компетенции	Объект оценки	Показатели оценивания компетенции	Критерии оценивания компетенции
ОК-1	способность использовать основы философских знаний для формирования мировоззренческой позиции	З1. знание философских основ профессиональной деятельности. З2. знание основных философских категорий и проблем человеческого бытия У умение приобретать и использовать философские знания для анализа предметно-практической деятельности В. владение навыками работы с основными философскими категориями	обзор литературы по теме ВКР	полнота представленного обзора литературы по теме ВКР

ОК-3	способность анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции	З1. знание основных этапов, тенденций и закономерностей исторического процесса У. умение выявлять значимость исторических знаний для анализа предметной области В. владение навыками исторического анализа для определения места профессиональной деятельности в культурно-исторической парадигме	обзор литературы по теме ВКР	полнота представленного обзора литературы по теме ВКР
ОК-2	способность использовать основы экономических знаний в различных сферах деятельности	З. знание основных экономических категорий У. умение использовать теоретические знания в прикладных целях В. владение инструментами экономического анализа предмета исследования	обзор литературы по теме ВКР	полнота представленного обзора литературы по теме ВКР

ОК-4	способность использовать основы правовых знаний в различных сферах жизнедеятельности	З. знание основных нормативно-правовых актов в предметной области У. умение использовать теоретические знания в правовой сфере в прикладных целях В. владение навыками применения правовых актов в профессиональной деятельности	систематизация нормативно-правовх актов, регламентирующих деятельность в предметной области	наличие в списке литературы к ВКР нормативно-правовых актов
ОК-7	способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и	З1. знание норм словоупотребления З2. знание языковых средств для обеспечения логической связанности письменного и устного текста У. умение свободно общаться	изложение результатов ВКР в виде краткого сообщения	ясность, четкость и последовательность изложения материала

	межкультурного взаимодействия	В. владение различными формами, видами учетной и письменной коммуникации в учебной и профессиональной деятельности		
ОК-6	способность работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	З. знание основных принципов работы в коллективе. У. умение аргументировать собственную мировоззренческую позицию в процессе межличностной коммуникации В. умение взаимодействовать с экспертами в профессиональной области	формулирование ответов на вопросы членов ГЭК	аргументированность ответов

ОК-8	способность к самоорганизации и самообразованию	З. знание путей профессионального самосовершенствования. У. умение анализировать информацию и использовать ее для повышения своей квалификации В. владение технологиями приобретения профессиональных знаний	использование дополнительной литературы при подготовке к ГЭ и написанию ВКР	полнота перечня литературы к ВКР
ОК-9	способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	З. знание основных методов укрепления здоровья У. умение заботиться о своем здоровье В. владение навыками самостоятельного достижения должного уровня физической подготовленности	обладание должной физической формой	активность профессиональной деятельности

ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	З. знание методов анализа физических явлений и процессов У. умение использовать технические навыки и приемы, средства для анализа физических явлений и процессов В. владение методиками проведения анализа физических явлений и процессов основными методами решения стандартных задач	использование методов анализа физических явлений и процессов	корректность использования методов анализа физических явлений и процессов

ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	З. знание математического аппарата применяемого для решения профессиональных задач У. умение применять соответствующий математический аппарат для решения профессиональных задач В. владение методиками проведения математической обработки информации при решении профессиональных задач	обладание математическим аппаратом, применяемым для решения профессиональных задач	адекватность применения математического аппарата для решения профессиональных задач

ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	З. знание основных положений электротехники, электроники и схемотехники У. умение осуществлять научно обоснованный выбор радиотехнических и электронных устройства для решения профессиональных задач В. владение навыками анализа эффективности применения радиотехнических и электронных устройств	применение основных положений электротехники, электроники и схемотехники	аргументированность применение основных положений электротехники, электроники и схемотехники

ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	З. знание закономерностей развития информационного общества У. умение применять программные и программно-аппаратные средства поиска и обработки информации В. владение методиками применения информационных технологий для поиска и обработки информации	обладание информационными технологиями для поиска и обработки информации	точность поиска и обработки информации
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	З. знание нормативных правовых актов, регламентирующие деятельность в области информационной безопасности	применение нормативных правовых актов, регламентирующие деятельность в области информационной безопасности	корректность применения нормативных правовых актов, регламентирующие деятельность в области информационной безопасности

