Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет «Высшая школа экономики»

УТВЕРЖДАЮ
Проректор
_____ С.Ю. Рощин

Одобрено на заседании Академического совета
Аспирантской школы по техническим наукам

Согласовано
Академический директор Аспирантской школы
по техническим наукам
_____ И.С. Монахов

Программа вступительного испытания по специальности основной образовательной программы высшего образования – программы подготовки научных и научно-педагогических кадров в аспирантуре
Информационная безопасность

Научная специальность:
2.3.6 Методы и системы защиты информации, информационная безопасность

Москва, 2023

1. Область применения и нормативные ссылки

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета или магистратуры.

2. Структура вступительного экзамена

Вступительное испытание основной образовательной программы высшего образования – программы подготовки научных и научно-педагогических кадров в аспирантуре Информационная безопасность состоит из двух частей: оценки индивидуальных достижений (портфолио) и оценки знаний по направлению подготовки (собеседование).

Максимальная возможная оценка за обе части вступительного испытания по специальности составляет 100 баллов.

Для участия в конкурсе по итогам вступительного испытания по специальности необходимо набрать суммарно не менее 30 баллов. Оценка за вступительное испытание по специальности от 1 до 29 баллов считается неудовлетворительной.

2.1. Оценка индивидуальных достижений. Структура портфолио Максимальная возможная оценка за индивидуальные достижения (портфолио) составляет 50 баллов.

Для участия в конкурсе оценки индивидуальных достижений (портфолио) абитуриент может представить следующие документы, подтверждающие его достижения:

1) **Документы, подтверждающие опыт научно-исследовательской деятельности абитуриента.**

a. Доклады на международных и российских конференциях, научных семинарах, научных школах и т.д. по направлению будущего диссертационного исследования. Подтверждается представлением программы конференции, диплома (сертификата) участника.

b. Опубликованные или принятые к публикации научные работы (статьи, доклады в сборниках докладов). Подтверждается представлением электронных копий подлинников, ссылкой на открытые источники, справкой из редакции о принятии к публикации с обязательным указанием номера журнала и страниц. Публикации должны относиться к тому же направлению, что и тема будущего диссертационного исследования.

c. Свидетельства о государственной регистрации программ и баз данных, патенты на изобретения, патенты на полезные модели, и проч.

d. Участие в научно-исследовательских проектах, академических грантах. Подтверждается данными проекта (название, номер гранта, фонд), контактными данными руководителя проекта и краткой аннотацией (не более 200 слов), разъясняющей суть работы абитуриента.

2) **Рекомендательное письмо** от потенциального научного руководителя планируемого диссертационного исследования, в котором отражено его согласие выступить научным руководителем абитуриента в аспирантуре, а также, при знакомстве потенциального руководителя с научной и учебной деятельностью абитуриента, ее характеристика.

3) **Описание исследовательского проекта** (не более четырех страниц), который поступающий предполагает реализовать во время обучения в аспирантуре (на русском или английском языке). Описание проекта должно содержать:

а) актуальность - краткое введение в область предполагаемого исследования, текущее состояние выбранной отрасли;

б) формулировку проблемы исследования и научную новизну;

в) цели и задачи исследования;

г) обоснование теоретической или практической значимости;

д) краткое описание предполагаемых подходов и методов в решении поставленных

задач.

2.2. Критерии оценки портфолио

Критерий оценки	Количество баллов
Доклады на конференциях	**Максимум 5 баллов**
с публикацией докладов (за каждую)	2 балла
без публикации докладов (за каждую)	1 балл
Публикация научных работ	**Максимум 20 баллов**
Публикация в журнале или в сборнике докладов, индексируемом в Web of Science/Scopus:	
публикация в журнале первого квартиля (Q1) без соавторов	20 баллов
публикация в журнале первого квартиля (Q1) в соавторстве	19 баллов
публикация в журнале второго квартиля (Q2) без соавторов	18 баллов
публикация в журнале второго квартиля (Q2) в соавторстве	17 баллов
публикация в журнале третьего квартиля (Q3) без соавторов	15 баллов
публикация в журнале третьего квартиля (Q3) в соавторстве	14 баллов
публикация в журнале четвертого квартиля (Q4) без соавторов	13 баллов
публикация в журнале четвертого квартиля (Q4) в соавторстве	12 баллов
публикация в журнале без квартиля без соавторов	11 баллов
публикация в журнале без квартиля в соавторстве	10 баллов
Публикация в журнале, входящем в Список D НИУ ВШЭ:*	
без соавторов	12 баллов
в соавторстве	10 баллов
Публикация в журнале или в сборнике докладов, не индексируемом в Web of Science/Scopus:	
Публикация в журнале из списка ВАК без соавторов	8 баллов
Публикация в журнале из списка ВАК в соавторстве	6 баллов
Свидетельства о государственной регистрации программ и баз данных, патенты на изобретения, патенты на полезные модели, и проч.	**5 баллов**

