МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по МДРМ МИЭТ

_____ Д.Г. Коваленко
«30» октября 2020 г.

Программа вступительных испытаний
по приему в магистратуру в 2021 году
Кафедры информационной безопасности
по направлению 10.04.01 «Информационная безопасность»
по образовательной программе «Аудит информационной безопасности автоматизированных систем»

Москва 2020 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 «Информационная безопасность» (уровень магистратуры) утвержден приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1513.

1.2. Область профессиональной деятельности выпускников, освоивших программу магистратуры, включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности и защиты информации.

1.3. Объектами профессиональной деятельности выпускников, освоивших программу магистратуры, являются:

фундаментальные и прикладные проблемы информационной безопасности;

объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы;

средства и технологии обеспечения информационной безопасности и защиты информации;

экспертиза, сертификация и контроль защищенности информации и объектов информатизации;

методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации;

организация и управление информационной безопасностью;

образовательный процесс в области информационной безопасности.

1.4. Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу магистратуры:

проектная;

научно-исследовательская;

контрольно-аналитическая;

педагогическая;

организационно-управленческая.

При разработке и реализации программы магистратуры МИЭТ ориентируется на все виды профессиональной деятельности, к которым готовится магистр. Основной вид деятельности, к которой готовятся выпускники, освоившие программу магистратуры –

контрольно-аналитическая.

Выпускник, освоивший программу магистратуры в соответствии с видами профессиональной деятельности, должен быть готов решать следующие профессиональные задачи:

проектная деятельность:

системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;

обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов

разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;

разработка программ и методик испытаний средств и систем обеспечения информационной безопасности;

научно-исследовательская деятельность:

анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;

разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;

выполнение научных исследований с применением соответствующих физических и математических методов;

подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях;

контрольно-аналитическая деятельность:

аудит информационной безопасности информационных систем и объектов информатизации;

аттестация объектов информатизации по требованиям безопасности информации;

педагогическая деятельность:

выполнение учебной и методической работы в образовательных организациях среднего профессионального, высшего образования и дополнительного профессионального образования в должностях преподавателя и ассистента под руководством ведущего преподавателя (профессора, доцента) по дисциплинам направления;

организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений,

определение порядка выполнения работ;

организация управления информационной безопасностью;

организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

2. УЧЕТ ИНДИВИДУАЛЬНЫХ ДОСТИЖЕНИЙ

В соответствии с правилами приема в магистратуру при поступлении на образовательную программу «Аудит информационной безопасности автоматизированных систем» установлено максимальное количество баллов за каждое индивидуальное достижение:

№ п/п	Наименование индивидуального достижения	Оценка индивидуального достижения	Документы для подтверждения наличия индивидуальных достижений
1.	Победитель или призер Международной или Всероссийской олимпиады или Международного или Всероссийского конкурса (выставки) в области информационной безопасности.	100 баллов	Диплом победителя или призера
2.	Участие в финале Международного или Всероссийского конкурса (выставки) научных и творческих работ, Международной или Всероссийской студенческой олимпиаде (чемпионате) по профилю магистратуры	10 баллов	Сертификат участника
3.	Победитель конкурса творческих и проектных работ по направлению подготовки 10.03.01 «Информационная безопасность», проводимого в МИЭТ.	100 баллов	Диплом победителя
4.	Призер конкурса творческих и	75 баллов	Диплом призера или лау-

