ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ В АСПИРАНТУРУ

по дисциплине

«СПЕЦИАЛЬНАЯ ДИСЦИПЛИНА»

для вступительных испытаний в аспирантуру

группа научных специальностей
2.3 Информационные технологии и телекоммуникации
Научная специальность
2.3.6 Методы и системы защиты информации, информационная безопасность

Форма обучения – очная

Санкт-Петербург
2023

Программа разработана и утверждена на основании приказа Министерства образования и науки Российской Федерации от 06 августа 2021 года № 721 «Об утверждении Порядка приема на обучение по образовательным программам высшего образования – программам подготовки научных и научно-педагогических кадров в аспирантуре».

Порядок проведения вступительных испытаний при поступлении в аспирантуру по группе научных специальностей 2.3 «Информационные технологии и телекоммуникации» по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» регламентируется Правилами приема в Петербургский государственный университет путей сообщения Императора Александра I для поступления на обучение по образовательным программам высшего образования – программам подготовки научных и научно-педагогических кадров в аспирантуре на 2023/2024 учебный год и данной программой.

Программа вступительных испытаний для поступления в аспирантуру по группе научных специальностей 2.3 «Информационные технологии и телекоммуникации» по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

1. Цель и задачи вступительных испытаний

Целью вступительных испытаний для поступления в аспирантуру по группе научных специальностей 2.3 «Информационные технологии и телекоммуникации» по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» является оценка сформированности у поступающего основных исследовательских и аналитических компетенций, позволяющих ему проводить научные исследования и самостоятельно решать профессиональные задачи разных типов и уровня сложности.

Задачи вступительных испытаний:

– Оценить уровень теоретической и практической подготовленности поступающих к обучению в аспирантуре;
– Выявить склонности к научно-исследовательской деятельности;
– Определить область научных интересов.

2. Требования к уровню подготовки поступающих

В аспирантуру по группе научных специальностей 2.3 «Информационные технологии и телекоммуникации» по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» принимаются лица, имеющие образование не ниже высшего образования (специалитет или магистратура).

3. Форма и процедура вступительных испытаний

Вступительные испытания в аспирантуру являются формой проверки профессиональной готовности поступающего к решению комплекса профессиональных задач. Порядок проведения вступительных испытаний при поступлении в аспирантуру регламентируется Правилами приема на

обучение по образовательным программам высшего образования – программам подготовки научно-педагогических кадров в аспирантуре федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I».

Приём на обучение по программам подготовки научно-педагогических кадров в аспирантуре осуществляется по результатам вступительных испытаний, принимаемого экзаменационной комиссией, назначенной приказом Ректора.

Вступительные испытания по специальной дисциплине включают в себя: реферат, экзамен и оценку индивидуальных достижений поступающего в научной деятельности.

Обязательной частью вступительных испытаний является наличие научного реферата по предполагаемой теме диссертационного исследования. Тема научного реферата выбирается самостоятельно выбирается поступающим, из списка, приведенного в соответствующем разделе данной программы, в соответствии с его научными интересами. По выполненному реферату проводится устное собеседование.

Экзамен проводится в письменной форме с устными комментариями по билетам, составленным из основных разделов программы вступительных испытаний. Экзаменационный билет содержит три вопроса.

4. Содержание программы вступительных испытаний

Целью вступительного испытания является определение уровня подготовки и степени сформированности у поступающего в аспирантуру аналитических, исследовательских и профессиональных компетенций, позволяющих вести самостоятельные научные исследования.

Темы рефератов и предполагаемое краткое содержание по научной специальности

Таблица 1 - Темы рефератов

№ п/п	Тема реферата	Рекомендуемое краткое содержание реферата
1	Методология управления информационной безопасностью	Проблема информационной безопасности и защиты информации. Верификационный и риск-ориентированный подходы к обеспечению и управлению информационной безопасностью. Организационно-правовые аспекты и процессная модель управления информационной безопасностью. Автоматизированные средства поддержки системы управления информационной безопасностью.
2	Управление рисками информационной безопасности	Критерии и процессы управления рисками. Методология оценки рисков информационной безопасности. Примеры методов оценки риска, основанных на использовании таблиц. Методики построения систем защиты информации, включающие этап анализа рисков. Методики и

		программные продукты для оценки рисков.
3	Управление инцидентами информационной безопасности	Основные категории инцидентов. Процесс управления инцидентами. Нормативные документы по управлению инцидентами. Процедура управления инцидентами. Модель управления инцидентами. Формальное описание процесса управления инцидентами. Эффект от внедрения процесса управления инцидентами. Средства автоматизации процесса управления инцидентами.
4	Архитектура систем защиты информации	Требования к защите компьютерной информации. Подходы к проектированию систем защиты информации. Оценивание эффективности систем защиты информации при их проектировании. Особенности архитектуры сетевой системы защиты информации.
5	Основы контроля эффективности мер защиты информации	Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Моделирование объектов защиты и угроз безопасности информации. Методы и средства контроля эффективности технической защиты информации. Методы и средства контроля эффективности защиты выделенных помещений от утечки информации по техническим каналам. Методы и средства выявления электронных устройств перехвата информации.

