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

УТВЕРЖДАЮ
Проректор по УР МИЭТ

_____ А.Г.Балашов
«18» января 2024 г.

Программа вступительных испытаний
по приему в магистратуру в 2024 году
кафедры «Информационная безопасность»
по направлению 10.04.01 «Информационная безопасность»
по образовательной программе «Аудит информационной безопасности»
(очная форма обучения)

Москва 2024 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 науки и высшего образования РФ от 26 ноября 2020 г. № 1455.

1.2. Область профессиональной деятельности выпускников, освоивших программу магистратуры, включает:

01 Образование и наука (в сферах: профессионального и дополнительного профессионального образования; научных исследований, связанных с обеспечением информационной безопасности и защиты информации);

06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности).

1.3. Типы профессиональной деятельности, к которым готовятся выпускники, освоившие программу магистратуры:

- проектная;
- научно-исследовательская;
- организационно-управленческая;
- педагогическая;
- контрольно-аналитическая.

При разработке и реализации программы магистратуры МИЭТ ориентируется на решение следующих задач профессиональной деятельности:

Область профессиональной деятельности	Типы задач профессиональной деятельности	Задачи профессиональной деятельности
01 Образование и наука (в сферах: профессионального и дополнительного профессионального образования; научных исследований, связанных и обеспечением информационной безопасности и защиты информации).	Научно-исследовательский	Сбор, обработка и анализ научно-технической информации по теме исследования, разработка планов и программ проведения научных исследований и технических разработок
		Проведение научных исследований, включая экспериментальные, обработка результатов исследований, оформление научно-технические отчетов, обзоров, подготовка по результатам выполненных исследований научных докладов и статей
	Педагогический	Поведение практических занятия по избранным дисциплинам данного направления подготовки, разработка методических материалов, используемых в образовательном процессе

Область профессиональной деятельности	Типы задач профессиональной деятельности	Задачи профессиональной деятельности
06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности).	Проектный	Обоснование требований к системе обеспечения информационной безопасности и разработка проекта технического задания на ее создание
		Разработка технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности
	Организационно-управленческий	Разработка проектов организационно-распорядительных документов по обеспечению информационной безопасности
	Контрольно-аналитический	Аттестация объектов информатизации на соответствие требованиям по защите информации
		Аудит информационной безопасности автоматизированных систем

1.4. Вступительные испытания при приеме в магистратуру по направлению 10.04.01 «Информационная безопасность» проводятся в форме собеседования.

Основной целью вступительного испытания является отбор абитуриентов, наиболее подготовленных к продолжению обучения в магистратуре высшего учебного заведения по направлению подготовки 10.04.01 «Информационная безопасность».

Задачами вступительного испытания являются:

– оценка уровня знаний и умений в профессиональной области;

– выявление степени подготовленности к продолжению обучения в магистратуре.

Вопросы, выносимые на собеседование, определяются настоящей программой, в основу которой положены квалификационные требования, предъявляемые к бакалаврам, в соответствии с федеральным государственным образовательным стандартом высшего образования по одноименному направлению подготовки 10.03.01 «Информационная безопасность».

Вступительное испытание содержит оценку знаний абитуриента по следующим дисциплинам:

– организационное и правовое обеспечение информационной безопасности;
– программно-аппаратные средства защиты информации;
– методы и средства криптографической защиты информации;
– защита информации от утечки по техническим каналам;
– основы управления информационной безопасностью.

2. УЧЕТ ИНДИВИДУАЛЬНЫХ ДОСТИЖЕНИЙ

Индивидуальные достижения (ИД) поступающего в магистратуру, указанные в п. 2-9, могут оцениваться суммарно в 100 баллов. Общая сумма индивидуальных достижений в п. 1, 10-11 могут оцениваться суммарно в 25 баллов.

Максимальное количество баллов, которое может получить поступающий за индивидуальные достижения – 100 баллов.

При поступлении в магистратуру учитываются индивидуальные достижения за последние 3 года.

№ п/п	Наименование ИД	Оценка ИД	Документы для подтверждения наличия ИД
1.	Диплом о высшем образовании с отличием	10 баллов	Копия (или подлинник) диплома
2.	Победитель проводимого МИЭТ конкурса творческих и проектных работ 2024 г. по направлению подготовки 10.04.01 «Информационная безопасность».	100 баллов	Диплом победителя
3.	Призер проводимого МИЭТ конкурса творческих и проектных работ 2024 г. по направлению подготовки 10.04.01 «Информационная безопасность».	25 баллов	Диплом призера
4.	Победитель (призер) Международной или Всероссийской олимпиады или Международного или Всероссийского конкурса (выставки) в области информационной безопасности.	100 баллов	Диплом победителя (призера)
5.	Призер или лауреат Международного или Всероссийского конкурса (выставки) научных и творческих работ, Международной или Всероссийской студенческой олимпиады (чемпионата) по профилю магистратуры	75 баллов	Диплом призера или лауреата
6.	Участие в финале Международного или Всероссийского конкурса (выставки) научных и творческих работ, Международной или Всероссийской студенческой олимпиаде (чемпионате) в области информационной безопасности.	25 баллов	Сертификат участника
7.	Победитель (призер) Добровольного квалификационного экзамена от правительства г. Москвы по направлению «Информационная безопасность»	25 баллов	Диплом победителя (призера)

