УТВЕРЖДАЮ
Проректор по образовательной деятельности
_____________ Л.А. Петручак
«01» октября 2019 года

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский государственный лингвистический университет»
(ФГБОУ ВО МГЛУ)

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (УРОВЕНЬ МАГИСТРАТУРЫ)

Направленность (профиль):
Информационная безопасность в международном сотрудничестве

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Москва
2019

Составители: О.Н. Ромашкова, доктор технических наук, профессор, заведующий кафедрой международной информационной безопасности Института информационных наук МГЛУ

И.А.Кириллов, кандидат технических наук, доцент, доцент кафедры международной информационной безопасности Института информационных наук МГЛУ

Программа вступительного испытания для поступления в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность» рассмотрена и утверждена на заседании Ученого Совета ФГБОУ ВО МГЛУ «30» сентября 2019 года, протокол № ______

1.Пояснительная записка

Программа вступительного испытания для поступления в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность» составлена на основе федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата), приказ № 1515 от 01.12.2016 г.). Программа определяет содержание и форму вступительного испытания.

Вступительное испытание в магистратуру проводится в форме собеседования с обязательным оформлением ответов на вопросы билета в письменном виде. Собеседование проводится с целью выявления у абитуриента объема знаний, необходимых для обучения в магистратуре.

Структура испытания: Испытание состоит из ответов на вопросы билета и дополнительные вопросы в рамках программы вступительного испытания. Билет состоит из 2 вопросов из перечня.

Оценка испытания: Оценка за собеседование выставляется по 100-балльной шкале.

Минимальный балл, необходимый для успешного прохождения собеседования и дальнейшего участия в конкурсе, ежегодно устанавливается приемной комиссией МГЛУ.

2. Содержание программы

1. Безопасность объекта как сущность состояния информационной обстановки. Факторы, оказывающие влияние на информационную безопасность.

2. Угрозы информационной безопасности. Классификация технических каналов утечки информации.

3. Прямой акустический канал утечки информации, методы и средства выявления и защиты.

4. Акусто-преобразовательные каналы утечки информации, методы и средства выявления и защиты.

5. Электрический канал утечки информации, методы и средства выявления и защиты.

6. Электромагнитный канал утечки информации, методы и средства выявления и защиты.

7. Оптический канал утечки информации, методы и средства выявления и защиты.

8. Сущность системы обеспечения информационной безопасности и принципы формирования в ней системы защиты информации.

9. Содержание организационных основ обеспечения информационной безопасности и защиты информации.

10. Силы, обеспечивающие информационную безопасность предприятия, в системе обеспечения его информационной безопасности. Роль органов управления предприятием в обеспечении его информационной безопасности.

11. Функции и задачи службы обеспечения информационной безопасности.

12. Средства обеспечения информационной безопасности предприятия в системе обеспечения его информационной безопасности.

13. Организационные аспекты защиты информации. Состав мероприятий по организации защиты информации на предприятии (организации, компании).

14. Сущность системы защиты информации, перечень и содержание мер по защите информации. Организационное построение и общая структурная схема системы защиты информации.

15. Основные международные стандарты в области информационной безопасности, их назначение и сфера применения.

16. Основные законы, законодательные акты и стандарты в Российской Федерации, регламентирующие вопросы в информационной безопасности и защиты информации, их назначение и сфера применения.

17. Установленные в Российской Федерации виды тайн, особенности их защиты.

18. Сущность, содержание, роль и место управления инцидентами в информационной безопасности и в обеспечении сервисов согласно положениям ГОСТ Р ИСО/МЭК ТО 18044-2007.

19. Содержание принципов эффективной политики реагирования на инциденты информационной безопасности.

20. Содержание политики расследования инцидентов информационной безопасности согласно положениям ГОСТ Р ИСО/МЭК ТО 18044-2007.

21. Сущность, роль, место и цель анализа информационных рисков.

22. Подходы к управлению информационными рисками. Оценивание рисков. Шкалы и критерии измерения.

