	Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный технологический университет»
	Программа вступительных испытаний
	Высшее образование – программы магистратуры

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «ПГТУ»
_____ И.В. Петухов
"29" октября 2024 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ ДЛЯ ПРИЕМА НА НАПРАВЛЕНИЕ ПОДГОТОВКИ МАГИСТРОВ

10.04.00 Информационная безопасность

Рассмотрено на заседании экзаменационной комиссии по приему на направление подготовки магистров ***10.04.01*** **Информационная безопасность**

протокол № 1 от 29 .10.2024 г.

2024

	Должность	***Фамилия И.О. / Подпись***	***Дата***
Разработал	*Председатель экзаменационной комиссии по приему на направление подготовки магистров 10.04.01 Информационная безопасность*	*Сидоркина И.Г.*	29.10.24
Согласовано	*Первый проректор*	*Роженцов А.А. /*	29.10.24
Действует до момента переутверждения			

Переутверждена			
		Фамилия И.О. / Подпись	***Дата***
Утверждено	*Председатель экзаменационной комиссии по приему на направление подготовки магистров 10.04.01 Информационная безопасность*	*Сидоркина И.Г.*	
Согласовано	*Первый проректор*		
Переутверждена			
		Фамилия И.О. / Подпись	***Дата***
Утверждено	*Председатель экзаменационной комиссии по приему на направление подготовки магистров 10.04.01 Информационная безопасность*		
Согласовано	*Первый проректор*		
Переутверждена			
		Фамилия И.О. / Подпись	***Дата***
Утверждено	*Председатель экзаменационной комиссии по приему на направление подготовки магистров 10.04.01 Информационная безопасность*		
Согласовано	*Первый проректор*		
Действует до момента переутверждения			

ВВЕДЕНИЕ

Согласно правилам приема в Поволжский государственный технологический университет, конкурсный отбор в магистратуру на факультете информатики и вычислительной техники проводится на основе результатов вступительных испытаний.

Программа содержит перечень основных тем, рекомендуемых для подготовки к вступительным испытаниям по следующим дисциплинам:

- Теория вероятности и математическая статистика;
- Алгебра;
- Структура данных и алгоритмы;
- Теория информации и копирования;
- Теоретические основы безопасности автоматизированных систем.

Перечень дисциплин соответствует учебному плану основной образовательной программы подготовки магистров по направлению 10.05.01 «Комплексное обеспечение информационной безопасности автоматизированных систем».

В программе представлены демонстрационный вариант экзаменационного билета для магистратуры, система оценки экзаменационных работ.

I. ОСНОВНЫЕ РАЗДЕЛЫ ПО ДИСЦИПЛИНАМ, РЕКОМЕНДОВАННЫМ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНЫМ ИСПЫТАНИЯМ

Раздел 1. ТЕОРИЯ ВЕРОЯТНОСТИ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА

1. Вероятностное пространство. Аксиомы теории вероятности. Классическое определение вероятности.

2. Случайные величины, функции распределения, их свойства. Абсолютно непрерывные и дискретные распределения. Типовые распределения: биноминальное, пуассоновское, нормальное. Схема Бернулли и полиноминальная схема: основные формулы.

3. Условные вероятности. Независимость событий. Формула полной вероятности. Формулы Байеса. Независимые случайные величины.

4. Математическое ожидание случайной величины и его свойства. Вычисление математических ожиданий и дисперсий типовых распределений.

5. Виды сходимости последовательностей случайных величин. Закон больших чисел. Теорема Чебышева.

6. Центральная предельная теорема для независимых одинаково распределенных случайных величин.

7. Основные понятия математической статистики: случайная выборка из распределения, выборочное пространство, вариационный ряд, эмпирическая функция распределения, выборочное среднее, выборочные дисперсии, выборочные моменты. Точечные оценки известных значений параметров распределений: несмещенные оценки, состоятельные оценки. Примеры.

8. Задача проверки статистических гипотез. Основная и альтернативная, простая и сложная гипотезы. Статистические критерии. Ошибки 1-ого и 2-ого родов при проверки гипотез. Функция мощности критерия. Наиболее мощный и равномерно наиболее мощный критерии. Лемма Неймана-Пирсона. Проверка простых гипотез о параметрах биноминального, полиноминального и нормального распределений.

