федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

УТВЕРЖДАЮ
Проректор по научно-организационной деятельности
_____Ю.С. Клочков
«14» апрель 2022 г.

ПРОГРАММА

вступительного испытания
по специальной дисциплине

для поступающих на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре

научная специальность
2.3.6 Методы и системы защиты информации, информационная безопасность

Санкт-Петербург
2022

Руководитель ОП

Кандидат технических наук	Е.Ю. Павленко
Составители:	
Доктор технических наук, профессор	Д.П. Зегжда
Доктор технических наук, профессор	М.О. Калинин
Доктор технических наук, доцент	Е.Б. Александрова

Программа рассмотрена и рекомендована к изданию Научно-техническим советом (протокол № 5 от «21» марта 2022 г.).

1. Область применения и нормативные ссылки

Программа вступительного испытания сформирована на основе федеральных государственных требований по программам по программам подготовки научных и научно-педагогических кадров в аспирантуре и порядка приема на обучение по образовательным программам высшего образования - программам подготовки научных и научно-педагогических кадров в аспирантуре.

2. Структура вступительного экзамена

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

Программа содержит перечень тем (вопросов) по специальной дисциплине соответствующей научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Вступительное испытание по специальной дисциплине состоит из двух блоков:

- теоретический экзамен, проводимый очно в письменной и/или устной форме (максимальный балл – 100);
- портфолио (максимальный балл – 100).

Минимальное количество баллов для теоретического экзамена составляет 50 баллов.

При получении по теоретическому экзамену результата ниже минимального балла, портфолио не рассматривается и не суммируется с результатом теоретического экзамена.

2.1.Оценка индивидуальных достижений. Структура портфолио

Максимальная возможная оценка за индивидуальные достижения (портфолио) составляет 100 баллов.

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

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.

Перечень достижений портфолио, учитываемых при приеме на обучение

№ п/п	Индивидуальное достижение	Подтверждающий документ	Количество баллов за каждое достижение
1.	Научные публикации (тематика публикации должна соответствовать научной специальности, по которой поступающий участвует в конкурсе):	Копия статьи с выходными данными журнала, DOI, URL	
	в журналах перечня ВАК;		10
	в журналах индексируемых в Scopus и (или) WoS (в том числе входящих в базу данных RSCI) Q1 или Q2;		25
	в журналах индексируемых в Scopus и (или) WoS (в том числе входящих в базу данных RSCI) Q3 или Q4.		15
2.	Гранты, проекты по выполнению научно-исследовательских и опытно-конструкторских работ, тематика которых соответствует направлению подготовки в конкурсе, по которому участвует поступающий, и в которых он являлся:	Копия подписанного соглашения с грантодателем	
	руководителем		10
	исполнителем		5
3.	Наличие документа, удостоверяющего авторство (соавторство) поступающего на достигнутый им научный (научно-методический, научно-технический, научно-творческий) результат интеллектуальной деятельности:	Копия патента или свидетельства	
	– патент на изобретение;		10
	– патент на полезную модель;		7
	– свидетельство о государственной регистрации программ для ЭВМ;		5
	– свидетельство о государственной регистрации базы данных;		5
	– свидетельство о государственной регистрации топологии интегральных микросхем.		5

№ п/п	Индивидуальное достижение	Подтверждающий документ	Количество баллов за каждое достижение
4.	Публикация в материалах международных и всероссийских научно-технических конференций, включая публикации в выпусках научных журналов, публикующих статьи по итогам конференций (изданиях типа Conference series и(или) Proceedings), проводимых не ранее чем за 2 года, предшествующих приему. Тематика публикации должна соответствовать научной специальности, по которой поступающий участвует в конкурсе:	Копии материалов конференций (тезисов докладов) с приложением титульных листов, DOI, URL (при наличии)	
	за конференцию, индексируемую в базе данных Web of Science и (или) Scopus (индексация сборника или журнала с публикацией подтверждается ссылкой или скриншотом из базы данных).		5
	за прочие конференции.		3
5.	Наличие дипломов победителей мероприятий международного и всероссийского значения, подтверждающие успехи в профессиональной подготовке кандидата для поступления в аспирантуру.	Копия диплома	3

Оценка индивидуальных достижений проводится на собеседовании.

2.2.Структура и процедура проведения теоретического экзамена

Максимальная возможная оценка за теоретический экзамен составляет 100 баллов.

Собеседование состоит из двух частей.

1) Ответ на вопросы в соответствии с 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.

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.

2.3. Перечень тем для теоретического экзамена

1) Безопасность операционных систем.
2) Теоретические основы защиты информации.
3) Модели безопасности информационных систем.

4) Безопасность программного обеспечения.

5) Программно-аппаратные системы обеспечения информационной безопасности.

6) Управление информационной безопасностью.

7) Безопасность современных информационных технологий.

8) Безопасность вычислительных сетей.

9) Криптографические методы защиты информации.

