Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тверской государственный университет»

Рассмотрено и рекомендовано
на заседании Ученого совета
математического факультета
протокол № 2 от 26.09.2017

«УТВЕРЖДАЮ»:
Руководитель ООП
Семыкина Н.А.
«__» 09 2017 г.

ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

по специальности 10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Уровень высшего образования
СПЕЦИАЛИТЕТ

Тверь 2017 г.

Пояснительная записка

Экзамен является междисциплинарным, проводится в соответствии с графиком учебного процесса. Цель экзамена – проверка овладения выпускником основных компетенций, требуемых в профессиональной деятельности.

К участию в государственном экзамене допускаются студенты, полностью выполнившие учебный план и не имеющие академической задолженности.

Экзамен может проводиться за один или несколько дней в зависимости от количества студентов, допущенных для его прохождения.

Экзамен проводится в устной форме. Каждый билет содержит два теоретических вопроса и одну задачу по теме, входящей в программу итогового квалификационного экзамена. В качестве вопросов формулируются основные теоретические положения, предполагающие их развернутое обоснование при ответе.

Время, выделяемое на подготовку ответов и выполнение задания – 1 час. Ответ студента производится в форме выступления перед членами Государственной экзаменационной комиссии, допускается использование записей, сделанных студентом при подготовке к ответу на вопросы комиссии. Продолжительность ответа 10–15 минут. Членами государственной экзаменационной комиссии студенту могут быть заданы дополнительные вопросы, относящиеся к дисциплинам, входящим в программу государственного экзамена.

Перечень компетенций, уровень сформированности которых будет оцениваться на экзамене

ОПК-2. способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теория

информации, теоретико-числовых методов.

ПК-5. способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

ПК-7. способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем.

ПК-15. способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

ПСК-2.1. способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации.

ПСК-2.2. способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.

ПСК-2.3. способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.

ПСК-2.5. способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

Требования к профессиональной подготовленности специалиста.

Математик, специалист по компьютерной безопасности, должен знать и уметь использовать:

- основные понятия и методы математического анализа, геометрии, алгебры, теории функций комплексного переменного, теории вероятностей и математической статистики;

- математические модели простейших систем и процессов в естествознании и технике;

- вероятностные модели для конкретных процессов и явлений, проводить необходимые расчеты в рамках построенной модели;

- основные понятия и методы математической логики и теории алгоритмов, теории передачи информации, теории кодирования;

- современные методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;

- принципы и методы организационной защиты информации в различных сферах деятельности государства;

- принципы построения современных систем защиты информации в компьютерных системах;

- руководящие документы по оценке защищенности компьютерных систем;

- методы проведения анализа надежности системы защиты информации в компьютерных системах;

- принципы построения современных криптографических систем;

- методы криптографического анализа типовых криптографических алгоритмов и протоколов;

- стандарты в области криптографической защиты информации;

- основные правовые понятия по проблемам информационной безопасности и защиты информации; владеть:

- методами разработки и исследования моделей надежности и безопасности компьютерных систем;

- методами организации деятельности подразделений защиты информации;

- методикой разработки нормативно-методических документов по организационной защите информации;

- методами определения организационных и технических каналов утечки информации.

Критерии оценки итогового государственного экзамена

Оценка ответа на вопрос (выполненного задания) выставляется членами Государственной экзаменационной комиссии.

Возможные оценки на государственном экзамене: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Результаты проведения государственного экзамена оглашаются после окончания государственного экзамена в день его проведения.

Отметка «**ОТЛИЧНО**». Ответ студента полный и правильный, содержит четкие формулировки и подтверждается примерами. Студент уверенно отвечает на дополнительные вопросы, свободно ориентируется в вопросах билета. Материал изложен в определенной логической последовательности, литературным языком, с использованием современных научных терминов; ответ самостоятельный.

Отметка «**ХОРОШО**». Ответ студента правильный. Студент показал знание основного программного материала. Студент испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Соблюдены нормы литературной речи. Ответ самостоятельный.

Отметка «**УДОВЛЕТВОРИТЕЛЬНО**». Студент показал поверхностные знания вопросов билета в объеме, необходимом для предстоящей работы по профессии. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Студент испытывает достаточные трудности в ответах на дополнительные вопросы. Научная терминология используется недостаточно, незначительные нарушения норм литературной речи.

