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
Протокол № _ от «__» _____ 2017 г.

Согласовано

Академический директор Аспирантской школы
по техническим наукам _____ /Э.С. Клышинский/

Программа вступительного испытания по специальности основной образовательной программы высшего образования – программы подготовки научно-педагогических кадров в аспирантуре по направлению 10.06.01 Информационная безопасность

Москва, 2017

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 научно-педагогических кадров в аспирантуре по направлению 10.06.01 Информационная безопасность состоит из двух частей: оценки индивидуальных достижений (конкурс портфолио) и собеседования.

2.1. Оценка индивидуальных достижений. Структура портфолио

Для участия в конкурсе оценки индивидуальных достижений (портфолио) абитуриент может предоставить следующие документы, подтверждающие его достижения, а также направление будущих исследований:

1. Документы, подтверждающие опыт научно-исследовательской деятельности абитуриента.
    a. Опубликованные или принятые к публикации научные работы (статьи, доклады в сборниках докладов). Подтверждается предоставлением электронных копий подлинников, ссылкой на открытые источники, справкой из редакции о принятии к публикации с обязательным указанием номера журнала и страниц. Публикации должны относится к тому же направлению, что и тема будущего диссертационного исследования.
    b. Доклады на международных и российских конференциях, научных семинарах, научных школах и т.д. по направлению будущего диссертационного исследования. Подтверждается предоставлением программы конференции.
    c. 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. **Предложение будущего направления исследований.** Предложение будущего направления исследований пишется в свободной форме и должно раскрывать следующие вопросы: текущее состояние выбранной отрасли, формулировка проблемы, цели ее исследования, возможные направления исследования, мотивация выбора научного руководителя.

3. **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.

2.2. Критерии оценки портфолио

Максимальная возможная оценка, в соответствии с перечисленными критериями, составляет 50 баллов.

Критерий оценки	**Количество баллов**
Опыт научно-исследовательской деятельности, Участие в конференциях	**Максимум 10 баллов**
с публикацией докладов (за каждую)	до 3 баллов
без публикации докладов (за каждую)	до 1 балла
Опыт научно-исследовательской деятельности, Публикация результатов	**Максимум 20 баллов**
Публикация в издании из списка РИНЦ / один автор (за каждую)	До 2 / до 3 баллов
Публикация в издании из списка ВАК / один автор (за каждую)	До 5 / до 10 баллов
Публикация в иностранном журнале / один автор (за каждую)	До 5 / до 10 баллов
Публикация в издании, входящем в индекс SCOPUS, WoS или аналогичных / один автор (за каждую)	До 10 / до 20 баллов
Свидетельства о государственной регистрации программ и баз данных, патенты на изобретения, патенты на полезные модели, и проч. (за каждую)	5 баллов
Участие в научно-исследовательских проектах (за каждую)	До 5 баллов
Предложение будущего направления исследований	**Максимум 10 баллов**
Рекомендательное письмо от потенциального научного руководителя	**10 баллов**

Оценка индивидуальных достижений проводится до начала собеседования.

Минимальный балл (неудовлетворительная оценка) за портфолио – 14 баллов. Для участия в конкурсе по итогам оценки индивидуальных достижений необходимо набрать суммарно не менее 15 баллов.

2.3. Структура и процедура проведения собеседования

1) Собеседование по вопросам в соответствии с направленностью (научной специальностью) будущей научно-исследовательской работы (диссертации).

Абитуриент получает два вопроса в соответствии с направленностью (научной специальностью) будущей научно-исследовательской работы (диссертации). Ему предоставляется 30 минут на подготовку.

В первой части собеседования абитуриент отвечает на подготовленные им два вопроса из программы собеседования. В ходе ответа комиссия может задавать уточняющие вопросы. Оценка за ответы по каждому из вопросов составляет максимум 15 баллов.

2) Во второй части абитуриент описывает свое видение будущей предметной области. Далее комиссия может задать ему вопросы по поданному предложению будущего направления исследований. 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

Каждый из трех вопросов по профилю оценивается в 20 баллов. Вопрос о планируемом диссертационном исследовании оценивается в 10 баллов.

Критерии оценивания вопроса по профилю	**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 вопроса о планируемом диссертационном исследовании	**Баллы**
Ответ полный, без замечаний, продемонстрировано представление о планируемом диссертационном исследовании	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

Для участия в конкурсе по итогам собеседования необходимо набрать суммарно не менее 15 баллов. Оценка за собеседование от 1 до 14 баллов считается неудовлетворительной.

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

1. оценка за собеседование;
2. оценка за наличие публикаций;
3. оценка за опыт научно-исследовательской деятельности;
4. средний балл в дипломе.

3. Программа собеседования

Для собеседования абитуриент выбирает билет, содержащий вопросы в соответствии с направленностью (научной специальностью) будущей научно-исследовательской работы (диссертации), указанной в заявлении о поступлении в аспирантуру.

Направленность 05.13.19 «Методы и системы защиты информации, информационная безопасность»

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, крипторoутеры. 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.

ЛИТЕРАТУРА

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.
6. Духин А.А. Теория информации (учебное пособие), МИЭМ, 2005 г.
7. Зубов А.Ю. Математики кодов аутентификации // М.:Гелиос АРВ, 2007.
8. Законы РФ «О государственной тайне», «Об информации, информационных технологиях и защите информации», «О стандартизации». Положения о лицензировании ФСБ и ФСТЭК.
9. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем, М: горячая линия – Телеком, 2000 г.
10. Фомичев В.М. Дискретная математика и криптология. М.: “ДИАЛОГ МИФИ”, 2003.
11. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005.
12. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004.

13. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
14. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994.
15. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996.
16. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО ТИД ДС, 2002.
17. 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.
18. Мамаев М., Петренко С. Технология защиты информации в Интернете. Специальный справочник. – СПб: Питер, 2002.
19. Мельников М.М. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997.
20. Першаков А.С. Одна реализация алгоритма гарантированного исключения постоянного влияния на программную среду. // Проблемы информационной безопасности. Компьютерные системы. – 1999.– Т. 1.– с. 56–62.
21. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь. 2000.
22. Петров А.А. Компьютерная безопасность. криптографические методы защиты. – М.: ДМК, 2000.
23. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
24. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М.: Военное издательство, 1992.
25. Трубачев А.П., Егоркин И.В. Общие критерии оценки безопасности информационных технологий. История вопроса // «Защита информации. Конфидент», №2, 2002.