Участие в научно-исследовательских проектах	**5 баллов**
Рекомендательное письмо от потенциального научного руководителя	**5 баллов**
Описание исследовательского проекта	**до 10 баллов**

* Список D НИУ ВШЭ представлен по ссылке: https://scientometrics.hse.ru/list_d

Оценка индивидуальных достижений проводится на собеседовании.

Минимальный балл (неудовлетворительная оценка) за портфолио – до 9 баллов включительно. Для участия в конкурсе по итогам оценки индивидуальных достижений необходимо набрать суммарно не менее 10 баллов.

2.3. Структура и процедура проведения оценки знаний по направлению подготовки (собеседование)

Максимальная возможная оценка за собеседование составляет 50 баллов.

Собеседование состоит из двух частей.

1) Ответ на вопросы в соответствии с направленностью (научной специальностью) будущей научно-исследовательской работы (диссертации). Абитуриент выбирает билет, содержащий два вопроса из представленных в программе собеседования тем.

Абитуриенту предоставляется 30 минут на подготовку. В ходе ответа комиссия может задавать уточняющие вопросы. Оценка за ответы по каждому из вопросов составляет максимум 15 баллов.

2) Беседа по планируемому направлению исследований. Абитуриенту необходимо раскрыть следующие вопросы: предполагаемая тема научно исследовательской работы, формулировка проблемы, цели ее исследования, новизна. В ходе ответа комиссия может задавать уточняющие вопросы. Оценка за данную часть собеседования составляет максимум 20 баллов.

Собеседование проводится на русском или английском языке (по желанию абитуриента), собеседование может проводиться дистанционно с использованием информационных технологий.

2.4. Критерии оценки собеседования

Критерии оценивания ответа по вопросам программы собеседования	**Баллы**
Ответ полный, без замечаний, продемонстрированы знания по специальной дисциплине	14-15
Ответ полный, с незначительными недочетами, продемонстрированы знания по специальной дисциплине	11-13
Ответ полный, с незначительными замечаниями	6-10
Ответ не полный, с существенными замечаниями	3-5
Ответ на поставленный вопрос не дан	0-2

Критерии оценивания ответа по планируемому направлению исследований	Баллы
Ответ полный, без замечаний, продемонстрировано представление о планируемом направлении исследований	20
Ответ полный, с незначительными недочетами, продемонстрировано представление о планируемом диссертационном исследовании	16-19
Ответ полный, с незначительными замечаниями	11-15
Ответ не полный, с существенными замечаниями	7-10
Ответ на поставленный вопрос не дан	0-6

В случае набора абитуриентами равного количества баллов (полупроходного балла), преимущество получает абитуриент, соответствующий перечисленным ниже критериями. Критерии представлены в порядке убывания значимости.

1. оценка за собеседование;
2. оценка за индивидуальные достижения;

3. Программа собеседования

1. Основные принципы современной концепции обеспечения защиты информации. Исходные предположения о возможностях злоумышленника. Требования к защите с позиции пользователя. Основные методы защиты.

2. Роль законодательного и организационного обеспечения защиты информации. Законы Российской Федерации, составляющие основу правовой базы защиты информации в стране. Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав. Порядок лицензирования и сертификации деятельности в области защиты информации.

3. Математические модели формальной теории защиты информации. Угрозы информации и политика безопасности. Классификация систем защиты. Стандарты в области защиты информации в вычислительной системе, «Оранжевая книга» США, российские стандарты.