Теоретические вопросы для проверки уровня сформированности компетенции ОПК – 2.

Математический анализ

1. Непрерывность действительных функций одного и многих действительных переменных. Свойства непрерывных функций.
2. Дифференцируемость функций одного и многих действительных переменных в точке и на множестве. Достаточные условия дифференцируемости. Производные и дифференциалы высших порядков. Теоремы о среднем для действительных функций одного действительного переменного (Ролля, Лагранжа, Коши).
3. Формула Тейлора для действительных функций одного и многих действительных переменных и ее применение. Экстремум действительной функции одного и многих действительных переменных достаточные условия его существования.
4. Числовой ряд. Сходящиеся ряды и их свойства. Признаки сходимости рядов с положительными членами (признаки сравнения, Даламбера, Коши). Абсолютная сходимость. Признак Лейбница.
5. Функциональные ряды. Равномерно сходящиеся ряды. Непрерывность суммы равномерно сходящегося ряда непрерывных функций. Теоремы о почленном интегрировании и дифференцировании ряда. Степенные ряды. Область и радиус сходимости степенного ряда. Равномерная сходимость степенного ряда. Непрерывность суммы, почленная дифференцируемость. Ряд Тейлора для функции одного действительного переменного.

Геометрия

1. Различные виды уравнения прямой на плоскости и в пространстве. Расстояние от точки до прямой на плоскости. Угол между двумя прямыми.

2. Скалярное, векторное, смешанное произведение векторов в пространстве, их свойства, выражение через координаты сомножителей.

Алгебра

1. Матрицы и операции над ними. Определители матриц и их свойства. Определитель произведения матриц. Критерий обратимости матриц. Ранг матрицы над полем, способы его вычисления. Ранг произведения матриц. Обратная матрица и способы ее вычисления.
2. Системы линейных уравнений над полем. Критерий Кронекера-Капелли. Алгоритм Гаусса. Фундаментальная система решений однородной системы линейных уравнений. Общее решение системы линейных уравнений.
3. Кольцо многочленов над кольцом с единицей. Делимость многочленов с остатком. Теорема Безу. Делимость многочленов над полем. Наибольший общий делитель (НОД) и наименьшее общее кратное многочленов. Взаимно простые многочлены и их свойства. Неприводимые многочлены и их свойства. Каноническое разложение многочлена и его однозначность.
4. Евклидово пространство. Существование ортонормированного базиса. Ортогональное дополнение подпространства.

Дискретная математика

1. Булевы функции, их суперпозиция. Полные системы булевых функций. Примеры полных систем. Замкнутые классы булевых функций. Общий критерий полноты.

2. Автоматные языки, примеры. Необходимые условия автоматности языка. Автоматность однословного и конечного языка. Пример неавтоматного языка.

Математическая логика и теория алгоритмов

1. Исчисления высказываний и предикатов, их полнота и непротиворечивость.

2. Основные подходы к формализации понятия алгоритма: машины Тьюринга, рекурсивные функции.
3. Понятие сложности алгоритма. Классы сложности.

Теория вероятностей и математическая статистика

1. Вероятностное пространство. Аксиомы вероятности. Свойства вероятности меры. Дискретное вероятностное пространство. Классическое определение вероятностей

2. Случайные величины. Функции распределения и их свойства. Абсолютно непрерывные, дискретные распределения. Типовые распределения: биномиальное, равномерное, геометрическое, пуассоновское, нормальное, показательное.

3. Условные вероятности. Независимость событий. Формула полной вероятности. Формула Бейеса.

4. Математическое ожидание случайной величины и его свойства. Вычисление математических ожиданий для типовых распределений. Дисперсия случайной величины и ее свойства. Коэффициент корреляции и его свойства.

5. Основные понятия математической статистики: понятия генеральной совокупности, выборки, дискретного вариационного ряда, эмпирической функции распределения, выборочных моментов. Примеры использования этих понятий в практических задачах.

6. Основные методы статистического оценивания. Метод моментов. Метод максимального правдоподобия. Применение к случаю нормального и биномиального распределения.

Практические вопросы для проверки уровня сформированности компетенции ОПК – 2.