		У. умение использовать нормативные правовые акты в профессиональной деятельности В. владение методами правового регулирования профессиональной деятельности		

ОПК-6	способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности	З. знание приемов оказания первой помощи и мероприятия по охране труда и технике безопасности У. умение применять методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций В. владение методиками оказания первой помощи, применения средств защиты персонала предприятия и населения в условиях чрезвычайных ситуаций и организации мероприятий по охране труда и технике безопасности	обладание приемами оказания первой помощи	адекватность применения приемов оказания первой помощи

ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	З. знание информационных ресурсов, подлежащих защите, угрозы безопасности информации и возможные пути их реализации У. умение анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты В. владение методиками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	применение методов определения информационных ресурсов, подлежащих защите	корректность применения методов определения информационных ресурсов, подлежащих защите
ПК-1	способность выполнять работы по установке, настройке и	З. знание основных способов выполнять работы по установке, настройке и	осуществление работ по установке, настройке и обслуживанию программных, программно-	осуществление работ по установке, настройке и обслуживанию программных,

	обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации У. умение проводить работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации В. владеть основными способами установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	аппаратных (в том числе криптографических) и технических средств защиты информации	программно-аппаратных (в том числе криптографических) и технических средств защиты информации

ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	З. знание программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования У. умение пользоваться программными средствами системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования В. владение методиками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и	использование программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования	корректность использования программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования

		систем программирования для решения профессиональных задач		
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	З. знание методов администрирования подсистемы информационной безопасности объекта защиты У. умение проводить выбор рациональных администрирования подсистемы информационной безопасности объекта защиты В. владение основными технологиями администрирования подсистемы информационной безопасности объекта защиты	реализация методов администрирования подсистемы информационной безопасности объекта защиты	обоснованность реализации методов администрирования подсистемы информационной безопасности объекта защиты
ПК-4	способность участвовать в работах по	З. знание содержания работ по реализации политики	реализация методов формирования политики информационной	корректность реализация методов формирования политики

	реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты У. умение проводить работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты В. владение основными способами проведения работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	безопасности объекта защиты	информационной безопасности объекта защиты

ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	З. знание методов организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации У. умение проводить с аттестацию объекта информатизации по требованиям безопасности информации В. владение основными методиками аттестации объекта информатизации по требованиям безопасности информации	обладание методами аттестации объекта информатизации по требованиям безопасности информации	адекватность применения методов аттестации объекта информатизации по требованиям безопасности информации

ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	З. знание методов контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации У. умение проводить контрольные проверки работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации В. владение основными методиками контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	обладание методами проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	точность применения методов проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	З. знание современных методик анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности У. умение проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности В. владение методиками методик анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	использование методик анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	аргументированность использования методик анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	З. знание основных способов оформления рабочей технической документации с учетом действующих нормативных и методических документов У. умение организовать оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов В. владение основными методиками оформления рабочей технической документации с учетом действующих нормативных и методических документов	выполнение функций по оформлению рабочей технической документации с учетом действующих нормативных и методических документов	корректность выполнения функций по оформлению рабочей технической документации с учетом действующих нормативных и методических документов

ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	З. знание основных способов подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности У. умение осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей	реализация подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности	полнота подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности

		профессиональной деятельности В. владение основными методиками подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности		
ПК-10	способность проводить анализ информационной безопасности	З. знание стандартов в области информационной безопасности	обладание методами применения стандартов в области информационной безопасности	корректность применения стандартов в области информационной безопасности

	объектов и систем на соответствие требованиям стандартов в области информационной безопасности	У. умение проводить анализ информационной безопасности объектов и систем В. владеть способами анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	З. знание методик, обработки, оценки погрешности и достоверности их результатов У. умение проводить эксперименты по заданной методике В. владение основными методиками, обработки, оценки погрешности и достоверности их результатов	выполнение экспериментов по заданной методике	точность выполнения экспериментов по заданной методике

ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	З. знание основных способов проведения экспериментальных исследований системы защиты информации У. умение выполнять экспериментальные исследования системы защиты информации В. владеть основными способами экспериментальных исследований системы защиты информации	обладание способами проведения экспериментальных исследований системы защиты информации	аргументированность использования способов проведения экспериментальных исследований системы защиты информации

ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	З. знание комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации У. умение формировать, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации В. владение основными способами формирования, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	использование комплекса мер по обеспечению информационной безопасности и управления процессом их реализации	адекватность использования комплекса мер по обеспечению информационной безопасности и управления процессом их реализации

ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	З. знание основ организации работ малого коллектива исполнителей в профессиональной деятельности У. умение организовывать работу малого коллектива исполнителей в профессиональной деятельности В. владение методами планирования и организации проектной деятельности на основе стандартов управления проектами	обладание методами организации работ малого коллектива исполнителей в профессиональной деятельности	корректность использования методов организации работ малого коллектива исполнителей в профессиональной деятельности

ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	З. знание нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю У. умение организовывать технологический процесс защиты информации ограниченного доступа В. владение способами организации технологических процессов защиты информации ограниченного доступа	выполнение мероприятий по организации технологического процесса защиты информации ограниченного доступа	полнота мероприятий по организации технологического процесса защиты информации ограниченного доступа

ПСК-2.1	способность проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз информационной безопасности, вероятности их реализации и размера ущерба	З. знание основных способов анализ функционального процесса объекта информатизации У. умение проводить анализ функционального процесса объекта информатизации В. владение на практике навыками анализ функционального процесса объекта информатизации с целью выявления возможных угроз информационной безопасности, вероятности их реализации и размера ущерба	обладание методами анализа функционального процесса объекта информатизации	адекватность применения методов анализа функционального процесса объекта информатизации

ПСК-2.2	способность формировать рекомендации по оптимизации функционального процесса объекта информатизации и разрабатывать комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты, с осуществлением его технико-экономического обоснования	З. знание основных методов оптимизации функционального процесса объекта информатизации и разработки комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты У. умение использовать основные методы методов оптимизации функционального процесса объекта информатизации и разработки комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты В. владение на практике навыками использования	выполнение оптимизации функционального процесса объекта информатизации	корректность выполнения оптимизации функционального процесса объекта информатизации

		основных методов оптимизации функционального процесса объекта информатизации и разработки комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты		

ПСК-2.3	способность организовать и принимать участие в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты, с последующим его сопровождением	З. знание комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты, с последующим его сопровождением У. умение организовать и принимать участие в реализации комплекса организационно-технических мер по обеспечению информационной безопасности В. владение на практике методами организации и реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты	владение комплексом организационно-технических мер по обеспечению информационной безопасности	полнота применения комплекса организационно-технических мер по обеспечению информационной безопасности

ПСК-2.4	способность организовать контроль защищенности объекта информатизации в соответствии с нормативными документами	З. знание основных способов контроля защищенности объекта информатизации в соответствии с нормативными документами У. умение организовать контроль защищенности объекта информатизации в соответствии с нормативными документами В. владеть навыками контроля защищенности объекта информатизации в соответствии с нормативными документами	выполнение контроля защищенности объекта информатизации в соответствии с нормативными документами	точность контроля защищенности объекта информатизации в соответствии с нормативными документами

3. Шкала оценивания

Результаты любого из видов аттестационных испытаний, включенных в государственную итоговую аттестацию, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично». Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.

Оценка «хорошо». Ответы на поставленные вопросы излагаются, систематизировано и последовательно. Базовые знания используются. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка «удовлетворительно». Допускаются нарушения в последовательности изложения. Неполно раскрываются поставленные вопросы. Демонстрируются поверхностные знания вопроса, а имеющиеся практические навыки с трудом позволяют решать конкретные задачи. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка «неудовлетворительно». Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Не раскрываются все поставленные вопросы. Имеются заметные нарушения норм литературной речи.