№ п/п	Наименование ИД	Оценка ИД	Документы для подтверждения наличия ИД
8.	Участие в очном туре Добровольного квалификационного экзамена от правительства г. Москвы по направлению «Информационная безопасность»	5 баллов	Сертификат участника
9.	Победитель (призер) регионального или ведомственного конкурса (выставки) или олимпиады в области информационной безопасности.	25 баллов	Диплом победителя или призера
10.	Наличие научных публикаций или по направлению «Информационная безопасность»	До 10 баллов 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	Ксерокопия (титульный лист, оглавление, текст публикации, выходные данные)
11.	Наличие РИД (патент на изобретение или полезную модель, свидетельство о регистрации топологии ИМС или базы данных, свидетельство о регистрации программы для ЭВМ и др.) по направлению «Информационная безопасность»	До 10 баллов РИД – 10/N баллов, где N – количество авторов.	Ксерокопия (титульный лист, оглавление, текст публикации, выходные данные)
12.	Письменное согласие организации о целевом обучении гражданина по направлению подготовки 10.04.01 «Информационная безопасность».	10 баллов	Письмо на официальном бланке организации

3. ПОРЯДОК И РЕГЛАМЕНТ ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

3.1. Порядок проведения собеседования

Вступительные испытания проводятся в форме собеседования.

Даты, время и аудитории проведения вступительных испытаний назначаются в соответствии с «Правилами приема в магистратуру Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Московский институт электронной техники» в 2022 году».

Во время вступительного испытания поступающему задается по одному теоретическому вопросу из трех разделов программы вступительных испытаний (всего три вопроса) и дается время на подготовку. Для подготовки выделено 45 минут, разрешено пользоваться собственными записями лекций и письменными материалами по практическим занятиям. Использование при подготовке к ответам на вопросы компьютеров, мобильных телефонов и иных средств связи не допускается.

При ответе экзаменационной комиссией может быть задано до трех дополнительных вопросов по каждому вопросу собеседования.

В ходе собеседования поступающим могут быть также заданы вопросы, направленные на уточнение причин выбора определенной программы магистерской подготовки, круга интересов поступающего и целей его поступления в магистратуру.

Максимальное количество баллов, которое может получить поступающий по результатам собеседования – 75 баллов.

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

Экзаменационная комиссия по приему вступительных испытаний в течение одного дня после проведения экзамена оценивает ответы поступающих и передает протоколы с результатами вступительных испытаний в приемную комиссию.

3.2. Порядок оценки индивидуальных достижений

Индивидуальные достижения оцениваются в день прохождения поступающим вступительных испытаний. Оцениваются только представленные в экзаменационную комиссию индивидуальные достижения в соответствии с разделом 2.

При учете п. 12 ИД экзаменационной комиссией устанавливается соответствие тематики профессиональной деятельности организации направлению подготовки магистратуры.

Экзаменационная комиссия оценивает представленные индивидуальные достижения в день проведения вступительных испытаний и передает протоколы оценки индивидуальных достижений вместе с протоколами результатов вступительных испытаний.

4. ПЕРЕЧЕНЬ ВОПРОСОВ, ВЫНОСИМЫХ НА ВСТУПИТЕЛЬНЫЕ ИСПЫТАНИЯ, ПО ОСНОВНЫМ УЧЕБНЫМ ДИСЦИПЛИНАМ

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

Вопросы для собеседования сгруппированы в три раздела.

В первый раздел включены вопросы из дисциплин: программно-аппаратные средства защиты информации; методы и средства криптографической защиты информации.

В второй раздел включены вопросы из дисциплины: защита информации от утечки по техническим каналам.

В третий раздел включены вопросы из дисциплин: организационное и правовое обеспечение информационной безопасности; основы управления информационной безопасностью.

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 34.12-2018. Режимы работы блочных шифров ГОСТ Р 34.13-2018. Алгоритм. Криптографические алгоритмы. Криптографическая стойкость. Иммитостойкость. Симметричные и асимметричные криптосистемы (общая характеристика).
19. Электронная подпись. Криптографические протоколы. Алгоритмы электронной подписи. Стандарт электронной подписи ГОСТ Р 34.10-2018. Функция

хеширования. Алгоритмы хеширования. Стандарт вычисления хеш-функции ГОСТ Р 34.11-2018.

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. Программно-аппаратные средства защиты информации: учебное пособие / В.А. Воеводин, А.В. Душкин, А.Н. Петухов, А.А. Хорев; под редакцией А.А. Хорева. – Москва: МИЭТ, 2021. – 280 с. – ISBN 978-5-7256-0972-1.