№ п/п	Наименование индивидуального достижения	Оценка индивидуального достижения	Документы для подтверждения наличия индивидуальных достижений
	проектных работ по направлению подготовки 10.03.01 «Информационная безопасность», проводимого в МИЭТ.		реата
5.	Победитель или призер Добровольного квалификационного экзамена от правительства г. Москвы по направлению «Информационная безопасность»	10 баллов	Диплом победителя или призера
6.	Участие в очном туре Добровольного квалификационного экзамена от правительства г. Москвы по направлению «Информационная безопасность»	5 баллов	Сертификат участника
7.	Победитель или призер регионального или ведомственного конкурса (выставки) или олимпиады в области информационной безопасности.	10 баллов	Диплом победителя или призера
8.	Диплом о высшем образовании с отличием	10 баллов	Копия (или подлинник) диплома
9.	Наличие научных публикаций или РИД (патент на изобретение или полезную модель, свидетельство о регистрации топологии ИМС или базы данных) по направлению «Информационная безопасность»	До 10 баллов 1 статья в сборнике тезисов докладов конференций – 2/N балла; 1 статья в сборнике трудов конференций – 3/N балла; 1 статья в сборнике трудов конференций или журнале с индексацией в РИНЦ – 5/N баллов; 1 статья в научном издании, входящем в перечни ВАК, Web of Science, SCOPUS – 10/N баллов; РИД – 10/N баллов, где N – количество авторов.	Ксерокопия (титульный лист, оглавление, текст публикации, выходные данные)

Максимальное количество баллов, набранных по совокупности вступительных испытаний и индивидуальных достижений – 100 баллов.

Согласно Правилам приема в магистратуру МИЭТ в 2021 году участие в конкурсе а творческих и проектных работ по направлению подготовки 10.03.01 «Информационная безопасность», проводимого в МИЭТ, принимают абитуриенты, набравшие не менее 25 баллов.

Прием вступительного испытания в форме собеседования производится экзаменационной комиссией в соответствии с расписанием и списками абитуриентов, подготовленными приемной комиссией.

3. ПОРЯДОК И РЕГЛАМЕНТ ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительные испытания проводит экзаменационная комиссия. Персональный состав комиссии утверждается ректором МИЭТ не позже, чем за месяц до начала экзамена.

Программа вступительных испытаний публикуется на сайте МИЭТ в сроки, определенные Правилами приема в магистратуру МИЭТ.

Вступительные испытания проводятся в форме собеседования. Собеседование предполагает письменный или устный ответ экзаменуемого по трем теоретическим вопросам из разных разделов, приведенных в п. 4. Экзаменующемуся предоставляется возможность подготовиться к предстоящему собеседованию в течении времени не более 45 минут.

При выставлении оценок за вопросы экзаменационная комиссия руководствуется следующими критериями:

- знаниями учебного материала предметов;
- умением студента выделять наиболее существенные положения;
- четко формулировать свои мысли;
- применять теоретические знания для анализа конкретных экономических ситуаций и решения прикладных проблем.

Каждый член экзаменационной комиссии выставляет индивидуальную оценку экзаменующемуся за ответ на вопрос.

Решение об оценке знаний экзаменующихся принимается экзаменационной комиссией открытым голосованием простым большинством членов комиссии, участвующих в

заседании. При выведении итоговых оценок, в случае равенства голосов, мнение председателя экзаменационной комиссии является решающим.

Результаты экзамена доводятся до экзаменуемых после закрытого заседания экзаменационной комиссии.

Экзаменационная комиссия в день проведения вступительных испытаний передает протоколы с результатами вступительных испытаний в приемную комиссию.

4. ПЕРЕЧЕНЬ ВОПРОСОВ ПО ОСНОВНЫМ УЧЕБНЫМ ДИСЦИПЛИНАМ, ВЫНОСИМЫМ НА ВСТУПИТЕЛЬНЫЕ ИСПЫТАНИЯ ПРИ ПОСТУПЛЕНИИ В МАГИСТРАТУРУ

Тематика вопросов для собеседования соответствует избранным разделам (темам) из учебных программ цикла профессиональных дисциплин, предусмотренных ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата)»:

основы информационной безопасности;

организационное и правовое обеспечение информационной безопасности;

программно-аппаратные средства защиты информации;

криптографические методы защиты информации;

техническая защита информации;

основы управления информационной безопасностью.

Программа собеседования разбита на тематические разделы. Каждый тематический раздел сформирован на основе дисциплин федерального компонента, что позволяет на экзамене осуществить комплексный контроль знаний студентов по основным направлениям защиты информации, предусмотренным ФГОС ВО.