9. Критерии согласия. Критерий согласия Пирсона (критерий $\chi 2$). Теорема Пирсона о предельном распределении $\chi 2$-статистики (без доказательства).

Раздел 2. АЛГЕБРА

10. Группы: теорема Лагранжа, теорема об эпиморфизме групп, прямое произведение групп. Циклические группы и их свойства. Группы подстановок, теорема Кели, образующие симметрической и знакопеременных групп.

11. Кольца: идеалы колец, прямые суммы колец. Кольцо матриц над полем, определитель и ранг матрицы. Кольцо многочленов над полем, каноническое разложение многочленов над полем, НОД и НОК многочленов,

алгоритм Евклида. Кольцо вычетов, китайская теорема об остатках, малая теорема Ферма, решение линейных сравнений.

12. Поле частных коммутативного кольца без делителей нуля. Простые поля. Расширения полей. Поле разложения многочлена. Конечные поля и их свойства.

13. Линейное пространство над полем, линейно зависимые и независимые системы векторов, базис и размерность линейного пространства. Решение систем линейных уравнений над полем.

14. Линейные преобразования линейного пространства над полем, характеристический и минимальный многочлены линейных преобразований. Собственные значения и собственные вектора линейного преобразования. Нормальные формы матрицы, с помощью которой задано линейное преобразование линейного пространства над полем. Граф линейного преобразования. Евклидово пространство и его свойства. Ортонормированный базис.

Раздел 3. СТРУКТУРА ДАННЫХ И АЛГОРИТМЫ

15. Внутренняя сортировка данных. Простейшие алгоритмы сортировки: метод "пузырька", сортировка вставками, сортировка с помощью выбора. Временная сложность этих алгоритмов. Быстрая сортировка, оценка временной сложности в лучшем случае, в худшем случае и в среднем. Сравнение алгоритмов сортировки (простейших алгоритмов и быстрой сортировки), области их эффективного применения в зависимости от размерности задач.

16. Внешняя сортировка данных. Модель внешней сортировки, её особенности, определяющие "узкое" место процесса упорядочения данных во внешней памяти. Сортировка слиянием, оценка её временной сложности. Подходы к минимизации полного времени выполнения внешней сортировки.

Раздел 4. ТЕОРИЯ ИНФОРМАЦИИ И КОПИРОВАНИЯ

17. Информация, данные, сигналы. Источники информации и ее носители. Количество информации и энтропия. Формулы Хартли и Шеннона. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация. Помехоустойчивость передачи информации. Пропускная способность каналов связи. Теорема Шеннона для каналов без помех и с ними.

18. Типы сигналов, их дискретизация и восстановление. Спектральная плотность сигналов. Частота Найквиста, теорема Котельникова. Частотное представление дискретных сигналов. Ортогональные преобразования дискретных сигналов. Задачи интерполяции и прореживания сигналов.

19. Классификация кодов. Линейные коды. Оптимальное кодирование. Геометрический подход к кодированию. Неравномерные коды Хемминга. Циклические коды. Помехоустойчивое кодирование. Корректирующие коды.

Раздел 5. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

20. Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества. Анализ развития подходов к защите информации. Современная постановка задачи защиты информации.

21. Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации. Основное содержание теории защиты информации. Модели систем и процессов защиты информации.

22. Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации.

23. Постановка задачи определения требований к защите информации. Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации.

24.Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты.

25. Основные выводы из теории и практики защиты информации. Перспективы развития теории и практики защиты информации. Трансформация проблемы защиты информации в проблему обеспечения информационной безопасности.

Раздел 6. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

26. Структура и состав системы нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ. Общая характеристика правовых систем ограничения в доступе к информации.

27. Порядок отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Порядок доступа к государственной тайне физических и юридических лиц. Юридическая ответственность за противоправное распространение сведений, составляющих государственную тайну.

28. Регулирование вопросов обеспечения сохранности сведений ограниченного распространения в трудовых отношениях. Правовое

регулирование порядка посещения режимных организаций иностранными специалистами, особенности организации защиты информации при осуществлении международного сотрудничества.

