

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)**

УТВЕРЖДАЮ

Директор АНОО ВО «Университет «Сириус»



Л.Г. Кирьянова

» 2024 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

для поступающих на обучение по образовательной программе
высшего образования – программе магистратуры

«Разработка и управление критической информационной инфраструктурой»
по направлению подготовки 09.04.01 Информатика и вычислительная техника

СОГЛАСОВАНО:

Заместитель директора
по образовательной деятельности

Е.В. Саврук

Исполнительный директор
Научного центра информационных технологий
и искусственного интеллекта

М.В. Ширяев

Руководитель
Приемной комиссии

Б.Е. Кадлубович

Федеральная территория «Сириус», 2024

ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительных испытаний предназначена для лиц, поступающих на обучение по образовательной программе высшего образования – программе магистратуры «Разработка и управление критической информационной инфраструктурой» по направлению подготовки 09.04.01 Информатика и вычислительная техника (далее – образовательная программа).

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

Цель проведения вступительных испытаний – отбор наиболее подготовленных поступающих на обучение по образовательной программе, 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 научно-исследовательской и проектной деятельности, работе в составе научно-исследовательских коллективов;
- выяснение познавательной и мотивационной сферы поступающего;
- выявление научных интересов;
- определение уровня научно-технической эрудиции и языковой подготовки поступающего.

Вступительные испытания проводятся в форме письменного экзамена и собеседования. Каждое вступительное испытание оценивается по стобалльной шкале. Язык (языки) проведения письменного экзамена – русский, собеседования – русский и английский.

Проведение вступительных испытаний осуществляется с применением дистанционных технологий.

Продолжительность письменного экзамена: 120 минут.

Продолжительность собеседования: 15 – 30 минут.

1. ТЕМЫ, ВКЛЮЧЕННЫЕ В ПРОГРАММУ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

- 1.1 Анализ уязвимостей, угрозы информационной безопасности, построение систем защиты информации;
- 1.2 Алгоритмы, структуры данных и программирование;
- 1.3 Операционные системы: виды процессов и управление ими, безопасность в современных операционных системах;
- 1.4 Стратегия развития Научно-технологического университета «Сириус»;

1.5 Нормативные правовые акты Российской Федерации, определяющие направления развития науки и отраслей экономики.

2. СОДЕРЖАНИЕ ОСНОВНЫХ ТЕМ

2.1 Анализ уязвимостей, угрозы информационной безопасности, построение систем защиты информации:

– Понятие угрозы информационной безопасности. Виды угроз. Модель угроз. Методы оценки уязвимостей автоматизированных систем.

– Понятие модели нарушителя. Цель, задачи, способы формирования и представления модели нарушителя.

– Построение систем защиты от угрозы нарушения конфиденциальности информации. Построение систем защиты от угрозы нарушения целостности информации. Построение систем защиты от угрозы отказа доступа к информации.

– Модели безопасности. Модели распространения прав доступа. Модели системы безопасности.

– Цели и концептуальные основы защиты информации. Современная концепция информационной безопасности. Место информационной безопасности в системе национальной безопасности.

– Критерии, условия и принципы отнесения информации к защищаемой. Классификация информации ограниченного доступа по видам тайны и степеням конфиденциальности.

– Виды уязвимостей информации и формы ее проявления. Каналы и методы несанкционированного доступа к информации ограниченного доступа.

– Системы симметричного шифрования. Вопросы генерации и распределения ключей. Обоснование надежности криптографической защиты.

– Системы асимметричного шифрования, открытый ключ, электронная подпись.

2.2 Алгоритмы, структуры данных и программирование:

– Понятие алгоритма, понятие сложности алгоритмов. Классы P и NP. Примеры NP-полных задач.

– Алгоритмы на графах. Обходы графов. Кратчайшие пути. Основные деревья. Задача о максимальном потоке, о паросочетании, о потоке минимальной стоимости.

– Деревья решений. Обходы деревьев. Двоичные деревья. Красно-черные деревья.

– Алгоритмы сортировки. Формулировка задачи. Устойчивая сортировка. Сортировка пузырьком. Сортировка вставками. Сортировка слиянием. Блочная сортировка. Сортировка Шелла. Быстрая сортировка.

– Понятие рекурсии. Рекурсивные функции. Возвратная последовательность. Математическая индукция. Фрактал.

– Теоретические основы реляционной модели данных. Реляционная алгебра, реляционное исчисление. Функциональные зависимости и нормализация отношений.