2.4. Перечень вопросов для теоретического экзамена

1) Задачи и проблемы распределенной обработки данных; классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основные сетевые стандарты; неоднородные вычислительные сети.

2) Защита в операционной системе. Проблемы внедрения политики безопасности. Требования к подсистеме взаимодействия с ресурсами для корректного внедрения абстрактной модели безопасности.

3) Информационные модели. Модели невыводимости и невмешательства. Вероятностные модели. Модель системы безопасности с полным перекрытием. Базовая система безопасности Клеменса.

4) Контроль защищенности информации, контроль функционирования механизмов защиты. Адаптивные модели и саморегулирующиеся модели. Динамические методы и алгоритмы противодействия и предупреждения НСД.

5) Криптографические протоколы и методы их анализа. Генераторы псевдослучайных последовательностей. Доказательства с нулевым разглашением. Отечественные стандарты криптографической защиты информации.

6) Методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменения и контроль целостности; методы обфускации программ.

7) Модели дискреционного доступа. Матрица доступа. Пятимерное пространство безопасности Хартстона. Модель Харрисона-Руззо-Ульмана. Способы реализации системы распространения прав.

8) Модели защиты от угрозы отказа в обслуживании. Мандатная модель защиты от угрозы отказа в обслуживании. Модель Миллена распределения ресурсов.

9) Модель Биба и ее вариации. Объединение модели Белла и Лападула с моделью Биба. Модель Кларка-Вилсона. Объединение модели Кларка-Вилсона с моделью Биба.

10) Облачные вычисления, организация внутренней инфраструктуры систем облачных вычислений, использование традиционных средств защиты для систем облачных вычислений, безопасность средств виртуализации.

11) Общая модель управления безопасностью. Макропроцессы управления. Поиск оптимального решения проблемы безопасности. Методы оптимизации управленческих решений.

12) Основные сетевые атаки. Классическая модель системы обнаружения вторжений (СОВ). Требования к СОВ. Информационные преобразования в СОВ. ROC-анализ.

13) Политика безопасности. Неформальное и формальное описание политики безопасности. Понятие монитора безопасности пересылок. TCB системы. Пример TCB системы.

14) Понятие стойкости криптографических алгоритмов. Симметричное и несимметричное шифрование. Цифровая подпись. Задачи, положенные в основу безопасности криптографических алгоритмов.

15) Понятия алгоритма и исчисления. Сложность алгоритма. Основные алгебраические структуры: группа, кольцо, поле. Гомоморфизмы групп и колец. Идеалы и классы вычетов.

16) Программно-аппаратные средства защиты ПЭВМ; методы и средства ограничения доступа к компонентам ЭВМ; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.

17) Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.

18) Простые поля. Расширения полей. Конечные поля. Квадратичные вычеты и невычеты. Квадратичный закон взаимности. Модульное умножение. Проверка чисел и полиномов на простоту. Эллиптические кривые. Закон сложения точек эллиптической кривой.

19) Сигнатурный метод обнаружения атак. Системы автоматического создания сигнатур. Методы выявления аномалий. Применение методов Data Mining для выявления аномалий.

20) Современное состояние проблемы информационной безопасности. Причины нарушения безопасности. Основные направления создания информационных систем.

21) Современные технологии защиты ресурсов от программных атак. Комплекс средств защиты и управления безопасностью. Задача управления безопасностью. Обобщенная структура системы управления защитой информации, ее компоненты. Элементы теории управления информационной безопасностью.

22) Состав и правила взаимодействия компонент в подсистеме обеспечения безопасности. Аппаратные средства защиты современных процессоров и материнских плат.

23) Сравнение выразительной мощности моделей контроля доступа. Подсистема идентификации - аутентификации. Подсистема аудита и подсистема обнаружения нарушителя.

24) Средства обеспечения защиты информации в СУБД; средства идентификации и аутентификации объектов баз данных, управление доступом; причины, виды, основные методы нарушения конфиденциальности в СУБД.

25) Типовая структура подсистемы безопасности ОС и выполняемые ей функции; реализация подсистем безопасности; домены безопасности; критерии защищенности ОС; средства защиты от атак переполнения буфера.

26) Типовые удаленные воздействия на распределенные вычислительные системы, понятие удаленной атаки. Причины успеха удаленных воздействий на распределенные вычислительные системы Принципы создания защищенных систем связи в распределенных вычислительных системах.

27) Троянские кони. Уровни безопасности. Секретность и степень доверия. Мандатная модель доступа. Модель Белла и Лападула. Критика модели Белла и Лападула.

28) Угрозы безопасности. Классификация источников, характеров и механизмов угроз. Классификация уязвимостей и мер защиты.

29) Управление рисками информационной безопасности. Этапы процесса управления рисками. Оценка рисков. Определение уязвимостей. Определение рисков. Качественные и количественные методы.

30) Цикл управления безопасностью: анализ систем, реализация, контроль, оценка безопасности. Непрерывность обеспечения безопасности.

2.5. Критерии оценки теоретического экзамена

Оценка знаний поступающего в аспирантуру производится по сто бальной шкале.

