МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
Национальный исследовательский ядерный университет «МИФИ»
(НИЯУ МИФИ)

УТВЕРЖДАЮ
Первый проректор НИЯУ МИФИ
_____О.В. Нагорнов
«16» января 2025 г.

Ответственный секретарь
приемной комиссии
_____В.И. Скрытный
«16» января 2025 г.

Программа вступительного испытания

по направлению подготовки магистров
10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

по образовательной программе
«Кибербезопасность»
(онлайн, совместно с Яндекс Практикум)

Форма обучения
Очная

Москва 2025

ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов высшего образования.

Форма проведения вступительного испытания:

Вступительное испытание в магистратуру проводится в форме письменного экзамена. Экзамен проводится с целью выявления у абитуриента объема знаний, необходимых для обучения в магистратуре, а также для определения области научных и профессиональных интересов, мотивов поступления в магистратуру, готовности абитуриента к ведению аналитической деятельности, наличия и направленности исследовательской и/или проектной деятельности, опыта профессиональной деятельности (при наличии).

Структура вступительного испытания:

Вступительное ииспытание состоит из двух частей.

Первая часть – оценка мотивационного письма.

Вторая часть - ответы на вопросы билета. Билет состоит из 3 вопросов. Первый вопрос выбирается из перечня общих вопросов, второй и третий вопросы - из перечня вопросов профильной части программы вступительного испытания. Во время проведения экзамена экзаменационной комиссией могут быть заданы дополнительные вопросы.

Оценка испытания:

Оценка за вступительное испытание выставляется по 100-балльной шкале. Минимальный балл, необходимый для успешного прохождения экзамена и дальнейшего участия в конкурсе, ежегодно устанавливается приемной комиссией НИЯУ МИФИ.

Максимальное число баллов, которое можно получить за первую часть вступительного собеседования – 50.

Максимальное число баллов, которое можно получить за вторую часть вступительного собеседования – 50.

Критерии оценки результатов вступительного испытания:

Критерии оценивания мотивационного письма

Критерий	**Виды результатов**	**Оценка**	**Максимальное количество баллов за критерий**
Понимание опыта исследовательской / проектной деятельности в бакалавриате / специалитете	Способен четко сформулировать суть исследовательской проблемы / прикладной задачи и методов их решения.	8-10	10
	Формулирует задачи и методы их решения, испытывает затруднения при их соотнесении	5-7	
	Не способен сформулировать суть задачи и методов их достижения	0-4	
Релевантность ожиданий от обучения и результатов, а также понимание предметной области	Абитуриент демонстрирует хороший уровень знаний о программе и понимание предметной области программы, демонстрирует релевантные и продуманные ожидания от результаты обучения.	8-10	10
	Абитуриент упоминает некоторые релевантные цели и ожидания от программы, но недостаточно детализировано, а также демонстрирует недостаточное понимание предметной области	5-7	
	Абитуриент упоминает некоторые цели и предполагаемые планы, которые не соотносятся с содержанием программы и предметной областью	0-4	
Индивидуальность сочинения, конкретизация деталей	Письмо содержит конкретные детали, описывающие предыдущий опыт абитуриента и	11-15	

	раскрывающие его индивидуальность		15
	Письмо содержит отдельные фрагменты, конкретизирующие предыдущий опыт абитуриента	6-10	
	Индивидуальные детали об абитуриенте практически не представлены или являются клишированными	0-5	
Логика и структура изложения, а также орфография, пунктуация и грамматика текста	Представлен ясный, структурированный и логичный текст. Отсутствуют ошибки. Основные идеи выделены и раскрыты.	11-15	15
	В тексте письма в целом отсутствуют ошибки. Наблюдаются недочеты в логике и стиле изложения, структуре текста, затрудняющие чтение и понимание письма.	6-10	
	Нарушена структура изложения, не ясны основные мысли письма. Допущенные ошибки мешают восприятию текста	0-5	
Всего:			**50**

Критерии оценивания ответов на вопросы:

Критерий	**Виды результатов**	**Общий вопрос**		**Профильный вопрос**	
		Оценка	**Максимальное количество баллов за критерий**	**Оценка**	**Максимальное количество баллов за критерий**
Понимание вопроса и полнота ответа	Полностью раскрывает суть вопроса, дает развернутый и обоснованный ответ	8-13	13	6-8	8
	Частично раскрывает суть вопроса, ответ содержит неполные или недостаточно обоснованные сведения	5-7		3-5	