1. Решите задачу Коши $\frac{dy}{dx} = \frac{y}{x+1}; \quad y(1) = 2$.
2. Решите задачу Коши $y'' - 2y = 0, \quad y(0) = 0, \quad y'(0) = 1.$

3. Решите задачу Коши $y'' + 4y = 0, \quad y(0) = 2, \quad y'(0) = 1.$

4. Исследовать на сходимость числовой ряд $\sum_{n=1}^{\infty} \frac{2^n n!}{n^n}$.

5. Исследовать на сходимость числовой ряд $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n(n+1)^2}$.

6. Исследовать на сходимость числовой ряд $\sum_{n=1}^{\infty} \frac{2n-1}{3^n}$.

7. Вычислить неопределенный интеграл $J = \int \frac{dx}{(x-1)(x-2)}$.

8. Вычислить определенный интеграл $J = \int_0^{\pi} x^2 \sin x \, dx.$

9. Найдите собственные значения (числа) и собственные векторы линейного преобразования, заданного матрицей $\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$

10. Найти общее решение системы уравнений и какую-нибудь её фундаментальную систему решений

$$\begin{cases} x_1 + x_3 = 0 \\ x_2 + x_6 = 0 \\ x_3 + x_6 = 0 \\ x_4 + x_7 = 0 \end{cases}$$

11. Выясните, какая из следующих формул логики предикатов тождественно истина, а какая – нет. Результат обоснуйте.

a) $\neg \forall x \exists y \; P(x, y) \to \forall y \exists x \, P(x, y)$;

b) $\exists x P(x) \wedge \exists x Q(x) \to \exists x (P(x) \wedge Q(x))$.

12. С помощью основных равносильностей приведите формулу логики высказываний

$$\neg(p \to \neg(q \to \neg r \vee p)) \wedge (q \to p \wedge r)$$

к дизъюнктивной нормальной форме. Результат проверьте построением истинностных таблиц для исходной и полученной формул.

13. Обосновав результат, запишите формулу логики высказываний $\phi(p, q, r)$, имеющую следующую таблицу истинности:

p	И	И	И	И	Л	Л	Л	Л
q	И	И	Л	Л	И	И	Л	Л
r	И	Л	И	Л	И	Л	И	Л
$\phi(p,q,r)$	И	Л	Л	И	Л	И	Л	Л

Результат обоснуйте.

Теоретические вопросы для проверки уровня сформированности компетенции ПК – 5.

1. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники (атаки на уровне систем управления базами данных. Атаки на уровне операционной системы. Атаки на уровне сетевого программного обеспечения. Программные закладки).
2. Классификация угроз информационной безопасности. Угрозы информационной безопасности баз данных.
3. Проектирование баз данных. E-R диаграммы. Нормальные формы отношений. Нормализация.
4. Реляционная алгебра. Основные определения, операторы. Реализационная полнота языка SQL.

Практические вопросы для проверки уровня сформированности компетенции ПК – 5.

1. Структура базы данных «Учредительство» содержит следующие таблицы:

• «Лицо» — *Код, ФИО, Дата рождения. Месторождения, Паспортные данные;*

• «Организация» — *Код ОКПО, Наименование, Условное наименование, Профиль деятельности* (Производственный, Коммерческий, Посреднический, научно-производственный), *Организационная форма* (ЗАО, ОАО, и т. д.). *Код Руководителя, Код глав. бухгалтера, Телефон;*

• «Учредительство»—*Код, Код учредителя-лица, Код учредителя-организации, Код учрежденной организации, Дата учреждения, Данные документа учредительства, Доля капитала, Форма капитала;*

• «Адрес» — *Код, Код Лица, Код Организации, Город, Район, Улица, № дома, № квартиры, Дата начала, Дата окончания.*

Вводом и корректировкой данных занимаются несколько сотрудников, за каждым из которых закрепляется регистрация и ведение БД по различным организационным формам, профилю деятельности и району размещения регистрируемых организации. Для работы и доступа только к «своим» данным составьте представления объектов (таблиц) базы данных сотруднику Петрову, отвечающему за регистрацию посреднических акционерных обществ, размещающихся в Железнодорожном районе, и предоставьте ему соответствующий доступ.