100 баллов выставляется экзаменационной комиссией за обстоятельный и обоснованный ответ на все вопросы экзаменационного билета и дополнительные вопросы

членов экзаменационной комиссии. Поступающий в аспирантуру в процессе ответа на вопросы экзаменационного билета правильно определяет основные понятия, свободно ориентируется в теоретическом и практическом материале по предложенной тематике.

75 баллов выставляется поступающему в аспирантуру за правильные и достаточно полные ответы на вопросы экзаменационного билета, которые не содержат грубых ошибок и неточностей в трактовке основных понятий и категорий, но в процессе ответа возникли определенные затруднения при ответе на дополнительные вопросы членов экзаменационной комиссии.

50 баллов выставляется поступающему в аспирантуру при недостаточно полном и обоснованном ответе на вопросы экзаменационного билета и при возникновении серьезных затруднений при ответе на дополнительные вопросы членов экзаменационной комиссии.

0 баллов выставляется в случае отсутствия необходимых для ответа на вопросы экзаменационного билета теоретических и практических знаний.

2.6.Список рекомендуемой литературы

1) Зегжда П.Д. и др. От информационной безопасности к кибербезопасности. Опыт научно-исследовательских работ и подготовки кадров в Санкт-Петербургском политехническом университете Петра Великого: Санкт-Петербург: Изд-во Политехн. унта, 2017.

2) Зегжда П.Д., Калинин М.О. Управление безопасностью компьютерных систем: Санкт-Петербург: Изд-во Политехн. ун-та, 2012.

3) Александрова Е.Б., Павленко Е.Ю., Шенец Н.Н. Криптографические методы защиты информации: Санкт-Петербург: Изд-во Политехн. унта, 2016.

4) Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом: Санкт-Петербург: Мир и Семья, 2001.

5) Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности: Санкт-Петербург: Изд-во СПбГПУ, 2004.

6) Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем: Москва: Горячая линия - Телеком, 2000.

7) Калинин М.О. Теория и системы управления информационной безопасностью. Анализ рисков информационной безопасности: лабораторный практикум. Санкт-Петербург: Изд-во Политехн. ун-та, 2010.

8) Калинин М.О., Коноплев А.С. Безопасность современных высокопроизводительных систем .Ч. 3. Грид-системы: лабораторный практикум. Санкт-Петербург: Изд-во Политехн. ун-та, 2013.

Приложение

Сведения об достижениях портфолио кандидата для поступления по программам подготовки научных и научно-педагогических кадров в аспирантуре СПбПУ

_____ (Ф.И.О. кандидата для поступления в аспирантуру)			
_____ (научная специальность)			
№ п/п	**Индивидуальное достижение**	**Количество баллов за каждое достижение**	**Рейтинговая оценка показателя, общий балл**
1.	Научные публикации (тематика публикации должна соответствовать научной специальности, по которой поступающий участвует в конкурсе): в журналах перечня ВАК;	10	
	в журналах индексируемых в Scopus и (или) WoS (в том числе входящих в базу данных RSCI) Q1 или Q2;	25	
	в журналах индексируемых в Scopus и (или) WoS (в том числе входящих в базу данных RSCI) Q3 или Q4.	15	
2.	Гранты, проекты по выполнению научно-исследовательских и опытно-конструкторских работ, тематика которых соответствует направлению подготовки в конкурсе, по которому участвует поступающий, и в которых он являлся: руководителем,	10	
	исполнителем.	5	
3.	Наличие документа, удостоверяющего авторство (соавторство) поступающего на достигнутый им научный (научно-методический, научно-технический, научно-творческий) результат интеллектуальной деятельности: – патент на изобретение;	10	
	– патент на полезную модель;	7	
	– свидетельство о государственной регистрации программ для ЭВМ;	5	
	– свидетельство о государственной регистрации базы данных;	5	
	– свидетельство о государственной регистрации топологии интегральных микросхем.	5	
4.	Публикация в материалах международных и всероссийских научно-технических конференций, включая публикации в выпусках научных журналов, публикующих статьи по итогам конференций (изданиях типа Conference series и(или) Proceedings), проводимых не ранее чем за 2 года, предшествующих приему (тематика публикации должна соответствовать научной специальности, по которой поступающий участвует в конкурсе): за конференцию, индексируемую в базе данных Web of Science и (или) Scopus (индексация сборника или журнала с публикацией подтверждается ссылкой или скриншотом из базы данных);	5	
	за прочие конференции.	3	
5.	Наличие дипломов победителей мероприятий международного и всероссийского значения, подтверждающие успехи в профессиональной подготовке кандидата для поступления в аспирантуру	3	
Суммарный рейтинговый балл			

Кандидат в аспирантуру _____ _____
(подпись) *(Ф.И.О).*

Предполагаемый научный руководитель _____ _____
(подпись) *(Ф.И.О).*

Руководитель образовательных программ
по аспирантуре института _____ _____
(подпись) *(Ф.И.О).*