4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

Вопросы для подготовки к государственному экзамену

1. Особенности обеспечения информационной безопасности РФ в сфере экономики
2. Особенности обеспечения информационной безопасности РФ в сфере внутренней политики
3. Особенности обеспечения информационной безопасности РФ в сфере внешней политики

4. Особенности обеспечения информационной безопасности РФ в области науки и техники

5. Особенности обеспечения информационной безопасности РФ в сфере духовной жизни

6. Особенности обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах

7. Особенности обеспечения информационной безопасности РФ в сфере обороны

8. Особенности обеспечения информационной безопасности РФ в правоохранительной и судебной сферах

9. Международное сотрудничество РФ в области обеспечения информационной безопасности

10. Основные положения государственной политики обеспечения информационной безопасности РФ

11. Основные функции системы обеспечения информационной безопасности РФ

12. Основные элементы организационной основы системы обеспечения информационной безопасности РФ

13. Угрозы безопасности информации.

14. Система защиты информации.

15. Законодательно – правовые и организационные основы обеспечения защиты информации.

16. Организация защиты информации на предприятии.

17. Политика безопасности предприятия.

18. Структура системы государственного лицензирования.

19. Порядок проведения аттестации и контроля объектов информатизации.

20. Организационные и технические способы защиты государственной тайны.

21. Организационное управление защитой информации.

22. Мероприятия по защите конфиденциальной информации.

23. Законодательство РФ о государственной тайне. Полномочия органов государственной власти и должностных лиц.

24. Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.

25. Порядок засекречивания и рассекречивания сведений и их носителей.

26. Органы защиты ГТ.

27. Порядок допуска к ГТ.

28. Контроль за обеспечением защиты государственной тайны.

29. Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.

30. Организация допуска должностных лиц и граждан к государственной тайне.

31. Система защиты государственной тайны.

32. Организационное управление защитой информации.

33. Организация и порядок проведения специальных экспертиз предприятий.

34. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.

35. Состав и структура системы безопасности предприятия.

36. Правовые основы деятельности службы безопасности.

37. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.

38. Требования внутриобъектового режима.

39. Оценка и управление рисками. Экономическая оценка систем и средств защиты.

40. Организационные методы защиты информации.

41. Технические методы защиты информации от утечки по техническим каналам.

42. Технические методы защиты информации от несанкционированного доступа.

43. Обоснование степени информационной безопасности проектируемых объектов информатизации.

44. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.

45. Специальные проверки технических средств и объектов информатизации.

46. Специальные исследования объектов информатизации.

47. Выбор и оптимизация требуемых средств защиты информации на объектах.

48. Контроль за обеспечением безопасной эксплуатации объектов информатизации.

49. Аттестация объектов информатизации.

50. Идентификация пользователя. Аутендефикация пользователя.

51. Управление доступом.

52. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования.

53. Электронная цифровая подпись.

54. Управление криптоключами.

55. Классификация возможных каналов утечки информации.

56. Технологии зашиты акустической информации от утечки.

57. Технологии зашиты информации от утечки по каналам ПЭМИН.

58. Технологии зашиты видовой информации от утечки.

59. Классификация методов зашиты информации от программно-математических воздействий.

60. Категорирование объектов информатизации.

61. Деятельность администратора безопасности по предотвращению программно-математических воздействий.

62. Основные концепции построения систем управления информационной безопасностью.

63. Основные архитектуры построения систем управления информационной безопасностью.

64. Управление средствами защиты акустической информации.

65. Управление средствами защиты информации, обрабатываемой на ПЭВМ.

66. Аудит состояния информационной безопасности на объектах информатизации.

67. Методы экспертного анализа состояния информационной безопасности на объектах информатизации.

68. Расчетно-аналитические методы анализа состояния информационной безопасности на объектах информатизации.

69. Виды контроля состояния информационной безопасности объектов.

70. Межведомственный контроль состояния информационной безопасности объектов.

71. Ведомственный контроль состояния информационной безопасности объектов.

72. Объектовый мониторинг состояния информационной безопасности.

73. Формы представления результатов контроля информационной безопасности.

74. Методы оценки эффективности мероприятий информационной безопасности.

75. Экспертные методы оценки эффективности систем информационной безопасности.

76. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.

77. Системы централизованного управления безопасностью.

78. Средства управления безопасностью локальных сетей.

79. Продукты для управления безопасностью кампании Cisco и IBM.