2. В базе данных «Штаты подразделений» содержатся следующие таблицы:

• «Сотрудники»— *Таб.№, ФИО, Подразделение, Должность (шт. категория);*

• «Штатные категории» — *Код категории, Наименование* (Начальник отдела. Зам. начальника отдела. Начальник сектора, Ведущий инженер. Старший инженер. Инженер, Техник), *должностной оклад;*

• «Подразделения»— *№№, Наименование, Руководитель;*

• «Штаты» —*№№ подразделения, Код штатной категории, Количество должностей.*

База данных необходима для обеспечения работы руководителей структурных подразделений (справочные функции), сотрудников отдела кадров (ведение базы данных) и бухгалтерии (использование в

начислении заработной платы). Составьте и обоснуйте целесообразную систему рабочих групп пользователей и таблицу доступа к объектам базы данных.

3. В базе данных «Преподаватели и занятия» содержатся следующие таблицы:

• «Преподаватели» — *Таб.№, ФИО, Кафедра* (Истории, Архивоведения, Документоведения), *Должность* (Зав.каф, Профессор, Преподаватель, Ассистент), *Ученая степень* (Кандидат наук, Доктор наук), *Ученое звание* (Старший научный сотрудник, Доцент, Профессор, Академик);

• «Контракты/Труд.Соглашения» — *№№. Код Преподавателя, Дата заключения, Срок действия, Ставка, Особые условия;*

• «Дисциплины»—*Код дисциплины, Наименование, Количество часов в учебном плане, Форма отчетности* (Экзамен, Дифференцированный зачет. Зачет);

• «Занятия» — *Дата, Время* (1-я пара, 2-я пара, 3-я пара, 4-я пара). *Аудитория, Вид* (Лекция, Практическое занятие, Семинар, Лабораторная работа. Экзамен, Зачет), *Преподаватель, Дисциплина, Код уч. группы;*

• «Итоги сессии» — *Код, Семестр, Код дисциплины, Код Студента, Отметка, Код Преподавателя*

• «Учебные группы» — *Код группы* (И101, И102, И103, И104, И105 и т.д.), *Специализация* (История, Архивоведение, Документоведение), *Таб.№_старосты, Таб.№№_куратора;* • «Студенты» — *Таб.№№, ФИО, Год рождения, Уч. группа, Отметка о переводе на след.курс.*

База данных необходима для методистов учебного отдела (составление и ведение расписания занятий, учетная работа по распределению студентов по группам, итогам сессий), профессорско-преподавательскому составу (справки по расписанию занятий), работникам отдела кадров (ведение установочных данных по преподавателям и студентам), студентам (справки по расписанию занятий). Составьте и обоснуйте целесообразную систему рабочих групп пользователей и таблицу доступа к объектам базы

данных.

Теоретические вопросы для проверки уровня сформированности компетенции ПК – 7.

1. Методы и средства защиты информации. Защита информации, обрабатываемой техническими средствами.
2. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание
3. Информационная безопасность в системе национальной безопасности Российской Федерации. Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.
4. Государственная информационная политика. Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности

Практические вопросы для проверки уровня сформированности компетенции ПК – 7.

1. При работе ПК необходимо периодически приостанавливать обработку информации и проверять ПК на наличие в нем вирусов. Приостановка в обработке информации приводит к определённым экономическим издержкам. В случае же если вирус вовремя обнаружен не будет, возможна потеря и некоторой части информации, что приведёт и ещё к большим убыткам.

   Варианты решения таковы:

   E1– полная проверка;

   E2– минимальная проверка;

   E3– отказ от проверки.

ПК может находиться в следующих состояниях:

- *F1*– вирус отсутствует;
- *F2*– вирус есть, но он не успел повредить информацию;
- *F3*– есть файлы, нуждающиеся в восстановлении.

Результаты, включающие затраты на поиск вируса и его ликвидацию, а также затраты, связанные с восстановлением информации, имеют вид:

	F_1	F_2	F_3
E_1	-20.0	-22.0	-25.0
E_2	-14.0	-23.0	-31.0
E_3	0	-24.0	-40.0

Используя критерий Вальда, определить оптимальную альтернативу.

2. Исходные данные аналогичны 22 заданию. Используя критерий Байеса-Лапласа, определить оптимальную альтернативу.

3. Исходные данные аналогичны 22 заданию. Построить матрицу потерь и определить вариант действий, используя критерий Сэвиджа.

Теоретические вопросы для проверки уровня сформированности компетенции ПК – 15.

1. Организация инженерно-технической защиты информации. Организационно-методические основы защиты информации. Общие требования к защите информации
2. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации. Методика принятия решения на защиту от утечки информации в организации.
3. Мероприятия по выявлению каналов утечки информации. Специальные проверки. Порядок проведения специальной проверки технических средств

Практические вопросы для проверки уровня сформированности компетенции ПК – 15.