Раздел 1. Способы и средства защиты информации от несанкционированного доступа

1. Классификация и характеристика угроз безопасности информации в автоматизированных системах (АС). Общая характеристика источников угроз несанкционированного доступа в АС.
2. Модель угроз безопасности информации, обрабатываемой в АС.
3. Характеристика угроз несанкционированного доступа к информации, обрабатываемой в АС.

4. Характеристика угроз безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия.
5. Характеристика угроз программно-математических воздействий. Вредоносные программы (программные закладки; классические программные (компьютерные) вирусы; вредоносные программы, распространяющиеся по сети (сетевые черви). Недекларированные возможности.
6. Классификация и общая характеристика методов (технологий) обеспечения безопасности информации, обрабатываемой в АС.
7. Современные технологии идентификации и аутентификации. Протоколы аутентификации.
8. Технологии управления доступом к информации. Дискреционный принцип контроля доступа.
9. Технологии управления доступом к информации. Мандатный принцип контроля доступа.
10. Технологии управления доступом к информации. Ролевая модель контроля за доступом.
11. Понятие межсетевого экрана (МЭ) и сетевого периметра. Классификация МЭ и показатели защищенности. Понятие и назначение DMZ.
12. Современные технологии контроля и обеспечения целостности информации.
13. Методы обнаружения вторжений. Системы обнаружения вторжений и предотвращения вторжений.
14. Технологии антивирусной защиты. Средства антивирусной защиты (САВЗ).
15. Криптографические алгоритмы. Криптографическая стойкость. Иммитостойкость. Симметричные и асимметричные криптосистемы (общая характеристика).
16. Управление криптографическими ключами. Понятие ключа шифрования, виды ключей. Постановка проблемы управления криптографическими ключами. Генерация ключей. Системы управления ключами в случае симметричного алгоритма шифрования.
17. Классификация шифров. Шифры перестановки. Шифры замены. Шифры гаммирования. Блочные и поточные системы шифрования. Алгоритмы блочного шифрования. Режимы шифрования блочных шифров.
18. Алгоритмы шифрования данных ГОСТ 28147-89, ГОСТ Р 34.12-2015. Режимы работы блочных шифров ГОСТ Р 34.13-2015. Алгоритм Криптографические алгоритмы. Криптографическая стойкость. Иммитостойкость. Симметричные и асимметричные криптосистемы (общая характеристика).

19. Электронная цифровая подпись. Криптографические протоколы. Алгоритмы цифровой подписи. Стандарт цифровой подписи ГОСТ Р 34.10-2012. Функция хеширования. Алгоритмы хеширования. Стандарт вычисления хеш-функции ГОСТ Р 34.11-2012.
20. Классы защищенности СВТ от НСД. Показатели защищенности средств вычислительной техники (СВТ) от несанкционированного доступа (НСД). Требования по защите СВТ от НСД различных классов.
21. Классы защищенности АС от НСД. Показатели защищенности АС от НСД. Требования по защите АС от НСД различных классов.
22. Классы защищенности МЭ от НСД. Показатели защищенности МЭ от НСД. Требования по защите МЭ от НСД различных классов.
23. Средства контроля защищенности информации от несанкционированного доступа типа «Ревизор-1», «Ревизор-2», «Терьер-3,0», «Фикс».
24. Сканеры безопасности «Сканер - ВС», «XSpider» и др.