80. Модели защиты электронной информации

81. Аналоговая и электронная среда существования документа

82. Аппаратная защита электронного обмена информацией

83. Принципы аппаратной реализации механизмов аутентификации в электронной

84. Интерфейсные средства электронного обмена информацией

85. Техническая реализация аппаратных средств защиты информации

86. Архитектура семейства технических устройств аппаратной защиты информации

87. Аппаратный модуль доверенной загрузки «Аккорд-АМДЗ»

88. Сопроцессор безопасности «Аккорд-СБ»

89. Использование аппаратных средств защиты

90. Применение кодов аутентификации в контрольно-кассовых машинах

91. Система контроля целостности и подтверждения достоверности электронных документов

92. Применение кодов аутентификации в подсистемах технологической защиты информации

93. Управление рисками. Модель безопасности с полным перекрытием

94. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками

95. ISO/IEC 15408. Критерии оценки безопасности информационных технологий

96. Стандарты ISO/IEC 17799/27002 и 27001

97. Методики построения систем защиты информации (Lifecycle Security, Модель многоуровневой защиты, Методика управления рисками, предлагаемая Microsoft)

98. Методики и программные продукты для оценки рисков (CRAMM, FRAP, OCTAVE, RiskWatch).

99. Проведение оценки рисков в соответствии с методикой Microsoft

100. Технические мероприятия по снижению уровня риска

101. Протокол Kerberos

102. Инфраструктура открытых ключей. Цифровые сертификаты

103. Протокол защиты электронной почты S/MIME

104. Протокол IPSec

105. Межсетевые экраны

5. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Методические материалы приведены в приложении 2 к программе государственной итоговой аттестации.

Приложение 2
к программе ГИА

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры ИТиЗИ
Протокол № 8 от «28» марта 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки / специальность

10.03.01 «Информационная безопасность»

Профиль (специализация)
10.03.01.02 "Организация и технология защиты информации"

Уровень образования
бакалавриат

Составитель _____ Скляров А.В., к.т.н., доцент

Ростов-на-Дону, 2018

Оглавление

1. Общие положения

1.1. Государственная итоговая аттестация включает государственный экзамен и защиту выпускной квалификационной работы.

1.2. Государственный экзамен проводится по одной или нескольким дисциплинам и (или) модулям образовательной программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников. Государственный экзамен проводится устно.

1.3. Выпускная квалификационная работа (далее – ВКР) представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

1.4 Вид выпускной квалификационной работы – бакалаврская работа.

2. Методические указания по подготовке к государственному экзамену

Государственный экзамен проводится государственными экзаменационными комиссиями на открытом заседании. Заседания комиссий правомочны, если в них участвуют не менее двух третей от числа лиц, входящих в состав комиссий. Заседания комиссий проводятся председателями комиссий.

Решения комиссий принимаются простым большинством голосов от числа лиц, входящих в состав комиссий и участвующих в заседании. При равном числе голосов председатель комиссии обладает правом решающего голоса.

Результаты любого из видов аттестационных испытаний, включенных в государственную итоговую аттестацию, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично». Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.

Оценка «хорошо». Ответы на поставленные вопросы излагаются, систематизировано и последовательно. Базовые знания используются. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка «удовлетворительно». Допускаются нарушения в последовательности изложения. Неполно раскрываются поставленные вопросы. Демонстрируются поверхностные знания вопроса, а имеющиеся практические навыки с трудом позволяют решать конкретные задачи. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка «неудовлетворительно». Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний

по дисциплине. Не раскрываются все поставленные вопросы. Имеются заметные нарушения норм литературной речи.

Члены ГАК оценивают выпускную квалификационную работу (далее ВКР), исходя из степени раскрытия темы, самостоятельности и глубины изучения проблемы, обоснованности выводов и предложений, а также исходя из уровня сформированности компетенций выпускника, который оценивают руководитель, рецензент и члены ГАК

3. Структура и оформление ВКР

Бакалаврская работа должна представлять собой законченную разработку на заданную тему, написанную лично автором под руководством руководителя ВКР, свидетельствующую об умении автора работать с литературой, обобщать и анализировать фактический материал, используя теоретические знания и практические навыки, полученные при освоении профессиональной образовательной программы по направлению «Бизнес-информатика».

Рекомендуемый объём выпускной квалификационной работы бакалавра от 70 до 100 страниц печатного текста без приложений. Оформление работы должно соответствовать требованиям, изложенным в соответствующих разделах настоящих методических рекомендаций.