1. Руководству фирмы предлагается выбрать одну из трех программ обслуживания по защите от утечки информации. Условия этих программ следующие:

Программа 1. Ежемесячная стоимость обслуживания 24 у.е. Фирма самостоятельно оплачивает все счета общей суммой до 500 у.е. в год, после этого оплачивает 90% суммы счетов, сверх этих 500 у.е.

Программа 2. Аналогична программе 1, но стоимость обслуживания в месяц 1 у.е. и самостоятельно оплачиваются счета, составляющие в сумме до 1 000 у.е. в год.

Программа 3. Ежемесячная стоимость 30 у.е. Фирма оплачивает 30% всех счетов.

Распределение вероятностей годовых затрат на обслуживание приведено в таблице:

Затраты	Вероятность
200	0,3
600	0,5
1000	0,15
5000	0,03
15000	0,02

Требуется определить, какая из программ обслуживания наиболее выгодна для фирмы.

2. Фирма рассматривает вопрос о приобретении одного из двух комплектов ПО. Оба комплекта полностью отвечают потребностям фирмы на следующие 3 года. Комплект 1 стоит 2 000 у.е. Имеется соглашение на техническое обслуживание, по которому ежегодная плата за обслуживание составляет 150 у.е. По этому договору все неполадки устраняются без дополнительной оплаты. Комплект 2 стоит 3 000 у.е., его техническое обслуживание не

оговаривается. По оценкам фирмы есть 40% вероятность того, что ежегодная стоимость обслуживания комплекта 2 будет составлять 0 у.е., 40% вероятность того, что стоимость обслуживания составит 100 у.е. и 20% вероятность того, что стоимость обслуживания составит 200 у.е.. Перед покупкой комплекта 2 фирма может дополнительно его протестировать. Если тест покажет высокое качество, то имеется 60% вероятность того, что стоимость ежегодного обслуживания будет отсутствовать и 40% вероятность того, что стоимость ежегодного обслуживания составит 100 у.е.. Если результат теста будет всего лишь удовлетворительным, то с вероятностью 20% ежегодная стоимость обслуживания будет 0 у.е., с вероятностью 40% – $100 и с вероятностью 40% – 200 у.е.. Ожидается, что результат теста будет удовлетворительным с вероятностью 50%. Стоимость дополнительного тестирования равна 40 у.е. Какое решение следует принять фирме?

Теоретические вопросы для проверки уровня сформированности компетенции ПСК – 2.1.

1. Блочные шифры. ГОСТ 28174-89; Rijndeal (AES).
2. Криптосистемы с открытым ключом. Понятие сертификата. Криптосистема *RSA*. Выбор параметров.
3. Сжатие информации. Универсальные методы сжатие информации. Классы методов сжатия.

Практические вопросы для проверки уровня сформированности компетенции ПСК – 2.1.

1. Определить ключ аффинного матричного преобразования (Шифр Хилла), если открытый текст:
   $X = \begin{pmatrix} 15 & 14 & 8 \\ 5 & 16 & 1 \\ 3 & 11 & 30 \end{pmatrix} (\text{mod } 32)$, $X^{-1} = \begin{pmatrix} 13 & 20 & 30 \\ 5 & 26 & 17 \\ 15 & 29 & 26 \end{pmatrix} (\text{mod } 32)$,
   $Y = \begin{pmatrix} 15 & 6 & 26 \\ 15 & 23 & 1 \\ 6 & 29 & 16 \end{pmatrix} (\text{mod } 32)$.
2. Вскрыть шифр аффинного преобразования y=Lx+a(mod32) если

$$L = \begin{pmatrix} 19 & 4 & 8 \\ 10 & 11 & 24 \\ 28 & 20 & 23 \end{pmatrix},$$

a=(1,2,3) и x1=(7,8,12), x2=(13,5,5), x3=(17,14,11), x4=(13,22,5) и y1=(5,30,24), y2=(19,17,3), y3=(19,12,17), y4=(23,12,23).

3. Вскрыть криптограмму 352420381123243438202416223324331538241116232 4 числовые эквиваленты букв открытого текста заданы следующим образом А=01, Б=02…Я=33.
4. Расшифровать фразу, зашифрованную столбцовой перестановкой**.** ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
5. Провести кодирование, используя метод Шеннона – Фано и методику Хаффмена.