2. Программно-аппаратные средства защиты информации: учебно-методическое пособие / А.В. Душкин, О.Р. Лукманова, А.Н. Петухов, А.А. Хорев; под редакцией А.А. Хорева. – Москва: МИЭТ, 2021. – 216 с. – ISBN 978-5-7256-0958-5.

3. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов; под редакцией А.В. Душкина. – Москва: Горячая линия-Телеком, 2018. – 248 с. – ISBN 978-5-9912-0470-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111053 (дата обращения: 15.09.2021). – Режим доступа: для авториз. пользователей.

4. 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.

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.

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. 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. 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. Системы и средства пространственного электромагнитного излучения. 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 виброакустической 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.

Список рекомендуемой литературы по разделу 2

1. Дураковский А.П., Куницын И.В. Оценка защищенности речевой информации. Том. 4. Проведение инструментального контроля в канале высокочастотного навязывания: учеб. пособие. – М., НИЯУ МИФИ, 2018. - 50 с. ISBN: 978-5-7262-2494-7

2. Тельный, А. В. Техническая защита информации: Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и

характеристики: учеб. пособие/А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова. – Владимир: Изд-во ВлГУ, 2018 – 161 с. – URL: https://search.rsl.ru/ru/record/01009895283?ysclid=ls8uy3pm2a272241706 (дата обращения: 05.02.2024). – Текст: электронный.

3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: справочник / Г.А. Бузов // М.: Горячая линия-Телеком, 2018. — 586 с. — URL: https://e.lanbook.com/book/94625 (дата обращения: 15.09.2021).

4. Сагдеев К.М. Физические основы защиты информации [Электронный ресурс]: Учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига // СПб.: Интермедия, 2017. — 408 с. — Режим доступа: http://www.bibliocomplectator.ru/book/?id=66804 (дата обращения: 15.09.2021).

5. Технические средства и методы защиты информации: учебник для вузов/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков / Под ред. А.П. Зайцева, А.А. Шелупанова. – М.: Горячая линия – Телеком, 2018. – 444 с. – URL: https://e.lanbook.com/book/111057 (дата обращения: 01.03.2022). – ISBN 978-5-9912-0233-6. – Текст: электронный.

6. 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. Аналитическое обоснование необходимости создания системы комплексной защиты информатизации (СЗИ) ОИ (содержание, порядок проведения).
10. Техническое задание на разработку СЗИ ОИ.
11. Технический проект СЗИ ОИ.
12. Организационно-распорядительные документы по защите информации, разрабатываемые на ОИ.
13. Порядок организации аттестации ОИ. Программа и методика аттестационных испытаний.

14. Порядок проведения аттестации объекта СВТ по требованиям безопасности информации.

15. Порядок проведения аттестации выделенного помещения по требованиям безопасности информации.

16. Система управления информационной безопасностью (структура, взаимосвязь основных процессов управления и их основное содержание).

17. Роль концепции информационной безопасности в процессах управления информационной безопасности. Основные положения концепции информационной безопасности организации (предприятия).

18. Понятие политики информационной безопасности. Основные требования, принципы и подходы к разработке политики информационной безопасности.

19. Практические правила управления информационной безопасностью.

20. Понятие аудита ИБ. Цели аудита. Объекты аудита ИБ. Внешний аудит ИБ. Внутренний аудит ИБ.

Список рекомендуемой литературы по разделу 3

1. Вострецова Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

2. 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: 15.09.2021). - ISBN 978-5-534-03600-8 : 0-00. - Текст : электронный.

3. Малюк А.А. Защита информации в информационном обществе: учебное пособие / А.А. Малюк // М.: Горячая линия-Телеком, 2017. — 230 с. — URL: https://e.lanbook.com/book/111078 (дата обращения: 15.09.2021).

4. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие / В.К. Новиков // М.: Горячая линия-Телеком, 2017. — 176 с. — URL: https://e.lanbook.com/book/111084 (дата обращения: 15.09.2021).

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. 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.

7. 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.

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

Показателями оценки знаний по ответам на вопросы являются:

– понимание сущности излагаемого материала;

– грамотность изложения сути вопроса, умение использовать научную и специальную терминологию и вести диалог с комиссией;

– способность иллюстрировать ответ на теоретический вопрос практическими примерами.

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 суммарная бальная оценка за ответы на собеседовании составляет 75 баллов.

Итоговая оценка абитуриента определяется коллегиально членами экзаменационной комиссии на основании голосования простым большинством. При равном числе голосов голос председателя является решающим.

Результаты проведения вступительных испытаний оглашаются в день проведения вступительных испытаний по окончании собеседования.

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

Заведующий кафедрой
«Информационная безопасность»,
руководитель магистерской программы А.А. Хорев

«15» января 2024 г.