Министерство образования и науки Российской Федерации
ФГАОУ ВО «Волгоградский государственный университет»
Институт приоритетных технологий
Кафедра информационной безопасности

УТВЕРЖДАЮ
Директор института
_____ И.В. Запороцкова
«26» 10 2023 г.

УТВЕРЖДАЮ
Председатель приемной комиссии
_____ А.Э. Калинина
«26» 10 2023 г.

ПРОГРАММА
вступительного испытания при приеме на обучение по программе магистратуры
Информационная безопасность

г. Волгоград, 2023 г.

1. Общие сведения

1.1. Цель проведения экзамена:

Вступительные испытания в магистратуру направлены на установление наличия у поступающих знаний, необходимых для продолжения обучения по направлению Информационная безопасность.

1.2. Форма проведения экзамена:

Вступительные испытания в магистратуру проводятся в форме портфолио и собеседования по нему, с возможностью проведения испытания в дистанционном режиме. Портфолио формируется абитуриентом по своему усмотрению, но должно включать копию вкладыша диплома бакалавра или специалиста с информацией об оценке итоговой аттестации и, хотя бы одну из перечисленных частей:

1) Выписка из протокола заседания государственной экзаменационной комиссии и заверенная копия листа ответа государственного экзамена по направлению «Информационная безопасность»;
2) Выпускная квалификационная работа бакалавра или специалиста (печатная или электронная версия);
3) Эссе на тему, соответствующую направлению магистратуры (тема выбирается абитуриентом из содержания программы самостоятельно).

Научные и академические достижения (индивидуальные достижения) оцениваются отдельно согласно правилам приема в ФГАОУ ВО «Волгоградский государственный университет» в 2024 году (высшее образование).

Предоставление эссе по выбранной теме предоставляется в установленный срок, а именно за 24 часа до проведения вступительного испытания на электронную почту указанной на сайте приемной комиссии.

1.3. Продолжительность экзамена:

Не регламентирована, зависит от количества подавших заявление на зачисление и предоставивших документы в приемную комиссию. Среднее время работы с одним поступающим – не более 20 минут.

2. Содержание программы:

Основные подходы к защите информации.

1. Резервное копирование. Полная копия. Разностная копия. Копия журнала транзакций. Резервное копирование файлов и групп. Планирование стратегии резервного копирования.
2. Правовой режим защиты государственной тайны. Правовые режимы защиты информации ограниченного доступа, не составляющей государственную тайну. Правовой режим защиты персональных данных.
3. Система лицензирования РФ. Лицензирование деятельности в области защиты информации. Органы лицензирования и их полномочия. Лицензируемые виды деятельности.
4. Сертификация средств защиты информации в системе сертификации ФСТЭК. Аттестация объектов информатизации по требованиям ФСТЭК.
5. Моделирование процессов защиты информации с использованием игровых моделей. Моделирование процессов защиты информации с использованием сетей Петри.
6. Типичный сценарий действий нарушителя. Сбор информации. Реализация атаки. Завершение атаки.
7. Средства обнаружения компьютерных атак. Признаки атак. Повтор определенных событий. Неправильные команды. Использование уязвимостей. Несоответствующие параметры сетевого трафика. Непредвиденные атрибуты. Необъяснимые проблемы. Дополнительные признаки.
8. Источники информации об атаках. Технологии обнаружения атак. Статистический анализ. Экспертные системы. Нейронные сети.

Криптографическая защита информации.

1. Введение в криптографию. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Классификация шифров. Модели шифров.
2. Шифры перестановки. Шифры подстановки. Шифры гаммирования. Алгоритмы формирования гаммы. Подходы к построению симметричных криптосистем.

3. Криптографическая стойкость шифров. Теоретически стойкие шифры. Имитостойкость шифров.

4. Системы шифрования с открытым ключом. Односторонние функции. Ассиметричная криптосистема RSA. Шифросистема Эль-Гамаля. Шифросистема Мак-Элиса.

5. Криптосистемы над группой точек эллиптической кривой. Схема открытого распределения ключей Диффи-Хеллмана над группой точек эллиптической кривой.

Программно-аппаратная защита информации.

1. Модель построения ПАСЗИ. Концепция диспетчера доступа. Состав подсистемы защиты информации: Подсистема управления доступом, Подсистема криптографической защиты. Подсистема регистрации и учета. Подсистема обеспечения целостности.
2. Состав типового комплекса защиты от несанкционированного доступа. Архитектура аппаратного контроллера.
3. Разграничение доступа. Дискреционная и мандатная модель разграничения доступа в СЗИ от НСД.
4. Электронные идентификаторы. eToken. PyToken, GuardantID; TouchMemory IButton, SMART-карты и магнитные пластиковые карты, RFID и Proximity карты. Применение электронных идентификаторов.