29. Правовые основы лицензирования и сертификации в области защиты информации. Органы, уполномоченные на ведение лицензионной деятельности, и их полномочия.

30. Краткая уголовно-правовая характеристика преступлений, связанных с компьютерной информацией. Основы методики расследования преступлений в этой области.

31. Основные положения закона РФ "О частной детективной и охранной деятельности" в части установления правового статуса служб безопасности. Модели структуры и основные задачи служб безопасности коммерческих организаций.

32. Основные положения патентного законодательства и закона РФ "Об авторском праве и смежных правах".

33.Основные положения информационно-психологической безопасности и правовое регулирование в данной сфере. Основы психологической устойчивости при работе в экстремальных условиях. Основы психологического тестирования.

34. Основные положения закона РФ "Об электронной цифровой подписи". Содержание сертификата ЭЦП. Правовой статус и задачи удостоверяющих центров. Правовые основы функционирования электронных платежных систем.

Раздел 7. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

35. Суть криптографических методов защиты информации (ЗИ). Основные задачи по ЗИ, решаемые с использованием криптографических методов. Значение криптографических методов в комплексной системе ЗИ. Базовые понятия криптологии (шифр, ключи, протоколы, шифрсистема). Этапы развития криптологии. Криптография с секретным (симметричная) и открытым ключом (асимметричная). Основные различия. Криптографические примитивы и криптографические протоколы по защите информации.

36. Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы, задачи криптоаналитика. Теоретически стойкие шифры. Практическая стойкость шифров, её основные характеристики (трудоёмкость и надёжность дешифрования, количество необходимого материала). Связь между временной и вычислительной сложностью дешифрования. Классификация методов криптографического анализа.

37. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные). Итерационные системы блочного шифрования (шифры Фейстеля, IDEA, RIJNAEL). Режимы шифрования. Автоматные модели шифров.

38. Системный подход к построению практически стойких шифров. Характеристики случайности и непредсказуемости выходных последовательностей генераторов (периодичность, линейная сложность, статистические характеристики). Характеристики нелинейности отображений, реализуемых алгоритмами шифрования (сбалансированность, совершенность, строгий лавинный критерий, совершенная нелинейность, корреляционный иммунитет). Генераторы на основе линейных регистров сдвига (фильтрующие, комбинирующие, с неравномерным движением).

39. Криптография с открытым ключом. Предпосылки появления. Однонаправленные и однонаправленные функции с секретом и их применение. Схемы шифрования с открытым ключом и цифровой подписи. Основные принципы. Схемы шифрования и подписи RSA и Рабина. Схемы открытого шифрования Эль Гамаля. Сравнение криптосистем с открытым и секретным ключом. Новые схемы шифрования.

40. Электронная цифровая подпись. Основные понятия. Схемы цифровой подписи RSA и Рабина и их применение. Схема цифровой подписи Эль Гамаля и ее модификации. Способы ускорения процедур подписи и проверки. Стандарты цифровой подписи США (DSA) и России (ГОСТ Р 34.10). Методы генерации секретных параметров для стандартов цифровой подписи. Разновидности схем электронной цифровой подписи и их применение.

Раздел 8. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

41. Операционные системы: классификация операционных систем; концепция процесса, состояние процесса, алгоритм планирования процессов; процедуры синхронизации процессов по времени и по событиям; концепция семафоров; стратегия управления памятью; основные механизмы безопасности (аутентификация, разграничение доступа, аудит); управление безопасностью.

42. Вычислительные сети: безопасность ресурсов сети (средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа); безопасность локальных сетей (основные протоколы, службы, функционирование, средства обеспечения безопасности, управления и контроля); безопасность глобальных сетей (основные протоколы, службы и предоставляемые услуги, технология и механизмы обеспечения безопасности и управления распределенными ресурсами, стандарты и платформы); безопасность интранет (принципы построения и основные методы защиты).