– Распределенное программирование. Процессы и их синхронизация. Объектно-ориентированное распределенное программирование. Параллельное программирование над общей памятью.

– Языки программирования высокого и низкого уровня. Понятие границы между высоким и низким уровнем языков программирования.

– Объектно-ориентированное программирование. Шаблоны проектирования, их применение. Классификация шаблонов проектирования. Примеры шаблонов проектирования.

– Функциональное программирование. Функциональная декомпозиция. Персистентные структуры данных. Подходы к проектированию и реализации функциональных программ.

2.3 Операционные системы: виды процессов и управление ими, безопасность в современных операционных системах:

– Виды процессов и управления ими в современных ОС. Представление процессов, их контексты, иерархии порождения, состояния и взаимодействие. Многозадачный (многопрограммный) режим работы. Команды управления процессами. Средства взаимодействия процессов.

– Параллельные процессы, схемы порождения и управления. Организация межпроцессного взаимодействия: общая память, обмен сообщениями.

– Операционные средства управления процессами при их реализации на параллельных и распределенных вычислительных системах и сетях: стандарты и программные средства PVM, MPI, OpenMP, POSIX.

– Оптимизация многозадачной работы компьютеров. Операционные системы Windows, Unix, Linux. Особенности организации, предоставляемые услуги пользовательского взаимодействия.

– Операционные средства управления сетями. Эталонная модель взаимодействия открытых систем ISO/OSI. Маршрутизация и управление потоками данных в сети.

2.4 Стратегия развития Научно-технологического университета «Сириус»: Миссия, цели и задачи университета. Основные принципы деятельности. Приоритетные направления развития.

2.5 Нормативные правовые акты Российской Федерации, определяющие направления развития науки и отраслей экономики:

Указ Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года»;

Указ Президента РФ от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации»;

Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»;

Прогноз научно-технологического развития Российской Федерации на период до 2030 года, утв. Правительством РФ;

Распоряжение Правительства РФ от 31.12.2020 № 3684-р «Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021 – 2030 годы)»;

Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»;

Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»);

Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации "Информационное общество"»;

Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»;

Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года».

Рекомендуемая литература:

1. Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд. Л. Ривест, Клиффорд Штайн. Алгоритмы: построение и анализ, 3-е М.: «Вильямс», 2013.
2. Шень А. Программирование: теоремы и задачи. МЦНМО, 2007.
3. Вирт Н. Алгоритмы и структуры данных. Изд-во Невский диалект, 2005.
4. Керниган Б., Ритчи Д. Язык программирования С. Изд-во Вильямс, 2008.
5. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ, 2-е издание. - М.: Издательский дом Вильямс, 2005.
6. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2017. — 324 с. — ISBN 978-5-8114-2290-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/90153> (дата обращения: 01.03.2024). — Режим доступа: для авториз. пользователей.
7. Баранова Е.К. Информационная безопасность и защита информации / Е.К. Баранова, А.В. Бабаш. - Москва : ИЦ РИОР, 2017. - 322 с. - ISBN 978-5-369-01450-9. - URL: <https://ibooks.ru/bookshelf/378011/reading> (дата обращения:

01.03.2024). - Текст: электронный.

8. Таненбаум Э. Современные операционные системы. 4-е изд. / Э. Таненбаум, Х. Бос. - Санкт-Петербург: Питер, 2019. - 1120 с. - ISBN 978-5-4461-1155-8. - URL: <https://www.ibooks.ru/bookshelf/364626/reading> (дата обращения: 01.03.2024). - Текст: электронный.

9. Стратегия развития Университета «Сириус»: <https://siriusuniversity.ru/about/concept>.

3. ПРИМЕРЫ ЗАДАНИЙ ПИСЬМЕННОГО ЭКЗАМЕНА

3.1. Тестовые вопросы (оцениваются по 8 баллов каждый):

1. Каким образом применение SELinux способствует усилению безопасности Linux?

- Запрет использования паролей;
- Контроль доступа на основе политик безопасности к файлам, процессам и ресурсам;
- Использование открытых методов аутентификации;
- Пропускание данных через нешифрованные порты.

2. Что представляет собой атака "брутфорс"?

- Отказ в обслуживании сетевых ресурсов;
- Попытки несанкционированного доступа к системе путем перебора паролей;
- Внедрение вредоносного кода в ядро операционной системы;
- Использование открытых портов для аутентификации.

3. Как можно повысить безопасность системы Linux через правильную конфигурацию SSH?