сообщение	1	2	3	4	5	6	7
вероятность	0,4	0,2	0,1	0,1	0,1	0,05	0,05

6. Построить циклический код длины 7 с порождающим многочленом $g(x) = x^4+x^2+x+1$. Найти его проверочный многочлен. Найти порождающую и проверочную матрицу.

Теоретические вопросы для проверки уровня сформированности компетенции ПСК– 2.2.

1. Понятия генератора псевдослучайных чисел и последовательности псевдослучайных чисел (ППЧ).
2. Понятия квазипериода последовательности псевдослучайных чисел, стартовой позиции квазипериода (ППЧ) и его длины. Необходимое и достаточное условие для квазипериода произвольной последовательности псевдослучайных чисел и его стартовой позиции.
3. Понятия периода последовательности псевдослучайных чисел, стартовой позиции периода (ППЧ) и его длины. Необходимое и достаточное условие для периода произвольной последовательности псевдослучайных чисел и его стартовой позиции.

4. Описание бескоалиционной игры Г двух лиц, моделирующей процесс обеспечения компьютерной системы средствами защиты. Свойства отношения доминирования на множестве стратегий игрока, реализующего процесс обеспечения компьютерной системы средствами защиты в игре Г.
5. Описание бескоалиционной игры Г двух лиц, моделирующей процесс обеспечения компьютерной системы средствами защиты. Гарантированный выигрыш игрока, реализующего процесс обеспечения компьютерной системы средствами защиты в игре Г.

Практические вопросы для проверки уровня сформированности компетенции ПСК– 2.2.

1. Используя значения параметров линейного конгруэнтного генератора, выяснить, является ли длина периода последовательности псевдослучайных чисел, формируемой генератором, максимальной.
2. Найти период последовательности псевдослучайных чисел, формируемой заданным линейным конгруэнтным генератором.
3. Найти множество максиминных стратегий некоторого игрока в заданной бескоалиционной игре.
4. Найти множество недоминируемых стратегий некоторого игрока в заданной бескоалиционной игре.

Теоретические вопросы для проверки уровня сформированности компетенции ПСК – 2.3.

1. Применение искусственных нейронных сетей в информационной и компьютерной безопасности. Динамические нейронные сети и методы их исследования.
2. Нейронные сети и проблемы искусственного интеллекта. Классификация ИНС. Способы обучения ИНС.

Практические вопросы для проверки уровня сформированности компетенции ПСК – 2.3.

1. Требуется провести оценку защищенности компьютерной сети по классу средств вычислительной техники (СВТ). Ниже в таблице приведены результаты оценивания значимость каждого критерия балльным методом (10-балльная шкала) двумя экспертами. Выставите свои оценки за 3 эксперта и определите четыре основных критерия. Найдите весовые коэффициенты важности этих критериев.

Показатель защищенности по классу средств вычислительной техники	1 эксперт	2 эксперт	3 эксперт
1 очистка памяти	8	7	
2 регистрация	9	5	
3 идентификация и аутентификация	9	10	
4 взаимодействие пользователя с комплексом средств защиты	7	10	
5 руководство по комплексу средств защиты	10	9	
6 защита ввода вывода на отчуждаемый физический носитель информации	5	4	

2. Для оценки защищенности по классу СВТ было предложено три объекта:

1) Третий корпус Тверского госуниверситета, аудитория 16.

2) Организация, в которой Вы проходили летнюю практику.

3) Расчетная группа Тверского госуниверситета, ректорат, 14 кабинет.

Какой из трех объектов имеет более высокий уровень защиты по классу СВТ? Определить ранговым методом.

3. Была проведена оценка защищенности компьютерной сети в трех подразделениях по пяти факторам. Ниже в таблице приведены результаты оценивания. Привести значения критериев к одинаковым единицам. Используя мультипликативную свёртку, выяснить, какое подразделение защищено лучшим образом. Веса критериев:

$\lambda_1 = 0{,}6$; $\lambda_2 = 0{,}7$; $\lambda_3 = 0{,}4$; $\lambda_4 = 0{,}5$; $\lambda_5 = 0{,}8$.