Объем реферата должен составлять не менее 20 стр. машинописного текста на бумаге формата А4. Допускается раскрыть часть вопросов из краткого содержания реферата (таблица 1. Реферат должен представлять собой самостоятельно выполненную оригинальную работу. Степень оригинальности контролируется при помощи системы Антиплагиат.ВУЗ на объем заимствования во время проверки. Реферат должен содержать список использованной литературы). Титульный лист должен быть выполнен в соответствии с приложением 1 к данной программе. Каждая страница подписывается поступающим, в конце указывается общее число страниц текста и ставится подпись поступающего.

Реферат и справка о прохождении объема заимствования предоставляются в печатном виде на вступительный экзамен по специальной дисциплине. Не позднее чем за 24 часа до начала вступительного испытания реферат передается в электронном виде на электронную почту asp@pgups.ru (почта Отдела аспирантуры) в формате pdf. В теме письма указывается «Реферат по специальности 2.3.6. ФИО поступающего». Письмо направляется с почты, указанной для контактов при подаче документов.

Вопросы к экзамену

1. Понятие информации. Классификация информации в зависимости от категории доступа. Основные понятия, цели и задачи обеспечения информационной безопасности и защиты информации.
2. Угрозы информационной безопасности, источники и способы их реализации. Модель нарушителя.
3. Основные меры и методы обеспечения информационной безопасности и защиты информации.
4. Подходы, стратегии и системы обеспечения информационной безопасности.
5. Организационно-правовое обеспечения информационной безопасности РФ и организации (на примере холдинга ОАО «РЖД»)
6. Принципы построения комплексных систем защиты информации корпоративных информационных систем и сетей.
7. Политика безопасности. Понятие и основные положения политики безопасности.
8. Руководящие документы ФСТЭК России по технической защите информации.
9. Основные критерии защищенности автоматизированных систем и требования к мерам защиты информации в государственных информационных системах.
10. Основные понятия и определения криптографии. Классификация криптографических методов. Теоретическая стойкость шифров.
11. Симметричные криптосистемы. Блоковые и потоковые шифры – основные принципы работы, отличия и примеры.
12. Ассиметричные криптосистемы (криптосистемы с открытым ключом) и их стойкость.
13. Криптографические хэш-функции, их свойства и использование. Цифровая подпись.
14. Методы получения случайных последовательностей, их использование в криптографии.
15. Криптографические протоколы. Протоколы распределения ключей. Протоколы аутентификации.
16. Идентификация и аутентификация. Аутентификация на основе паролей. Биометрическая аутентификация.
17. Разграничение доступа. Основные модели управления доступом.
18. Основные механизмы безопасности операционных систем.
19. Методы и механизмы управления параллельностью работы транзакций в СУБД и обеспечения целостности информации в базах данных.
20. Основные механизмы управления учетными записями пользователей, ролями и правами доступа в СУБД.
21. Методы и средства обеспечения информационной безопасности телекоммуникационной сети (на примере одной из корпоративных телекоммуникационных систем ОАО «РЖД»).
22. Методы и средства обеспечения информационной безопасности ERP-системы (на примере корпоративной ERP-системы ОАО «РЖД»).

23. Методы и средства обеспечения информационной безопасности АСУ технологическими процессами (на примере одной из корпоративных информационно-управляющих систем ОАО «РЖД»).

24. Электронные платежные системы. Информационная безопасность электронных платежей.

25. Структура, классификация и характеристики технических каналов утечки информации.

26. Применение помехоустойчивого кодирования в качестве метода защиты информации, его преимущества и недостатки по сравнению с криптографическими методами защиты.

27. Правовые основы защиты информации с использованием технических средств

28. Побочные электромагнитные излучения и наводки (ПЭМИН). Способы защиты от перехвата информации по каналам ПЭМИН.

29. Методы скрытия речевой информации в каналах связи.

30. Анализ безопасности программных и программно-аппаратных средств защиты информации.

5. Учебно-методическое обеспечение подготовки к вступительному испытанию

Перечень литературы, необходимой для подготовки к вступительному испытанию

1. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 440 с.

2. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 448 с.

