

УТВЕРЖДЕНА

заместитель директора
по образовательной деятельности
АНОО ВО «Университет «Сириус»

О. Д. Федоров

_____ 2026 г.



ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

для поступающих на обучение по образовательной программе
высшего образования – программе подготовки научных и научно-педагогических
кадров в аспирантуре по научной специальности

2.3.6. Методы и системы защиты информации, информационная безопасность

СОГЛАСОВАНО:

Руководитель группы научного центра
информационных технологий и
искусственного интеллекта

А.С. Петренко

Руководитель приёмной комиссии

Б. Е. Кадлубович

Федеральная территория «Сириус»

2026

ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительных испытаний предназначена для лиц, поступающих на обучение по образовательной программе высшего образования – программе подготовки научных и научно-педагогических кадров в аспирантуре по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (далее – образовательная программа).

В программу вступительных испытаний включено описание форм и процедур вступительных испытаний, представлено содержание тем и критерии оценки.

Вступительные испытания проводятся в следующей форме:

- письменный экзамен;
- резюме;
- исследовательское предложение.

Письменное вступительное испытание оценивается по 30-балльной шкале. Резюме и исследовательское предложение оцениваются по 10-балльной шкале. Язык проведения письменного экзамена – русский, материалы резюме и исследовательского предложения принимаются на русском языке.

Проведение вступительных испытаний осуществляется с применением дистанционных технологий.

Продолжительность письменного экзамена: 120 минут.

1. Цель и задачи вступительных испытаний

Цель проведения вступительных испытаний – отбор наиболее подготовленных поступающих на обучение по образовательной программе 2.3.6. Методы и системы защиты информации, информационная безопасность, в том числе определение уровня их готовности к самостоятельной научной и проектной деятельности.

Основные задачи вступительных испытаний:

- выявление и оценка уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций поступающего;
- определение уровня готовности к работе и проектной деятельности в компаниях и на производствах и, а также научно-исследовательской деятельности в рамках НИОКР;
- выяснение познавательной и мотивационной сферы поступающего;
- выявление научных и профессиональных интересов;
- определение уровня научно-технической эрудиции и языковой подготовки поступающего;
- выяснение опыта и готовности работы в рамках проектной деятельности в компаниях и на производствах.

Целью вступительных испытаний является проверка следующих знаний и умений:

- знание основ высшей математики: математического анализа, линейной алгебры и аналитической геометрии, теории функций комплексного переменного, теории обыкновенных дифференциальных уравнений, математической логики, алгебры, теории чисел, дискретной математики;
- знание основ теорий защиты информации и обеспечения информационной безопасности: методы защиты информации и языков программирования Python и C++;
- владение навыками чтения научной литературы (на русском и английском языках) и базовыми инструментами поиска научной информации, в том числе в сети «Интернет».

2. Содержание вступительных испытаний

2.1. Общие вопросы

1. Функции алгебры логики. Реализация их формулами. Совершенная дизъюнктивная нормальная форма.
2. Язык логики высказываний. Булевы функции. Исчисление высказываний, его непротиворечивость и полнота.
3. Непрерывность функций одной переменной, свойства непрерывных функций.
4. Функции многих переменных, полный дифференциал и его геометрический смысл. Достаточные условия дифференцируемости. Градиент.
5. Определенный интеграл. Интегрируемость непрерывной функции. Первообразная непрерывной функции.
6. Неявные функции. Существование, непрерывность и дифференцируемость неявных функций.
7. Числовые ряды. Сходимость рядов. Критерий сходимости Коши. Достаточные признаки сходимости (Коши, Даламбера, интегральный, Лейбница).
8. Абсолютная и условная сходимость ряда. Свойства абсолютно сходящихся рядов. Перестановка членов ряда. Теорема Римана. Умножение рядов.
9. Ряды и последовательности функций. Равномерная сходимость. Признак Вейерштрасса. Свойства равномерно сходящихся рядов (непрерывность суммы, почленное интегрирование и дифференцирование).
10. Степенные ряды в действительной и комплексной области. Радиус сходимости. Теорема Коши-Адамара. Теорема Абеля. Свойства степенных рядов (почленное интегрирование, дифференцирование). Разложение элементарных функций.
11. Несобственные интегралы и их сходимость. Равномерная сходимость интегралов, зависящих от параметра. Свойства равномерно сходящихся интегралов.
12. Ряды Фурье. Достаточные условия представимости функции рядом Фурье.
13. Линейные пространства, их подпространства. Базис. Размерность. Теорема о ранге матрицы.