Техническая защита информации.

1. Демаскирующие признаки объектов в видимом, инфракрасном и радиодиапазоне.
2. Обоснование расчетных соотношений для обоснования дальности перехвата речевой информации.
3. Формирование маскирующей помехи на базе белого шума и определение её статистических характеристик.
4. Технические каналы утечки информации (ТКУИ) средствами приема, обработки, хранения и передачи информации (ТСПИ). Понятие ОТСС и ВТСС. Электромагнитный, электрический, параметрический ТКУИ.
5. Технические каналы утечки информации (ТКУИ) речевой информации. Акустический, виброакустический, электроакустический, оптико-электрический, параметрический.
6. Организация защиты речевой информации. Пассивные и активные средства защиты выделенных помещений. Методика проведения специальных исследований в области защиты речевой информации (виброаккустический канал).
7. Методы съема и защиты информации в линиях связи. Гальванический и индуктивный метод. Методы защиты.

3. Методика и критерии формирования оценки

3.1. На основании предоставленного портфолио предметная комиссия формирует итоговую оценку следующим образом по бальной шкале.

Оцениваются предоставленные части портфолио:

1) Выпускная квалификационная работа бакалавра или специалиста оценивается тем же баллом по 5-ти балльной шкале, который поставила государственная аттестационная комиссия. Перевод в 100-балльную шкалу проводится предметной комиссией на основании анализа текста работы по следующей шкале: «удовлетворительно» от 60 до 70 баллов, «хорошо» от 71 до 90 баллов, «отлично» от 91 до 100 баллов.

2) Оценка по государственному экзамену оценивается тем же баллом по 5-ти балльной шкале, который поставила государственная экзаменационная комиссия. Перевод в 100-балльную шкалу проводится предметной комиссией на основании анализа копии листа ответов по следующей шкале: «удовлетворительно» от 60 до 70 баллов, «хорошо» от 71 до 90 баллов, «отлично» от 91 до 100 баллов.

3) Эссе на выбранную тему выставляется предметной комиссией по результатам собеседования.

Баллы	Полнота ответов при собеседовании
91-100	Продемонстрировано уверенное знание выбранной тематики, понимание основных принципов, закономерностей предметной области, знакомство с историей развития предметной области. Возможны несущественные упущения

	при изложении или обсуждении вопроса.
81-90	Наличие упущений при изложении или обсуждении вопроса, которые абитуриент в состоянии исправить либо самостоятельно, либо отвечая на дополнительные вопросы предметной комиссии. При этом также продемонстрирован высокий уровень знакомства с предметной областью.
71-80	Наличие ошибок, серьезных упущений при изложении или обсуждении вопроса, устранить которые абитуриент смог только в процессе дискуссии. При этом также продемонстрирован хороший уровень знакомства с предметной областью
60-70	Абитуриент допускает серьезные ошибки при изложении или обсуждении тематики эссе, однако дает корректные ответы на дополнительные вопросы экзаменаторов. Продемонстрирован не глубокий уровень знакомства с предметной областью при обсуждении тематики эссе
31-59	Продемонстрирован поверхностный уровень знакомства с предметной областью при обсуждении тематики эссе
0-30	Продемонстрировано незнание предметной область и при обсуждении тематики эссе, не понимание ее основных принципов, закономерностей, незнание истории развития предметной области.

Итоговая оценка формируется как наибольшая из оценок представленных частей портфолио.

Если итоговая оценка составляет 60 баллов и более, то считается, что студент сдал вступительные испытания с положительной оценкой.

4. Список рекомендуемой литературы.

1. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft // Интуит НОУ, 2016
2. Проскурин В.Г. Защита в операционных системах, Горячая линия - Телеком, 2014
3. Лапонина О.Р. Криптографические основы безопасности // Интуит НОУ, 2016
4. Бехроуз А. Фороузан Математика криптографии и теория шифрования // Интуит НОУ, 2016
5. Басалова Г.В. Основы криптографии // Интуит НОУ, 2016
6. Федеральный закон Российской Федерации "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. N 149-ФЗ.
7. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1.
8. Скрипник Д. А. Общие вопросы технической защиты информации. Национальный Открытый Университет «ИНТУИТ». - 2016 г. - 425 с.
9. Инструментальный контроль и защита информации: учебное пособие. ВГУИТ. - 2013 г. - 192 с.
10. Сагдеев К. М., Петренко В. И., Чипига А. Ф. Физические основы защиты информации: учебное пособие. - СКФУ 2015 г. - 394 с.
11. Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 442 с. — Режим доступа: http://e. Программные средства защиты информации lanbook.com/book/5155
12. Долозов Н. Л., Гультяева Т. А.: конспект лекций. НГТУ – 2015 г. – 63 с.
13. Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография. Статут – 2016 г. 190 страниц
14. Курило А.П.., Милославская Н.Г., Толстой А.И., Сенаторов М.Ю. Основы управления информационной безопасностью. М.: Горячая линия-Телеком, 2014.
15. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. - М.: ГТК - 1992 г. - 13с.
16. Гостехкомиссия России. Руководящий документ: Средства вычислительной техники. Межсетевые экраны. Показатели защищенности от несанкционированного доступа. - М.: ГТК - 1997 г. - 17с.

17. Платунова, С.М. Построение корпоративной сети с применением коммутационного оборудования и настройкой безопасности. Учебное пособие по дисциплине «Корпоративные сети». [Электронный ресурс] — Электрон. дан. — СПб. : НИУ ИТМО, 2012. — 85 с.

18. Мэйволд Э.Безопасность сетей. Национальный Открытый Университет «ИНТУИТ» Национальный Открытый Университет «ИНТУИТ» – 2016 г. – 572 с.

19. Брэгг Р., Родс-Оусли М., Страссберг К.Безопасность сетей. Полное руководство

20. Советов, Б. Я. Моделирование систем : учебник для академического бакалавриата / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — М. : Издательство Юрайт, 2017. — 343 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-9916-3916-3.

21. Петров, А.В. Моделирование процессов и систем [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург : Лань, 2015. — 288 с. — Режим доступа: https://e.lanbook.com/book/68472. — Загл. с экрана.

22. Акопов, А. С. Имитационное моделирование : учебник и практикум для академического бакалавриата / А. С. Акопов. — М. : Издательство Юрайт, 2018. — 389 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02528-6.

23. Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1

24. Рембовский, А.М. Радиомониторинг: задачи, методы, средства. [Электронный ресурс] / А.М. Рембовский, А.В. Ашихмин, В.А. Козьмин. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 624 с.

25. Дятлов, А.П. Корреляционная обработка широкополосных сигналов в автоматизированных комплексах радиомониторинга. [Электронный ресурс] / А.П. Дятлов, Б.Х. Кульбикаян. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 332 с.

26. Кирсанов, Э.А. Обработка информации в пространственно-распределенных системах радиомониторинга: статистический и нейросетевой подходы. [Электронный ресурс] / Э.А. Кирсанов, А.А. Сирота. — Электрон. дан. — М. : Физматлит, 2012. — 344 с.

27. Сагдеев К. М., Петренко В. И., Чипига А. Ф. Физические основы защиты информации: учебное пособие. - СКФУ 2015 г. - 394 с.Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 442 с. — Режим доступа: http://e.lanbook.com/book/5155

28. ГОСТ Р 51320-99. Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных радиопомех.

29. Сакалема Д.Ж., Филинова А.С., Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) // Учебное пособие для вузов / М.: Горячая линия–Телеком, 2013. – 220 с.

30. О.И.Шелухин, А.Н.Руднев, А.В.Савелов Системы обнаружения вторжений в компьютерные сети // Учебное пособие. МТУСИ, Москва, 2013 г, 97 стр.

31. Богомолова О.Б., Усенков Д.Ю. Защита компьютера от вредоносных воздействий: практикум // М.: БИНОМ. Лаборатория знаний, 2012.— 175 с.

32. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие // Омск: Омский государственный университет, 2013.— 160 с.

33. Милославская. Н.Г. Вопросы управление информационной безопасностью Москва : Горячая линия-Телеком, 2013.

34. Сакалема Д.Ж., Филинова А.С., Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) // Учебное пособие для вузов / М.: Горячая линия–Телеком, 2015. – 220 с.

35. О.И. Шелухин, А.Н.Руднев, А.В.Савелов Системы обнаружения вторжений в компьютерные сети // Учебное пособие. МТУСИ, Москва, 2015 г, 97 стр.

36. Мошков М.Е. Введение в системное администрирование Unix // Интуит НОУ, 2016

Председатель предметной комиссии О.А. Какорина