3. Корниенко А. А., Еремеев М. А., Ададуров С. Е. Средства защиты информации на железнодорожном транспорте (криптографические методы и средства): учебное пособие для студентов вузов железнодорожного транспорта / под ред. проф. А. А. Корниенко. – М.: Маршрут, 2006. - 252 с.

4. Шаньгин В.Ф. Информационная безопасность. – М.: ДМК Пресс, 2014. – 702 с.

5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. - М.: Горячая линия — Телеком, 2013. - 338 с.

6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В и др. Технические средства и методы защиты информации: Учебник для вузов – М.: ООО «Машиностроение», 2009. – 508 с.

7. Хомоненко А. Д., Цыганков В. М., Мальцев М. Г. Базы данных: учебник для высших учебных заведений: в области автоматики, электроники, микроэлектроники и радиотехники при обучении по техническим и экономическим специальностям / под ред. проф. А.Д. Хомоненко. - 5-е изд., доп. - М: Бином-Пресс; СПб: КОРОНА принт, 2006. - 736 с.

8. Олифер В., Олифер Н. Сетевые операционные системы: Учебник для вузов. — СПб.: Питер, 2009. — 669 с.

9. Галатенко В.А. Основы информационной безопасности. – М.: Бином, 2010. - 205 с.

10. Савельев А., Электронная коммерция в России и за рубежом. Правовое регулирование. – М.:Статут, 2014,-544 с.

6. Шкала оценивания и минимальное количество баллов, подтверждающее успешное прохождение вступительных испытаний

Для вступительных испытаний устанавливается шкала оценивания и минимальное количество баллов, подтверждающее успешное прохождение вступительных испытаний.

Вступительные испытания оцениваются по 100-балльной шкале оценивания. Общий балл по результатам вступительных испытаний составляет сумму баллов, выставленных за ответы на экзамене, и баллов, учитывающих индивидуальные достижения поступающего.

Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, – 50 баллов.

Экзамен проводится в письменной форме с устными комментариями по билетам, включающим 3 вопроса. Показатели, критерии и шкала оценивания результатов прохождения вступительных испытаний приведены в таблице.

Таблица 2. - Показатели, критерии и шкала оценивания результатов прохождения вступительных испытаний

№ п/п	Материалы необходимые для оценки знаний, умений и навыков	Показатель оценивания	Критерии оценивания	Шкала оценивания
1	Реферат по специальности	Оригинальность представленного реферата	Оригинальность выше 65%	5
			Оригинальность ниже 65%	0
		Качество текста, обоснованность выводов	Текст логически связан, выводы аргументированы	6-10
			Текст не имеет достаточной логической связи, выводы отсутствуют или доказаны	0-5
		Собеседование по реферату	получены полные ответы на вопросы по теме реферата	6-10
			не получен ответ на вопросы по теме реферата или ответ не раскрыт	0-5
Итого максимальное количество баллов за реферат				**25**

2	Ответ на вопросы экзаменационного билета	Правильность ответа	получен полный ответ на вопрос	16 - 20
			получен достаточно полный ответ на вопрос	11 – 15
			получен неполный ответ на вопрос	5 – 10
			не получен ответ на вопрос или вопрос не раскрыт	0 – 5
		И того максимальное количество баллов за ответ на вопрос		**20***
Итого максимальное количество баллов за 3 вопроса				**60**
3	Индивидуальные достижения поступающего:	Наличие опубликованных трудов в научном издании из перечня ВАК		**10**
		В журналах и сборниках научных трудов индексированных в РИНЦ (в том числе студенческих конференций);		**5**
		Наличие документов, подтверждающих участие занятие призовых мест во Всероссийских студенческих олимпиадах		**5**
Максимальное количество баллов за индивидуальные достижения				**15****
ИТОГО максимальное количество баллов				**100**

Примечание:

* - количество баллов определяется как сумма баллов, определенная каждым членом экзаменационной комиссии, деленная на количество членов экзаменационной комиссии по приему вступительных испытаний.

** - дополнительные баллы начисляются при наличии доказательной базы (копии диплома победителя (призера) конкурса, копии научного издания с опубликованной статьей или тезисами и др.) – баллы суммируются, при этом общее число баллов за индивидуальные достижения поступающего не может превышать 15.

Приложение 1. Образец титульного листа реферата для сдачи вступительных испытаний

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Реферат для сдачи вступительных испытаний в аспирантуру по дисциплине

«Специальная дисциплина»

группа научных специальностей
2.3 Информационные технологии и телекоммуникации
Научная специальность
2.3.6 Методы и системы защиты информации, информационная безопасность

Тема реферата:
«…..».

Выполнил:
Ф.И.О.

_____
(подпись)

«_____»_____2023 г.

Санкт-Петербург
2023