	Ответ неполный, с ошибками, основные аспекты не раскрыты	0-4		0-2	
Логика и структура изложения	Ответ логичен, структурирован, основные идеи выделены и последовательно изложены	4-5	5	4-5	5
	Логика ответа не всегда ясна, структура нарушена	2-3		2-3	
	Логика отсутствует, структура хаотична	0-1		0-1	
Грамотность и ясность изложения	Ответ написан грамотно, без ошибок, понятен и легко воспринимается	2	2	2	2
	Присутствуют незначительные грамматические или стилистические ошибки	1		1	
	Грубые ошибки, затрудняющие восприятие	0		0	
Всего:			**20**		**15**

ЧАСТЬ 1. МОТИВАЦИОННОЕ ПИСЬМО

Данное задание ставит перед собой главную цель - познакомиться с абитуриентом, его опытом, целями и ожиданиями от программы. Это возможность, которая дается абитуриенту показать осознанную заинтересованность в обучении на выбранной магистерской программе. Ответ на данный вопрос позволяет приёмной комиссии понять, насколько абитуриент готов к углубленному профессиональному обучению, насколько осознанным является выбор конкретной программы и как он видит свою дальнейшую профессиональную траекторию.

Требования к мотивационному письму

Мотивационное письмо должно состоять из структурированного текста объемом от 3000 до 4500 знаков без учета пробелов, в котором содержится обоснование выбора магистерской программы «Кибербезопасность».

Мотивационное письмо должно быть логично структурируровано, ответы аргументированы и не содержать дублирования информации. Нам важно увидеть и понять вашу мотивацию, осознанность вашего выбора поступать в

магистратуру, а еще иметь представление о потенциале вашего развития в данной области.

Мотивационное письмо должно отражать ответы на каждый из нижеперечисленных вопрос. Подробное раскрытие каждого пункта поможет вам набрать максимальный балл за это задание:

1. Образовательный и профессиональный бэкграунд.

- Укажите, по какому направлению бакалавриата/специалитета вы получили базовое образование.
- Охарактеризуйте исследовательскую или проектную задачу, решаемую в вашей выпускной квалификационной работе.
- Опишите методы, которые вы использовали при ее решении.

2. Выбор магистерской программы.

- Объясните, почему вы решили поступать именно на данную программу.
- Какая дисциплина в программе заинтересовала вас больше всего и почему?
- Есть ли у вас опыт в выбранной профессиональной деятельности? Если да, расскажите о нем.

3. Компетенции и подготовленность к обучению.

- Какие знания, навыки и опыт (учебный и/или профессиональный) помогут вам успешно освоить программу?
- В чем вы видите свою ключевую силу как будущего специалиста в этой области?

4. Кибербезопасность: вызовы и перспективы.

- Почему вы считаете информационную безопасность стратегически важной областью?
- Какие ключевые угрозы и риски, по вашему мнению, стоят перед цифровым обществом и бизнесом сегодня?
- Какие задачи или идеи вам было бы интересно реализовать в области кибербезопасности?
- Какие вызовы, связанные с этикой, правом или технологиями, вы видите в будущем этой области?

5. Будущая профессиональная траектория.

- Как вы видите свое развитие после окончания магистратуры?
- Какие навыки и компетенции вам необходимы для достижения карьерных целей?
- Сформулируйте исследовательскую или прикладную задачу, которую вам было бы интересно решить в рамках обучения на программе.

ЧАСТЬ 2. ОБЩИЕ И ПРОФИЛЬНЫЕ ВОПРОСЫ

Перечень общих вопросов

1. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается каждый из них?
2. Дайте определения идентификации, аутентификации и авторизации пользователей. Чем отличаются эти понятиями, в каких случаях происходят данные процессы?
3. Каковы особенности симметричных и асимметричных шифров? Приведите примеры этих способов шифрования.
4. Что такое компьютерный вирус, какие виды вирусов существуют?
5. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.
6. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
7. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?
8. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
9. Что представляет из себя алгоритм электронной подписи и для чего применяется?
10. Что такое распределенная атака типа «отказ в обслуживании» (DDoS)?

Перечень профильных вопросов

1. Какие вам известны подходы к классификации угроз безопасности информации? Опишите их.
2. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.
3. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Каковы преимущества и недостатки методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?
4. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.
5. Охарактеризуйте основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.
6. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
7. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Опишите их.
8. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?
9. Опишите методы сигнатурного анализа для выявления вирусов.
10. Опишите методы эвристического анализа для выявления вирусов.
11. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации?
12. Изложите кратко основное содержание деятельности ФСТЭК и ФСБ России в области обеспечения информационной безопасности.
13. Объясните, почему важными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.
14. Приведите классификацию источников утечки информации по техническим каналам.

15. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.
16. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.
17. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?
18. Что такое целенаправленные атаки? Приведите примеры.
19. Что такое виртуальные защищенные каналы связи?
20. Опишите преимущества и недостатки использования менеджеров паролей.
21. Какие уязвимости информационных систем или ПО вы знаете?