4. Криптографические методы защиты информации. Основные понятия криптографии. Исторические шифры. Теоретическая, практическая и временная стойкость системы криптографической защиты. Криптографические параметры узлов и блоков шифрующих автоматов. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования. Системы ассиметричного шифрования, открытый ключ, электронная подпись. Вопросы генерации и распределения ключей. Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические. Методология обоснования надежность криптографической защиты.

5. Криптографические протоколы. Криптографические протоколы с использованием симметричного и асимметричного шифрования. Криптографические протоколы с использованием цифровой подписи. Криптографические протоколы генерации и распределения ключей. Протоколы разделения секрета и доказательства без разглашения.

6. Теоретико-числовые методы в криптографии. Оценка сложности арифметических операций. Непрерывные дроби и их свойства, квадратичные вычеты, асимптотический закон распределения простых чисел. Арифметические алгоритмы, (вычисление НОД, Символа Якоби), решение квадратных уравнений

в конечных простых полях, алгоритмы построения и проверки простоты чисел, алгоритмы факторизации и дискретного логарифмирования. Криптосистема RSA, выбор параметров и взаимосвязь между ними.

7. Программно-аппаратные средства обеспечения информационной безопасности. Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Средства обеспечения безопасности в ОС, критерии защищенности ОС. Средства обеспечения безопасности в сетях. Протоколы аутентификации при удаленном доступе. Средства защиты серверов и рабочих станций. Средства защиты локальных сетей при подключении к Internet. Межсетевые экраны, электронные замки, криптофильтры, криптороутеры. Области применения, достоинства, недостатки, реализуемые политики безопасности. Методы оценки качества применяемых средств защиты. Методы и средства защиты информации в СУБД. Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности. Критерии защищенности БД и АИС.

8. Защита информации от технической разведки. Основные физические каналы утечки информации о функционировании информационной системы. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки. Технические параметры современных средств перехвата побочных сигналов. Методы и средства защиты от инженерно-технической разведки. Методика оценки качества инженерно-технической защиты.

9. Особенности защиты информации в вычислительной системе. Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника. Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит). Защита информации в локальных и глобальных вычислительных сетях и ее особенности. Роль и задачи администратора вычислительной системы и службы безопасности.

10. Разрушающие программные воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов. Методы выявления и защиты от вирусов. Изолированные программные среды. Защита программных продуктов от изменения и контроль целостности, защита от изучения.

11. Методика анализа программных реализаций алгоритмов защиты. Методы восстановления алгоритмов защиты в программных продуктах. Оценка уровня криптографической защиты типовых программных продуктов. Анализ особенностей выработки и распределения ключей. Анализ возможности внедрения криптографических закладок. Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.

Список рекомендуемой литературы

1. Кабанов А.С., Лось А.Б., Першаков А.С., Теоретические основы компьютерной безопасности, М: РИО МИЭМ, 2010 г.

2. Девянин П.Н., Ивашко А.М., Першаков А.С., Проскурин В.Г., Черемушкин А.В. Программно-аппаратные средства защиты от НСД к компьютерным криптографическим системам обработки информации (учебное пособие), МИЭМ, 2003.

3. Проскурин В.Г., Защита программ и данных, ИД «Академия», 2011 г. 4. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.

5. Духин А.А. Теория информации (учебное пособие), МИЭМ, 2005 г. 6. Зубов А.Ю. Математики кодов аутентификации // М.:Гелиос АРВ, 2007. 7. Законы РФ «О государственной тайне», «Об информации, информационных

технологиях и защите информации», «О стандартизации». Положения о лицензировании ФСБ и ФСТЭК.

8. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем, М:

горячая линия – Телеком, 2000 г.

9. Фомичев В.М. Дискретная математика и криптология. М.: «Диалог-МИФИ», 2003.

10. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005.

11. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004.

12. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008.

13. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994.

14. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996.

15. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО ТИД ДС, 2002.

16. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему? / Под ред. Д.П. Зегжды и В.В. Платонова. – СПб: Мир и семья, 1997. 17. Мамаев М., Петренко С. Технология защиты информации в Интернете. Специальный справочник. – СПб: Питер, 2002.