14. Система линейных уравнений. Геометрическая интерпретация системы линейных уравнений. Фундаментальная система решений системы однородных линейных уравнений. Теорема Кронекера - Капелли.
15. Билинейные и квадратичные функции и формы в линейных пространствах и их матрицы. Приведение к нормальному виду. Закон инерции.
16. Линейные преобразования линейного пространства, их задание матрицами. Характеристический многочлен линейного преобразования. Собственные векторы и собственные значения, связь последних с характеристическими корнями.
17. Евклидово пространство. Ортонормированные базисы. Ортогональные матрицы. Симметрические преобразования. Приведение квадратичной формы к главным осям.
18. Группы, подгруппы, теорема Лагранжа. Порядок элемента. Циклические группы, факторгруппа. Теорема о гомоморфизмах.
19. Аффинная и метрическая классификация кривых и поверхностей второго порядка. Проективная классификация кривых.
20. Дифференциальное уравнение первого порядка. Теорема о существовании и единственности решения.
21. Линейное дифференциальное уравнение второго порядка. Линейное однородное уравнение. Линейная зависимость функций. Фундаментальная система решений. Определитель Вронского. Линейное неоднородное уравнение.
22. Линейное дифференциальное уравнение с постоянными коэффициентами: однородное и неоднородное.
23. Функции комплексного переменного. Условия Коши - Римана. Геометрический смысл аргумента и модуля производной.
24. Элементарные функции комплексного переменного и даваемые ими конформные отображения. Простейшие многозначные функции. Дробно-линейные преобразования.
25. Теорема Коши об интеграле по замкнутому контуру. Интеграл Коши. Ряд Тейлора.
26. Ряд Лорана. Полус и существенно особая точка. Вычеты.

27. Аксиоматическая теория множеств. Парадоксы наивной теории множеств. Аксиома выбора. Вполне упорядоченные множества и теорема Цермело. Лемма Цорна.
28. Функции алгебры логики. Полнота в алгебре логики, критерий полноты Поста.
29. Общее понятие алгоритма. Вариант формализации понятия алгоритма. Универсальный алгоритм. Вычислимые функции, перечислимые и разрешимые множества. Теорема Гёделя о неполноте. Неразрешимость формальной арифметики.
30. Время и память как меры сложности вычислений. Классы P, NP, PSPACE. Полиномиальная сводимость. NP-полные проблемы.
31. Графы, деревья. Основные свойства деревьев.
31. Планарность графов, теорема Эйлера. Критерий планарности Понтрягина-Куратовского.
33. Конечные автоматы, эксперименты с автоматами, теорема Мура.
34. Машины Тьюринга и рекурсивные функции, совпадение классов частично рекурсивных функций и функций, вычислимых на машинах Тьюринга.
35. Линейные операторы линейного пространства, их задания матрицами. Характеристический многочлен линейного оператора. Собственные векторы и собственные значения, связь последних с характеристическими корнями. Теорема Гамильтона-Кэли. Жорданова нормальная форма линейного оператора.
36. Евклидово пространство. Ортонормированные базисы. Ортогональные и самосопряженные линейные операторы, их матрицы. Приведение квадратичной формы к главным. Перестановки. Симметрическая группа перестановок. Теорема Кэли о конечных группах.
37. Группы, подгруппы, теорема Лагранжа. Факторгруппа. Теорема о гомоморфизмах для групп. Порядок элемента. Циклические группы. Коммутант группы, разрешимые группы. Классы сопряженности, центр группы. Действие групп на множестве, стабилизаторы, орбиты.
38. Кольца, поля. Кольцо многочленов. Деление с остатком многочленов над полем, алгоритм Евклида. Неприводимые многочлены над полем, критерий

неприводимости многочленов степени 2 и 3, разложение многочлена над полем в произведение неприводимых многочленов.

39. Алгоритм Евклида поиска наибольшего общего делителя целых чисел. Решение линейных уравнений в целых числах.

40. Мультипликативные функции. Функция Мёбиуса, формула обращения Мёбиуса. Формулы для количества и для суммы делителей. Функция Эйлера и её свойства.

41. Символ Лежандра. Квадратичный закон взаимности. Символ Якоби и его вычисление.