Содержание выпускной квалификационной работы бакалавра должно учитывать требования ФГОС ВО направления «Бизнес-информатика» к профессиональной подготовленности студента.

Содержание выпускной квалификационной работы бакалавра включает:

- обоснование выбора предмета исследования и постановку задачи;
- выполненные на основе обзора научно-технической литературы, в том числе с учетом периодических научных изданий;
- теоретическую и (или) экспериментальную части, включающие методы и средства исследований;
- математические модели; расчеты;
- проектную и (или) технологическую части;
- анализ полученных результатов;
- выводы и рекомендации;
- список использованных источников.

Бакалаврская работа должна полностью соответствовать заданию, содержать пояснительную записку, демонстрационный материал в соответствии с требованиями и правилами оформления.

В ходе выполнения бакалаврской работы студент должен изучить достаточный объем отечественной и зарубежной литературы, имеющейся по исследуемой теме (особенно вышедшей в последние годы).

Бакалаврская работа должна проводиться в соответствии с системным подходом и должна включать в себя следующие основные этапы: постановка цели исследования, описание предметной области, анализ предметной

области и выявление проблем, выработка рекомендаций по устранению проблем, организация выполнения и оценка эффективности.

Студент должен продемонстрировать применение теоретических знаний, полученных в процессе обучения:

- использовать математические, информационные модели, методы анализа систем и принятия решений;
- грамотно обосновывать выбор основных решений, например, по функциональной части автоматизированной системы, по комплексу технических средств, по видам обеспечений (программному, техническому, информационному, лингвистическому, организационному), по программным и аппаратным методам обеспечения достоверности и защиты информации и др.

Студент обязан грамотно, четко и ясно, в логической последовательности излагать материал в пояснительной записке.

Оформление выпускной квалификационной работы должно соответствовать требованиям государственных стандартов, в т.ч. и стандартов вуза. Текст работы должен быть набран на белой бумаге формата А4 с одной стороны листа. Размер шрифта: 12-14, интервал:1,3-1,5.

Поля: левое - 30мм, правое – 10мм, верхнее – 15мм, нижнее – 20 мм.

Рекомендуется следующее содержание бакалаврской работы:

- титульный лист;
- реферат на русском языке;
- реферат на иностранном языке;
- задание;
- содержание;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения.

Титульный лист — пример оформления приведен в приложении 1.

Реферат размещается на отдельном листе (приложение 2) и содержит:

- сведения о количестве страниц ВКР, количестве иллюстраций, таблиц, использованных источников, приложений;
- перечень ключевых слов (включает от 5 до 15 слов или словосочетаний из текста ВКР, которые в наибольшей мере характеризуют его содержание);

Основной текст реферата должен быть кратким, точным и отражать:

- объект исследования или разработки;
- цель работы;
- методы и средства исследования;
- полученные результаты и их новизну;
- степень внедрения: рекомендации по внедрению или анализ результатов внедрения, область применения работы;

- экономическую эффективность или социальную значимость работы;
- предположения о развитии результатов исследования.

Если ВКР не содержит сведений по какому-либо из перечисленных пунктов, то и в тексте реферата он соответственно опускается.

Задание. В задании указывается тема бакалаврской работы, сроки принятия к исполнению и сдачи законченной работы, исходные данные, перечень подлежащих разработке вопросов. Задание утверждается заведующим кафедрой, подписывается руководителем работы и студентом (приложение 3).

Содержание. Слово «Содержание» записывается в виде заголовка, симметрично тексту, с заглавной буквы. Нумерация проставляется, начиная с листа «Содержание» (предыдущие листы, включая титульный, подсчитываются, но номер на них не ставится).

Введение. Во введении раскрываются актуальность темы, ее научная новизна и практическая значимость, уровень научной разработки, цели и задачи данного исследования, его предмет и объект; исходные теоретические идеи. Заголовок «Введение», так же как и все последующие заголовки разделов (глав) и подразделов основной части, записывается с абзаца с заглавной буквы.