23. Сущность, роль, место политик безопасности в организации работы предприятия. Содержание политики информационной безопасности согласно требованиям ГОСТ 13335-3-2006.

24. Структура и базовые принципы политики информационной безопасности.

25. Подходы к разработке политики безопасности информационных технологий согласно требованиям ГОСТ 13335-3-2006.

26. Особенности защиты персональных данных на предприятии (организации, компании), государственные регуляторы и их требования.

27. Режим защиты и обработки конфиденциальных документов на предприятии (организации, компании), основные этапы, мероприятия и сопровождающие документы.

28. Электронная цифровая подпись, организационные, технические и правовые аспекты.

29. Сущность, модели и принципы процессного подхода в совершенствовании информационной безопасности предприятия.

30. Алгоритм внедрения системы менеджмента информационной безопасности в соответствии с требованиями стандарта ISO/IEC 27001.

31. Виртуальные защищённые (частные) сети (Virtual Private Network - VPN), назначение, принципы построения, особенности выбора решения.

32. Инфраструктура открытых криптографических ключей, удостоверяющие центры и цифровые сертификаты.

33. Межсетевое экранирование компьютерных сетей, основные принципы и решаемые задачи. Особенности выбора и настроек межсетевого экрана.

34. Облачные вычисления. Защита информации в информационных системах, функционирующих на основе технологии облачных вычислений.

35. Разграничение доступа пользователей компьютерных систем, идентификация и аутентификация, основные понятия, программная и техническая реализация.

36. Системы контроля и управления доступом (СКУД) на объектах информатизации, решаемые задачи, программно-аппаратные решения.

37. Системы предотвращения и обнаружения вторжений в компьютерных системах и сетях, назначение, решаемые задачи, программные реализации.

3. Современные стандарты шифрования, используемые в компьютерных системах, их достоинства и недостатки.

4. Критерии оценки работы

100-95 баллов – даны исчерпывающие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует глубокие теоретические знания, умение сравнивать и оценивать различные научные подходы, пользоваться современной научной терминологией.

94-90 баллов – даны полные, достаточно глубокие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания, умение пользоваться современной научной терминологией.

89-85 баллов – даны обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания.

84-80 баллов – даны в целом правильные ответы на вопросы, поставленные экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы.

79-65 баллов – даны правильные ответы не на вопросы, поставленные экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы и не может привести практические примеры.

64-0 баллов – поступающий демонстрирует непонимание основного содержания теоретического материала, поверхностность и слабую аргументацию суждений или допущены значительные ошибки.

Оценка за вступительное испытание выставляется по 100-бальной системе. Набранные поступающий баллы должны превышать минимальный порог, установленный в МГЛУ.

Продолжительность экзамена — 1 астрономический час (30 минут - подготовка, 30минут - ответ).

Выходить из аудитории во время экзамена не разрешается.

4. Список рекомендуемой литературы

1. Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с.: ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429032.

2. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет».- Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с.: табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331.

3. Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.: табл., схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605.

4. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557.

5. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / авт.-сост. М.А. Лапина, Д.М. Марков, Т.А. Гиш, М.В. Песков и др. - Ставрополь : СКФУ, 2016. - 242 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012.

6. Кремер, А.С. Обеспечение доверия и безопасности при использовании ИКТ [Текст] : учебное пособие / А. С. Кремер, С. А. Мальянов, А. А. Малюк ;

Федер. агентсво связи ; Моск. техн. ун-т связи и информатики. - 2-е изд., доп. - М. : МТУСИ, 2017. - 314 с. : табл.

7. Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет.- Санкт-Петербург: Издательство Политехнического университета, 2014.-322 с.: схем., табл., ил. - ISBN 978-5-7422-4331-1; То же [Электронный ресурс]. URL : http//biblioclub.ru/index.php?page=book&id=363040.

Заведующий кафедрой международной
информационной безопасности О.Н. Ромашкова