42. Представление чисел цепными дробями. Теорема Дирихле о приближении действительных чисел рациональными. Цепные дроби квадратичных иррациональностей.

43. Конечные поля и их расширения. Цикличность мультипликативной группы конечного поля. Автоморфизм Фробениуса, группа Галуа для конечных полей.

44. Характеры абелевых групп. Двойственная группа, свойства ортогональности. Аддитивные и мультипликативные характеры конечного поля. Суммы Гаусса.

45. Вариационное исчисление: вариация функционала, вариационная производная (первая вариационная производная, вариации и вариационные производные второго и высших порядков), вариационная задача.

2.2. Специальные вопросы

1. Математический аппарат для криптографии. Модульная арифметика. Теорема Эйлера и малая теорема Ферма. Китайская теорема об остатках. Решение полиномиальных сравнений по простому модулю. Расширенный алгоритм Евклида, арифметика в конечных полях. Эллиптические кривые в криптографии

2. Первообразные корни. Существование первообразных корней по простому модулю p , модулям p^k , $2p^k$, $k > 1$. Индексы и их свойства.

3. Методы защиты информации. Организационные, технические, программно-аппаратные и криптографические средства защиты информации.

4. Криптографические алгоритмы. Симметричное и асимметричное шифрование. Алгоритмы формирования электронной цифровой подписи. Квантовая и постквантовая криптография.

Классификация вредоносных программ. Классические определения четырех основных типов вредоносных программ. Методы борьбы с вредоносными программами.

Риск информационной безопасности: понятие, задача управления рисками, методологические основы и инструментальные средства оценки рисков информационной безопасности.

3. Демонстрационный вариант письменного экзамена

Вопрос 1. Теорема Коши об интеграле по замкнутому контуру. Интеграл Коши. Ряд Тейлора.

Вопрос 2. Сигнатурные методы обнаружения вторжений и аномальной активности. Алгоритмы статистического анализа регистрационной информации.

Вопрос 3. Разложить функцию $y = (1+x) e^{-x}$ в ряд Маклорена. Определить радиус сходимости ряда. Ответ обосновать.

Вопрос 4. Решите сравнение: $31x^4 + 57x^3 + 96x + 191 = 0 \pmod{225}$.

4. Требования к оформлению резюме

Резюме, самостоятельно составленное поступающим, должно быть предоставлено на русском языке, объем – не менее 1 и не более 5 машинописных страниц, шрифт Times New Roman прямого начертания, кегль (размер) шрифта 12, междустрочный интервал – полуторный.

Резюме должно содержать:

- 1) Личную информацию и контактные данные поступающего;
- 2) Фотографию поступающего;
- 3) Сведения об имеющемся у поступающем образовании;
- 4) Опыт работы поступающего;
- 5) Результаты общественной, научной и профессиональной деятельности поступающего (членство в объединениях, организация, опыт волонтерской деятельности, участие в НИР, грантах, значимых проектах);
- 6) Ключевые индивидуальные достижения поступающего;
- 7) Сведения о квалификации и имеющихся у поступающего практических навыках;
- 8) Сведения об уровне владения иностранными языками;
- 9) Список публикаций и объектов интеллектуальной собственности (при наличии);
- 10) Информация о выпускной квалификационной (научно-исследовательской) работе поступающего (тема, кратка аннотация, объемом не более 200 слов);
- 11) Информация о хобби и увлечениях поступающего.

Допускается приводить названия публикаций, грантов, проектов, сертификатов на языке, использованном в оригинале. Перевод в этом случае не обязателен.

При оценке резюме экзаменационная комиссия учитывает индивидуальные достижения, подтвержденные документами, приложенными к заявлению о приеме, в соответствии с пунктом 3.17 Правил.

Максимальная оценка за резюме – 10 (десять) баллов, минимальная – 6 (шесть) баллов.