Основная часть. Текст ВКР включает разделы (главы), подразделы, пункты. Слово «глава» не пишется. *Разделы* нумеруются арабскими цифрами с абзаца. Каждый раздел начинается с новой страницы. *Подразделы и пункты* нумеруют в пределах каждого раздела или подраздела; подпункты – в пределах пункта. Подразделы не следует начинать с новой страницы. Если раздел или подраздел состоит из одного пункта, этот пункт также нумеруется. *Точка* в конце номеров разделов, подразделов, пунктов не ставится.

Заключение должно содержать краткие выводы по результатам выполненной работы, оценку полноты решения поставленных задач, рекомендации по конкретному использованию результатов работы, ее экономическую, научную, социальную значимость. Заголовок «Заключение» записывается с абзаца.

Список использованных источников. Заголовок «Список использованных источников» записывают симметрично тексту с прописной буквы. В список включаются все источники, на которые имеются ссылки в пояснительной записке ВКР. Источники в списке нумеруются в порядке их упоминания в тексте, записываются арабскими цифрами без точки (приложение 4).

Приложения включают материалы иллюстративного и вспомогательного характера (таблицы большого формата; дополнительные расчеты; распечатки и проч.) Приложения обозначаются русскими заглавными буквами - А, Б, В и т.д.(например «Приложение А»), располагаются в виде заголовка, по центру.

Таблицы, рисунки, формулы оформляются в соответствии со внутривузовским стандартом. На все таблицы, рисунки, литературные источники, приложения в тексте должны быть ссылки.

4. Порядок защиты ВКР

Защита выпускной квалификационной работы (далее – ВКР) проводится государственными экзаменационными комиссиями на открытом заседании. Заседания комиссий правомочны, если в них участвуют не менее двух третей от числа лиц, входящих в состав комиссий. Заседания комиссий проводятся председателями комиссий.

Решения комиссий принимаются простым большинством голосов от числа лиц, входящих в состав комиссий и участвующих в заседании. При равном числе голосов председатель комиссии обладает правом решающего голоса.

На представление основных результатов ВКР выпускнику отводится от от 7 до 10 минут. В своем докладе обучающийся раскрывает актуальность выбранной темы, постановка задачи, описание существующих продуктов (решений, технологий); выбор и обоснование методики (методов, способов, инструментальных средств) сравнительного анализа существующих продуктов (решений, технологий); сравнительный анализ достоинств и недостатков существующих продуктов (решений, технологий); разработка рекомендаций по практическому использованию существующих продуктов (решений, технологий), их развитию и модернизации

После выступления выпускник отвечает на вопросы и замечания членов комиссии. Далее слово предоставляется научному руководителю и рецензенту (при наличии); если таковые на защите отсутствуют, то отзыв руководителя и рецензию зачитывают вслух члены комиссии или ее секретарь.

Оценивание ВКР комиссией осуществляется по основным критериям, представленным в табл. 1.

Таблица 1

Критерии оценки ВКР

Критерии	**Отлично**	**Хорошо**	**Удовлетвори тельно**	**Неудовлетво рительно**
Уровень научно-теоретического обоснования темы	Достаточно высокий	Достаточный	Допустимый	Низкий
Структура исследования, соответствие теме и виду дипломной работы	Полностью соответствует	Соответствует	Частично соответствует	Не соответствует
Анализ исследований по проблеме, освещение исторического аспекта, формулирование основных	Достаточно высокий	Достаточный	Допустимый	Низкий

теоретических позиций				
Комплексность использования методов	Полностью обеспечено	Обеспечено	Недостаточно обеспечено	Не обеспечена
Качество оформления (общий уровень грамотности, стиль изложения, наличие иллюстративного материала, соответствие требованиям оформления ВКР)	Полностью соответствует предъявляемым требованиям	В целом соответствует предъявляемым требованиям, но имеются незначительные погрешности	Выполнено с многочисленными ошибками в оформлении, не влияющими на качество полученных результатов	Выполнено с многочисленными ошибками в оформлении, искажающими качество полученных результатов
Качество доклада (ясность, четкость, последовательность и обоснованность изложения)	Соблюден регламент доклада, материал изложен уверенно, без ошибок	Регламент доклада нарушен, материал изложен уверенно, без ошибок	Регламент доклада нарушен, материал изложен неуверенно, с ошибками	Материал изложен с грубыми ошибками, доклад не структурирован
Уровень ответов на вопросы	Получены правильные ответы на все заданные вопросы	Получены правильные ответы на большую часть заданных вопросов	Ответы раскрывают вопросы лишь частично	Ответы на вопросы не получены.
Отзыв научного руководителя	Положительный, без замечаний	Положительный, с незначительными замечаниями	Положительный, с замечаниями	Отрицательный
Оценка рецензента	Положительная, без замечаний	Положительная с незначительными замечаниями	Положительная, с замечаниями	Отрицательная