Список рекомендуемой литературы по разделу 1

1. Бутакова Н.Г., Федоров Н.В. Криптографические методы и средства защиты информации: учеб. пособие. – СПб.: ИЦ «Интермедия», 2017. – 384 с. – ISBN 978-5-4383-0135-6.
2. Введение в информационную безопасность: учеб. пособие для вузов / А. А. Малюк [и др.] ; Под ред. В.С. Горбатова. - М.: Горячая линия-Телеком, 2011. - 288 с.- URL: https://e.lanbook.com/book/100636.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учеб. пособие. - М. : Горячая линия-Телеком, 2012. - 320 с. - URL: https://e.lanbook.com/book/5150. - ISBN 978-5-9912-0147-6.
4. Информационная безопасность открытых систем: учебник/ Д.А. Мельников. - М. : Флинта : Наука, 2013. - 448 с. - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7 : 412-83; 004.056(075.8).
5. Основы информационной безопасности : Учеб. пособие / В.А. Галатенко. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: https://e.lanbook.com/book/100295. - ISBN 978-5-94774-821-5 : 0-00.
6. Программно-аппаратные средства обеспечения информационной безопасности : учеб. пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. - М. : Горячая линия-Телеком, 2018. - 248 с. - URL: https://e.lanbook.com/book/111053. - ISBN 978-5-9912-0470-5.

7. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие.- М.: Форум, 2012. – 352 с.

Раздел 2. Способы и средства защиты информации от утечки по техническим каналам

1. Объект информатизации. Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Посторонние проводники. Контролируемая зона объекта. Утечка информации по техническому каналу. Перехват информации. Технический канал утечки информации (определение). Схема технического канала утечки информации. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
2. Причины образования технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений (электромагнитные ТКУИ). Определение зоны R2. Схема электромагнитного ТКУИ. Порядок определения зоны R2.
3. Причины образования технических каналов утечки информации, возникающих за счет наводок побочных электромагнитных излучений (электрических ТКУИ). Определение зоны r1. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений. Схема технического канала утечки информации, возникающего за счет «просачивания» информативных сигналов в цепи электропитания и заземления ТСПИ. Порядок определения зоны r1.
4. Специально создаваемые технические каналы утечки информации, обрабатываемой СВТ. Схема технического канала утечки информации, создаваемого путем высокочастотного облучения СВТ. Схема технического канала утечки информации создаваемого путем внедрения в СВТ электронных устройств перехвата информации (аппаратных закладок).
5. Основные характеристики речи и речевого сигнала. Методика расчета словесной разборчивости речи.
6. Выделенное помещение (определение). Вспомогательные технические средства и системы (ВТСС). Контролируемая зона объекта. Утечка информации по техническому каналу. Перехват информации. Технический канал утечки информации (определение). Классификация технических каналов утечки акустической речевой информации и способов перехвата речевой информации.

7. Схема прямого технического канала утечки речевой информации. Способы перехвата речевой информации по прямому техническому каналу утечки акустической речевой информации (схемы каналов перехвата информации). Средства перехвата акустической речевой информации по прямому акустическому каналу.
8. Схема акустовибрационного технического канала утечки информации. Средства перехвата акустической речевой информации по акустовибрационному каналу.
9. Схема акустооптического (лазерного) канала утечки акустической речевой информации. Триппель-призмы. Основные характеристики лазерных акустических систем разведки.
10. Схема пассивного акустоэлектрического канала утечки информации. Виды акустоэлектрических преобразователей. Схема активного акустоэлектрического канала утечки информации. Виды акустоэлектрических преобразователей модуляторного типа. Схема пассивного акустоэлектромагнитного канала утечки информации. Схема активного акустоэлектромагнитного канала утечки информации (схема высокочастотного облучения).
11. Классификация пассивных способов и средств защиты информации, обрабатываемой техническими средствами. Классификация активных способов и средств защиты информации, обрабатываемой техническими средствами.
12. Экранирующие материалы, их основные характеристики. Экранированные помещения и экранированные камеры.
13. Основные требования к заземлению технических средств. Схемы заземления технических средств. Схемы измерения сопротивления заземления.
14. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации. Основные требования при установке системы пространственного зашумления на объекте информатизации.
15. Основные требования к системе электропитания технических средств. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств. Схемы установки помехоподавляющих фильтров на объекте информатизации. Системы линейного электромагнитного зашумления инженерных коммуникаций и цепей электропитания технических средств (основные характеристики, требования по установке).
16. Классификация пассивных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Классификация активных

способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

17. Средства звуко- и виброизоляции выделенных помещений. Звукоизолирующие кабины. Специальные защищенные помещения.
18. Основные требования к системе выброакустической маскировки. Состав систем виброакустичекой маскировки типов А и Б. Виброизлучатели (классификация, принципы построения, основные характеристики). Рекомендации по установке виброизлучателей и акустических излучателей. Основные характеристики типовых систем виброакустичекой маскировки.
19. Способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Средства защиты телефонных аппаратов от утечки речевой информации по акустоэлектрическим каналам (принципы построения и основные характеристики).
20. Состав и основные требования к аппаратуре контроля эффективности защиты выделенных помещений от утечки речевой информации по прямому акустическому каналу. Схема измерительной установки при контроле выполнения норм защищенности речевой информации с использованием шумомера.
21. Состав и основные требования к аппаратуре контроля эффективности защиты выделенных помещений от утечки речевой информации по акустовибрационному и акустооптическому каналам. Схема измерительной установки при контроле выполнения норм защищенности речевой информации с использованием вибромера.
22. Состав и основные требования к аппаратуре контроля эффективности защиты выделенных помещений от утечки речевой информации по акустоэлектрическим каналам. Схема измерительной установки при контроле выполнения норм защищенности речевой информации от ее утечки по акустоэлектрическим каналам.
23. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИ. Схема измерения ПЭМИ.
24. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет наводок ПЭМИ. Схема измерения наводок ПЭМИ в исследуемой линии. Оценка эффективности защиты информации от утечки, возникающей за счет наводок ПЭМИ.
25. Методы выявления электронных устройств перехвата информации. Средства выявления электронных устройств перехвата информации.

Список рекомендуемой литературы по разделу 2

1. Технические средства и методы защиты информации: Учеб. пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков [и др.]. - 4-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2012. - 616 с. - URL: https://e.lanbook.com/book/5154. - ISBN 978-5-9912-0084-4.
2. Хорев А.А. Техническая защита информации: Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации. - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9.

Раздел 3 «Организация защиты информации на объектах информатизации»

1. Государственная система обеспечения ИБ и ЗИ в Российской Федерации. Структура органов государственного управления в области обеспечения ИБ и ЗИ
2. Сведения, составляющие государственную тайну. Уровни секретностей сведений, составляющих государственную тайну. Ответственность за разглашение и неправомерный доступ к сведениям, составляющим государственную тайну.
3. Сущность и содержание коммерческой тайны. Подходы к определению уровней конфиденциальности сведений, составляющих коммерческую тайну. Порядок отнесения информации к коммерческой тайне. Ответственность за разглашение и неправомерный доступ к сведениям, составляющим коммерческую тайну.
4. Сущность и содержание обработки и защиты персональных данных. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные. Ответственность за разглашение и неправомерный доступ к персональным данным.
5. Защита информации (определение). Направления защиты информации. Основные задачи защиты информации.
6. Лицензирование деятельности в области защиты информации.
7. Сертификация средств защиты информации.
8. Порядок организации защиты информации на объекте информатизации (ОИ).
9. Предварительное специальное обследование ОИ.
10. Аналитическое обоснование необходимости создания системы комплексной защиты информатизации (СЗИ) ОИ (содержание, порядок проведения).
11. Техническое задание на разработку СЗИ ОИ.
12. Технический проект СЗИ ОИ.
13. Организационно-распорядительные документы по защите информации, разрабаты-

ваемые на ОИ.

14. Порядок организации аттестации ОИ. Программа и методика аттестационных испытаний.
15. Порядок проведения аттестации объекта СВТ по требованиям безопасности информации.
16. Порядок проведения аттестации выделенного помещения по требованиям безопасности информации.
17. Система управления информационной безопасностью (структура, взаимосвязь основных процессов управления и их основное содержание).
18. Роль концепции информационной безопасности в процессах управления информационной безопасности. Основные положения концепции информационной безопасности организации (предприятия).
19. Понятие политики информационной безопасности. Основные требования, принципы и подходы к разработке политики информационной безопасности.
20. Практические правила управления информационной безопасностью.
21. Понятие аудита ИБ. Цели аудита. Объекты аудита ИБ. Внешний аудит ИБ. Внутренний аудит ИБ.