5. Требования к оформлению исследовательского предложения

Исследовательское предложение должно быть составлено поступающим самостоятельно на русском языке, рекомендуемый объем - не менее 2 и не более 5 страниц, шрифт Times New Roman прямого начертания, кегль (размер) шрифта 12, междустрочный интервал - полуторный. Примерная форма исследовательского предложения:

Исследовательское предложение по теме научного исследования

(наименование темы)

Я, _____, хочу принять участие в конкурсе на обучение по образовательной программе высшего образования – программе подготовки научных и научно-педагогических кадров

в аспирантуре АНОО ВО «Университет «Сириус» по научной специальности:

_____ (далее – программ аспирантуры).

Выбор обозначенной программы аспирантуры обусловлен (указать причины, которые побудили принять решение о выборе именно этой научной специальности и темы научного исследования; почему выбран именно АНОО ВО «Университет «Сириус», что знаете о нем, о научном центре (коллективе), реализующем соответствующую программу аспирантуры, об их достижениях и направлениях исследований, о лабораторном комплексе АНОО ВО «Университет «Сириус», о федеральной территории «Сириус»);

Необходимо:

- 1) провести оценку актуальности выбранной научной специальности, состояния и перспективы проведения научного исследования по выбранной тематике в рамках обучения в Университете и для страны в целом;
- 2) раскрыть предложения, которые планируется реализовать в рамках научного исследования и предполагаемые результаты, которых планирует достичь;
- 3) указать каким образом поможет имеющийся научный и (или) практический опыт и планы на будущее, при условии успешного завершения аспирантуры.

_____ / _____ / « _____ » _____ 20 _____ г.

Максимальная оценка за исследовательское предложение-10 (десять) баллов,
минимальная - 7 (семь) баллов

6. Литература для подготовки к вступительным испытаниям

а. Основная

1. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления: в 3 т. — 18-е изд. — Санкт-Петербург: Лань, 2024
2. Практикум по дискретной математике : учебное пособие / Н. Ю. Василенко, Н. Е. Дегтярева, И. В. Плаксина, П. В. Зиновьев. — Казань : Бук, 2022. — 80 с.
3. Васильева И.Н. Развитие квантовых технологий и квантовая угроза современной криптографии // Проблемы информационной безопасности в киберпространстве: монография. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2024. – С. 108 – 118.
4. Курош А. Г. Курс высшей алгебры. – 26-е изд. – Санкт-Петербург: Лань, 2025.
5. Гнидко К. О. Квантовоподобные феномены распространения коллективных эмоций в социальных сетях: модель, набор данных и результаты экспериментального исследования / К. О. Гнидко, Д. Н. Лисов // Правовая информатика. – 2025. – № 2. – С. 79–94.
6. Дехтярь М.И. Лекции по дискретной математике: учебник / М.И. Дехтярь, С.М. Дудаков, Б.Н. Карлов. – 3-е изд., испр. и доп. – Тверь: Тверской государственный университет, 2021. – 528 с.
7. Еловская М.А. Кибербезопасность и защита данных: вызовы цифрового мира // Актуальные направления научных исследований XXI века: теория и практика. – 2025. – Т. 13, № 1(68). – С. 117–127.
8. Ларина М.В. Модель цифровой платформы для анализа устойчивости к квантовым угрозам / М.В. Ларина, В.Ю. Скиба // Правовая информатика. – 2025. – № 3. – С. 12–26.

9. Ларина М.В. О классификации угроз информационных систем в условиях развития квантовых технологий / М.В. Ларина, В.Ю. Скиба // Правовая информатика. – 2026. – № 1. – С. 5–15.
10. Лившиц К.И. Курс линейной алгебры и аналитической геометрии: учебник для вузов. – 3-е изд., стер. – Санкт-Петербург: Лань, 2023. – 508 с.
11. Тенденции повышения уязвимости современных информационных систем со стороны квантовых компьютеров / А.В. Лукашев, В.В. Шабуня, В.С. Сарафанников [и др.] // Известия Тульского государственного университета. Технические науки. – 2023. – № 11. – С. 324–331.
12. Петренко А.С. Метод оценивания квантовой устойчивости блокчейн-платформ / А.С. Петренко, С.А. Петренко // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 2–22.
13. Платонов В.В. Методы обнаружения сетевых атак. Технологии машинного обучения в кибербезопасности: учебное пособие для студентов высших учебных заведений, обучающихся по УГСН 10.00.00 «Информационная безопасность» по программам подготовки бакалавров, магистров, специалистов. – Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого, 2022. – 85 с.
14. Родионов А.А. Введение в вариационное исчисление: учебное пособие / А.А. Родионов, В.А. Коршунов, Д.А. Пономарев. – Санкт-Петербург: Санкт-Петербургский государственный морской технический университет, 2022. – 138 с.
15. Adversarial attacks on machine learning cybersecurity defences in industrial control systems / E. Anthi, L. Williams, M. Rhode, P. Burnap, A. Wedgbury // Journal of Information Security and Applications. – 2021. – Vol. 58. – P. 102717.
16. Gnidko K. Quantum-Like Phenomena in the Spread of Collective Emotions in Social Networks: Model, Experiment, and Dataset / K. Gnidko, I. Vasilenko // Proceedings of the Ninth International Scientific Conference «Intelligent Information

Technologies for Industry» (IITI'25), Volume 1 / ed. by S. Kovalev, I. Kotenko, A. Sukhanov. – Cham: Springer, 2025. – P. 352–361. – (Lecture Notes in Networks and Systems; vol. 1762).