ПРИЛОЖЕНИЕ 1

ОБРАЗЕЦ ОФОРМЛЕНИЯ ТИТУЛЬНОГО ЛИСТА ВКР

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ (РИНХ)

Наименование факультета (филиала)

Наименование кафедры

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой _____
д.э.н., профессор Фамилия И.О.
«_____» _____ 20__г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
на тему:
«ТЕМА ВКР В СООТВЕТСТВИИ С ПРИКАЗОМ»

Выполнил
студент группы *подпись* *И.О.Фамилия*

Направление *код и наименование направления (специальности)*

Профиль *код и наименование профиля (специализации)*

Руководитель выпускной
квалификационной работы
ученая степень, звание, должность *подпись* *И.О.Фамилия*

Ростов-на-Дону, 20_

ПРИЛОЖЕНИЕ 2

ПРИМЕР ОФОРМЛЕНИЯ РЕФЕРАТА

РЕФЕРАТ

Бакалаврская работа 100 с., 24 рис., 21 табл., 22 источника, 3 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ТЕХНОПАРК, УГРОЗЫ, КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Объектом исследования является выставочно-ярмарочная деятельность ОАО ТМДЦ «Технопарк».

Целью работы является на основе анализа предметной области определить угрозы информационной безопасности, составить план по их минимизации.

Результатом выполнения бакалаврской работы являются проект комплексной системы обеспечения информационной безопасности.

Пояснительная записка содержит описание предметной области и проблемной ситуации, пути решения проблемы, описание функций созданной системы, ее достоинств и недостатков, условий и области применения, обоснование выбранного программно-аппаратного обеспечения.

ПРИЛОЖЕНИЕ 3

ФОРМА ИНДИВИДУАЛЬНОГО ЗАДАНИЯ НА ПРЕДДИПЛОМНУЮ ПРАКТИКУ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Ростовский государственный экономический университет (РИНХ)»
Кафедра Информационных технологий и защиты информации

УТВЕРЖДАЮ
Зав. кафедрой ИТ и ЗИ,
д.э.н., профессор
_____Е.Н. Тищенко
«____» _____ 201 г.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на преддипломную практику

студенту_____
группа_____факультет_____
1.Тема задания_____
2.Вопросы и задачи, подлежащие разработке_____
_____
_____
3.Методы исследования_____
…_____
4.Ориентировочная тема выпускной квалификационной работы: _____
5.Перечень задач и работ на период подготовки ВКР _____

РУКОВОДИТЕЛЬ_____
(должность, место работы, фамилия, имя, отчество)

Задание принял к исполнению
«__»_____20_г._____(подпись студента)

ПРИЛОЖЕНИЕ 4

ПРИМЕР ОФОРМЛЕНИЯ СПИСКА ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Список использованных источников

ПРИЛОЖЕНИЕ 5

ОТЗЫВ

руководителя выпускной квалификационной работы студента

_____

(фамилия, имя, отчество, группа)

Направление подготовки (специальность): _____

Профиль (специализация): _____

Тема ВКР: _____

Актуальность работы.

_____

_____

_____

Отмеченные достоинства.

_____

_____

_____

Отмеченные недостатки.

_____

_____

_____

Работа проверена на наличие заимствований с помощью системы «Антиплагиат ВУЗ».

Дата проверки «___» _____ 20___ г.

По результатам проверки итоговая оценка оригинальности составляет _____ %.

Заимствования объясняются следующими причинами[1]:

_____

_____

_____

Заключение:

_____

_____

_____

Руководитель ВКР_____

(ученая степень, ученое звание, И.О. Фамилия)

Подпись_____ «___»_____ 20__г.

С отзывом ознакомлен_____

Студент:_____(И.О. Фамилия), «____»_____20___г.

[1] Указываются, если итоговая оценка оригинальности не соответствует установленным значениям.