- Использование открытых методов аутентификации;
- Запрет доступа к системе с использованием устаревших протоколов;
- Разрешение аутентификации без пароля;
- Отключение SSH для уменьшения риска;

4. Какие из указанных ниже множеств являются декартовым произведением множеств $A \times B$, где $A = \{3, 5\}$ и $B = \{1, 2\}$?

- $\{(1,2), (1, 3), (2, 5), (3, 5)\}$
- $\{(1,3), (1,5), (2,3), (2,5)\}$
- $\{(5,1), (5,2), (3,1), (3,2)\}$
- $\{(3,1), (3,2), (5,1), (5,2)\}$.

5. В чем заключается преимущество алгоритма Ed по сравнению с классическими алгоритмами, такими как RSA?

- Использование открытых методов передачи данных;

- Более высокая производительность и безопасность благодаря эффективной реализации с использованием кривых Эдвардса;

- Применение симметричного блочного шифрования;

- Отправка данных через открытые порты для аутентификации.

6. Как сетевые маски могут повысить безопасность сети?

- Отключение всех масок подсетей;

- Обеспечение логического разделения сетей и управление доступом;

- Шифрование данных между сетевыми устройствами;

- Использование открытых портов для аутентификации.

3.2. Задачи с открытым ответом (оцениваются максимально до 12 баллов каждая):

5. На примере «победитель» – «ОПАЖГЙСЖКЭ» установите правило, по которому при шифровании производится замена букв открытого текста, и прочтите сообщение ЧЙУ СЪУ НУЯ КМЬ ИАЖ ЫЕ КАР ПНВ ШОЗ ЛНГ. Запишите ответ заглавными буквами без пробелов.

6. Активист Гидеон Белфорд разместил в Интернет секретные материалы, зашифрованные с помощью AES-256. Каждый месяц Гидеон рассылает в редакции газет всего мира ключ, на котором был зашифрован очередной секретный документ, делая его содержимое общедоступным. Документы Гидеона производят фурор, все редакции пытаются первыми опубликовать выдержки из них. Уже второй раз подряд в газету Gnutiez приходят письма Джона Смита. Джен утверждает, что умеет атаковать AES-256 и в качестве доказательства указывает первый байт следующего ключа, который будет раскрыт Гидеоном. Этот прогноз каждый раз оказывается верным! В третьем письме Джон предлагает заплатить за предсказание всех следующих ключей. Редактор газеты отказывается платить, утверждая, что Джон — мошенник. Почему редактор так считает?

3.3. Задача на программирование (оценивается максимально до 28 баллов):

7. Никита – дизайнер в Университете Сириус. Ему необходимо разработать дизайн флага для магистерской программы по КИИ. Никита любит геометрические фигуры, комбинаторику и задачи о раскраске, а потому он решает, что флаг программы будет не прямоугольником, а m -угольником с длиной стороны 1 (многоугольник правильный). Никита решает заполнить флаг треугольниками, которые при этом должны иметь вершины, совпадающие с вершинами m -угольника, а также не иметь общих между собой точек, в том числе вершин.

Никита хочет покрыть максимальную площадь хочет покрыть треугольниками наибольшую площадь флага, чтобы он не выглядел слишком пустым. Вычислите, какую максимальную площадь m -угольника он сможет заполнить.

Вход: В единственной строке вводится целое число t ($3 < t < 400$) — число вершин n -угольника.

Выход: Выведите одно вещественное число — максимальную суммарную площадь, которую можно покрыть треугольниками. Ответ будет считаться верным, если его абсолютная или относительная погрешность не более 10^{-6} .

4. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ СОБЕСЕДОВАНИЯ

При оценке ответов поступающего экзаменационная комиссия руководствуется следующими критериями:

- способность структурировать и аргументировать свои высказывания;
- способность к анализу и интерпретации фактов и явлений;
- понимание сущности научно-исследовательской деятельности;
- понимание концепции Стратегии развития Университета «Сириус»;
- понимание роли и задач науки и технологий в достижении целей национального развития России, повышении безопасности и качества жизни граждан, в том числе в выбранной сфере профессиональной деятельности;
- уровень имеющихся к данному моменту общекультурных, общепрофессиональных и профессиональных компетенций;
- публикационная активность поступающего;
- умение определить область научных интересов и планы, связанные с осуществлением дальнейших научных исследований в Университете «Сириус»;
- способность поступающего сделать краткую презентацию своих научных интересов и (или) поддержать беседу на научную тему на английском языке.