43. Системы баз данных: принципы обеспечения безопасности баз данных различного типа; средства обеспечения безопасности баз данных (идентификация и аутентификация объектов баз данных, языковые средства разграничения доступа), концепция и реализация механизма ролей; организация аудита событий; средства контроля целостности информации; задачи и средства администратора безопасности баз данных.

44. Разновидности вредоносных компьютерных программ (ВрКП) и их особенности. Возможные вредоносные воздействия ВрКП. Определение и классификация вирусов, особенности классов. Средства борьбы с вирусными атаками. Методика применения средств борьбы с вирусами.

Раздел 9. ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

45. Концепция инженерно-технической защиты информации (ИТЗИ): характеристика ИТЗИ как области информационной безопасности; основные задачи, показатели эффективности и факторы, влияющие на эффективность ИТЗИ; базовые принципы и основные направления ИТЗИ.

46. Основные методы и средства защиты информации от утечки по техническим каналам.

47. Основные методы и средства инженерной защиты и технической охраны объекта.

48. Основные методы и средства защиты информации в каналах связи.

ЛИТЕРАТУРА

1. Малюк А.А, Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. - М.: Горячая линия - Телеком, 2001.-148с.
2. Герасименко В.А., Малюк А.А. Основы защиты информации: учебник для вузов; М., 1997.-538 с.
3. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. Учеб. пособие для вузов, П.Ю. Белкин, О.О. Михальский, А.С.Першаков и др.— М.: Радио и связь, 2000.-168с.
4. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах. Учеб. Пособие для вузов.- М.: Радио и связь, 2000.-168с.
5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учеб. Пособие для вузов.- М.: Гелиос АРИ, 2001.- 480с.
6. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учеб.пособие для вузов. - М.: ЮНИТА-ДАНА, 2000.-527с.
7. Фатьянов А.А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве). - М.: МИФИ, 1998.-285 с.
8. Торокин А.А. Основы инженерно-технической защиты информации. - М.:"Ось-89", 1998 г.- 336 с.
9. Доктрина информационной безопасности РФ.
10. Галочкин В.И. Структуры и алгоритмы обработки данных. Учебное пособие. – Йошкар-Ола: МарГТУ, 2004. – 148 с.
11. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. – М.: ГелиосАРВ, 2004. – 224 с.
12. Романец Ю.В., Тимофеев П.А., Шньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 348 с.
13. Ярочкин В.И. Информационная безопасность. – М.: Академический проект . Фонд "Мир", 2003. – 640 .
14. Вирт Н.Алгоритмы и структуры данных,1989.

15. ФароновВ.В.Турбо Паскаль (в 3-х кн.) ,1992.

16. Гаранин М. В. Системы и сети передачи информации,2001.

17. Каган, Борис Моисеевич. Электронные вычислительные машины и системы: Учеб. Пособие для вузов по спец. "Вычисл. машины, комплексы, системы и сети", "Прогр. обесп. выч. техн. и автомат. систем".-3-е изд., перераб. и доп. М. Энергоатомиздат, 1991.590[1]с.:ил SBN 5-283-01531-9:2.00:560.00.

18. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии ,протоколы: Учеб. пособие для студ-ов вузов, обуч. по направлению "Информатика и выч. техника" и по спец."Выч. машины, комплексы, системы ,сети" и др. СПб.и др.: Питер,2001.-668с. ISBN 5-8046-0133-4:75.00.

19. Медведовский И.Д., Безгачев В.А., Гореленков А.П. Информационная безопасность распределенных вычислительных систем. Рук-во к практ. занятиям. – С.-Петербург, 73 с.1998.

20. Мельников, В. В.. Защита информации в компьютерных системах.- М.:Финансы и статистика: Электронинформ,1997.-364с.:ил. ISBN 5-279-01631-4:42000.00: 30000.00:25500.00:41.00:48.60.

21. Безопасность сети на основе Microsoft Windows 2000: Учебный курс MCSE: Официальное пособие Microsoft для самостоятельной подготовки:[Пер. с англ.].-.:Русская Редакция,2001. 847, [3] с. :ил. + CD-ROM.-(Гарантия квалификации) ISBN5-7502-0176-7:311.99. Хранение: кнхр-591781.