17. Potential Vulnerabilities of Cryptographic Primitives in Modern Blockchain Platforms / E. A. Ishchukova, S. A. Petrenko, K. O. Gnidko, A. V. Nekrasov // Sci. – 2025. – Vol. 7, No. 3.

18. Quantum optimal control – quantum stochastic master equation as model background Introduction and pedagogical Benchmarks / R.Yu. Kapkov, S.V. Ulyanov, S.A. Petrenko, V.Yu. Skiba, M.V. Shiryaev // Системный анализ в науке и образовании. – 2025. – № 3. – P. 52–100.

19. Skiba V. Yu. Education system of engineers and scientific personnel in the sphere of quantum information technologies, quantum robust artificial intelligence and quantum resilience / V. Yu. Skiba, S. A. Petrenko, E. M. Abakumov // Computing, Telecommunications and Control. – 2025. – Vol. 18, No. 4. – P. 44–52.

20. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security / V. Yu. Skiba, S. A. Petrenko, K. O. Gnidko, A. S. Petrenko // Computing, Telecommunications and Control. – 2025. – Vol. 18, № 2. – P. 56–73.

21. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity / V.Yu. Skiba, S.A. Petrenko, A.A. Murzina, K.R. Popova // Computing, Telecommunications and Control. – 2024. – Vol. 17, № 4. – P. 16–34.

в. Дополнительная

1. Боровских А.В. Лекции по обыкновенным дифференциальным уравнениям: учебник / А.В. Боровских, А.И. Перов. – 2-е изд., испр. и доп. – Воронеж: Воронежский государственный университет, 2013. – 548 с.

2. Бухштаб А.А. Теория чисел: учебное пособие. – 3-е изд., стер. – Санкт-Петербург [и др.]: Лань, 2008.
3. Винберг Э.Б. Курс алгебры. – Москва: МЦНМО, 2011. – 592 с.
4. Данеев О.В. О проблеме квантового распределения ключей: состояние и перспективы // Хроноэкономика. – 2020. – № 2 (23). – С. 19–23.
5. Кострикин А.И. Линейная алгебра и геометрия: учебное пособие / А.И. Кострикин, Ю.И. Манин. – 4-е изд., стер. – Санкт-Петербург: Лань, 2008.
6. Скиба В.Ю. Основы информационной безопасности предпринимательской деятельности / В. Ю. Скиба, Т. Г. Садовская, В. А. Дадонов. – Москва: МГТУ им. Н. Э. Баумана, 2004. – 51 с.
7. Основы квантовых вычислений: учебное пособие / С.Н. Торгаев, И.Д. Шульга, Е.А. Юрченко, М. Л. Громов. – Томск: СТТ, 2020. – 88 с.
8. Обеспечение безопасности информации в центрах управления полетами космических аппаратов / Л.М. Ухлинов, М.П. Сычев, В.Ю. Скиба, О.В. Казарин. – Москва: МГТУ им. Н. Э. Баумана, 2000. – 364 с.
9. Шабат Б.В. Введение в комплексный анализ: учеб. для студентов ун-тов, обучающихся по специальностям «Математика», «Механика»: в 2 ч. – 4-е изд., стер. – Санкт-Петербург: Лань, 2004. – 21 с.

с. Цифровые образовательные ресурсы

1. Общероссийский портал Math-Net.Ru <https://www.mathnet.ru/> — Современная информационная система, предоставляющая российским и зарубежным ученым различные возможности в поиске научной информации по математике, физике, информационным технологиям и смежным наукам.
2. Электронный ресурс arXiv <https://arxiv.org/> — Крупнейшим бесплатный архив электронных научных публикаций по разделам физики, математики, информатики,

механики, астрономии и биологии. Имеется подробный тематический каталог и возможность поиска статей по множеству критериев.