Список рекомендуемой литературы по разделу 3

1. Введение в информационную безопасность : Учеб. пособие для вузов / А.А.Малюк, В.С. Горбатов, В.И. Королев [и др.]; под ред. В.С. Горбатова. - М. : Горячая линия-Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5. – URL:https://e.lanbook.com/book/5171.
2. Вострецова Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.
3. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158 (дата обращения: 30.12.2020). - ISBN 978-5-534-03600-8 : 0-00. - Текст : электронный.
4. Организационное и правовое обеспечение информационной безопасности : В 2-х ч.: Учеб. пособие. Ч. 1 : Правовое обеспечение информационной безопасности /

В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 184 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0733-8 : б.ц., 200 экз.

5. Организационное и правовое обеспечение информационной безопасности : В 2-х ч.: Учеб. пособие. Ч. 2 : Организационное обеспечение информационной безопасности / В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 172 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0738-3 : б.ц., 200 экз.
6. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158: 30.12.2020). - ISBN 978-5-534-03600-8 : 0-00. - Текст : электронный.
7. Основы информационной безопасности : Учеб. пособие / В.А. Галатенко. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: https://e.lanbook.com/book/100295. - ISBN 978-5-94774-821-5 : 0-00.
8. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью: учеб. пособие. – М.: "Горячая линия-Телеком, 2012. – 244 с. SBN978-5-9912-0271-8
9. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учеб. пособие / Ю.И. Коваленко. - М. : Горячая линия-Телеком, 2012. - 140 с. - URL: https://e.lanbook.com/book/5163. - ISBN 978-5-9912-0261-9.

5. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Уровень знаний абитуриента определяется следующими оценками: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Общими критериями, определяющими оценку знаний по вопросу являются:

а) «отлично» - наличие глубоких исчерпывающих знаний в объеме пройденного курса в соответствии с поставленными программой курса и целями обучения, правильное и логически стройное изложение материала, наличие знаний по дополнительно рекомендованной литературы, иллюстрация ответа (если это требуется логикой изложения ответа)

графиками, структурными схемами и др. иллюстрационными материалами, выполненными правильно и аккуратно;

б) «хорошо» - наличие твердых и достаточно полных знаний в объеме пройденного курса, незначительные ошибки при освещении заданных вопросов, логичное изложение материала, иллюстрация ответа (если это требуется логикой изложения ответа) графиками, структурными схемами и др. иллюстрационными материалами, в которых имеются отдельные неточности;

в) «удовлетворительно» - наличие твердых знаний, изложение ответов с ошибками, уверенно исправляемых после дополнительных вопросов, ответ не проиллюстрирован необходимыми графиками, структурными схемами и др. иллюстрационными материалами, нарушена логика изложения ответа на вопрос;

г) «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса.

По окончании ответов всех экзаменующихся, экзаменационная комиссия проводит обсуждение индивидуальных оценок членов комиссии и выводит итоговые оценки для всех экзаменовавшихся. Обсуждение и окончательное оценивание ответов студента экзаменационная комиссия проводит на закрытом заседании, определяя итоговую оценку за каждый вопрос – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Максимальное количество баллов за ответ на один вопрос:

оценка «отлично» – 25 баллов;

оценка «хорошо» – 15 баллов;

оценка «удовлетворительно» – 10 баллов;

оценка «неудовлетворительно» – 0 баллов.

Минимальная сумма баллов, позволяющая поступающему участвовать в конкурсе в магистратуру, – 25. Максимальная сумма баллов – 75.

Заведующий кафедрой
«Информационная безопасность» А.А. Хорев

Руководитель магистерской программы А.А. Хорев

«30» октября 2020 г.