22. Карпова, Т. С.. Базы данных: модели, разработка, реализация: Учебник].-СПб .и др.:Питер,2001.-303с.:ил. ISBN 5-272-00278-4:85.00.

23. Гаврилова Т.А., Хорошевский В.Ф. Базы знаний интелл-х систем: Учеб. Пос. для вузов по напр. "Прик. матем. и информ.", "Информ и вычис. тех." спец. "Прикл. инфом." (по обл. Прикл. матем. и информ.".- СПб. и др.:,2001.-382с.

24. Виноградова С.М. Войтович Н.А. Вус М.А. Информационное общество. Информационные войны. Информационное управление. Информационная безопасность.1999.

25. Расторгуев С.П. Информационная война.1998.

26. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агенства "Яхтсмен", - 1996. –92 с.1996

27. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. –М.: Радио и связь, 2000. –192 с.2000

28. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем 2000.

29. Романец, Ю. В. и др.Защита информации в компьютерных системах и сетях /В.Романец, П.А.Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф.Шаньгина. -М.: Радио и связь,1999.-328.с.ISBN 5-256-01436-6:36.55:38.00:84.00.

30. Ярочкин В.И. Информационная безопасность. М. Международные отношения.2000

31. Петраков А.В.Охрана и защита современного предприятия. М. Энергоатомиздат.1999

32. Баричев С.Г. и др. Основы современной криптографии: Учебный курс. 2-е изд. Баричев С.Г., Гончаров В.В., Серов Р.Е. М.: Горячая линия-Телеком,2002.

33. Криптографические методы защиты информации в компьютерных системах и сетях: [Учеб. пособие] Иванов, М. А.. М.: КУДИЦ-ОБРАЗ, 2001.

34. Хорев А.А. Способы и средства защиты информации.1998.

35. Меньшаков Ю.К. Защита информации от технических разведок.2001.

36. Конявский В.А. Программно-аппаратные средства защиты информации. – М,2002

37.Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности: Защита в операционных системах. — М.: Радио и связь,2000.

38. Программно- аппаратные средства обеспечения информационной безопасности: Защита программ и данных: Учеб. пособ. для студ-ов вузов, обуч. по спец. "Защищен. телекоммуникац. Системы", "Комплекс. обеспечение инф. безопасности автоматизирован.систем" /[П.Ю.Белкин, О.О.Михальский, А.С.Першаков и др.].-М.:Радио и связь,1999.-168,[1] с. ISBN 5-256-01416-1:26.00.

39. Проскурин В.Г. Программно-аппаратные средства информационной безопасности: защита программ и баз данных.2000.

40.Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности,2000.

41. Щербаков А.Ю.Введение в теорию и практику компьютерной безопасности,2001.

42. Зегжда, Д. П., Ивашко, А. М. Основы безопасности информационных систем: Учеб. Пособие для вузов по спец. "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизир. систем". - М.: Горячая линия-Телеком, 2000.-449,[2]с. ISBN 5-93517-018-3:99.00.

II. ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Билет состоит из 4 вопросов.
Форма нулевого варианта билета

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

По дисциплине Вступительный экзамен в магистратуру

Направление 10.04.01 «Комплексное обеспечение информационной безопасности автоматизированных систем»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 0

1. Поле частных коммутативного кольца без делителей нуля. Простые поля. Расширения полей. Поле разложения многочлена. Конечные поля и их свойства.
2. Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации.
3. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные). Итерационные системы блочного шифрования (шифры Фейстеля, IDEA, RIJNAEL). Режимы шифрования. Автоматные модели шифров.
4. Основные методы и средства защиты информации от утечки по техническим каналам.

Председатель экзаменационной комиссии _____ «___»_____201__ г.

III. СИСТЕМА ОЦЕНКИ ЭКЗАМЕНАЦИОННЫХ РАБОТ

Работы оцениваются по 100 балльной шкале.

В билете содержится 4 вопроса, каждый правильный ответ оценивается максимально в 25 баллов.

Минимальное количество баллов по итогам вступительных испытаний, необходимое для поступления в ФГБОУ ВО «ПГТУ» на направление подготовки 10.04.01 «Информационная безопасность» - 50.