факторы / подразделение	**1**	**2**	**3**	**4**	**5**
A	15 чел.	50 тыс. руб.	4 шт.	3 месяца	- 372 тыс. руб.
B	17 чел.	75 тыс. руб.	3 шт.	2 месяца	-256 тыс. руб.

С	20 чел.	70 тыс. руб.	7 шт.	1 месяц	-538 тыс. руб.

4. Оценка компьютерной защиты банковской информации происходит по двум критериям:

$$300x_1+500x_2 \rightarrow max, \qquad x_1+4x_2 \rightarrow max.$$

При этом должны выполняться ограничения, характеризующие экономические и технические возможности $1,2x_1+4x_2 \leq 240$, $0,5x_1+x_2 \leq 81$, $0 \leq x_1$, $0 \leq x_2 \leq 40$. Используя линейную аддитивную свёртку с нормирующими множителями (0,5; 0,5) найти оптимальное решение.

Теоретические вопросы для проверки уровня сформированности компетенции ПСК – 2.5.

1. Организация защиты ПЭВМ от несанкционированного доступа. Состав типового комплекса защиты от несанкционированного доступа. Динамика работы комплекса защиты от НСД
2. Защита конфиденциальной информации. Безопасность персональных данных при их обработке в информационных системах. Порядок проведения классификации информационных систем персональных данных.

Практические вопросы для проверки уровня сформированности компетенции ПСК – 2.5.

1. Используя матрицу знаний оценить качество системы защиты информации 3 корпуса ТвГУ по направлению **Защита каналов связи** и по трем этапам:

   1) Определение информационных и технических ресурсов, подлежащих защите.

   2) Выявление полного множества потенциально возможных угроз и каналов утечки информации.

   3) Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки.

2. Используя матрицу знаний оценить качество системы защиты информации 3 корпуса ТвГУ по направлению **Защита процессов и программ** и по трем

этапам:

1) Определение требований к системе защиты.

2) Осуществление выбора средств защиты информации и их характеристик.

3) Внедрение и организация использования выбранных мер, способов и средств защиты.

ЛИТЕРАТУРА, РЕКОМЕНДУЕМАЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Математический анализ. Теория и практика: учебное пособие / В.С. Шипачев. - 3-е изд. - М.: НИЦ ИНФРА-М, 2015. - 351 с.: 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-16-010073-9, http://znanium.com/go.php?id=469727
2. Гурьянова, К.Н. Математический анализ: учебное пособие / К.Н. Гурьянова, У.А. Алексеева, В.В. Бояршинов ; Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. - Екатеринбург : Издательство Уральского университета, 2014. - 332 с. - ISBN 978-5-7996-1340-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=275708
3. Будаев, В.Д. Математический анализ. Функции одной переменной. [Электронный ресурс] / В.Д. Будаев, М.Я. Якубсон. — Электрон. дан. — СПб.: Лань, 2012. — 544 с. — Режим доступа: http://e.lanbook.com/book/3173 — Загл. с экрана.
4. Асташова, И.В. Геометрия и топология: учебно-методический комплекс / И.В. Асташова, В.А. Никишкин. - 4-е изд., испр. и доп. - М.: Евразийский открытый институт, 2011. - 258 с. - ISBN 978-5-374-00489-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90953
5. Асташова И.В. Геометрия и топология [Электронный ресурс]: учебное пособие И.В. Асташова, В.А. Никишкин.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 94 с.— Режим доступа: http://www.iprbookshop.ru/10645.html.— ЭБС «IPRbooks»
6. Примаков Д.А. Геометрия и топология [Электронный ресурс]: учебное пособие/ Д.А. 3. Примаков, Р.Я. Хамидуллин.— Электрон. текстовые данные.— М.: Московский финансово-промышленный университет

«Синергия», 2011.— 272 с.— Режим доступа: http://www.iprbookshop.ru/17013.html.— ЭБС «IPRbooks»

7. Кострикин, А.И. Введение в алгебру: учебник / А.И. Кострикин. - М.: МЦНМО, 2009. - Ч. 1. Основы алгебры. - 273 с. - ISBN 978-5-94057-453-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63140
8. Кострикин, А.И. Введение в алгебру: учебник / А.И. Кострикин. - М.: МЦНМО, 2009. - Ч. 2. Линейная алгебра. - 368 с. - ISBN 978-5-94057-454-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63144
9. Кострикин, А.И. Введение в алгебру: учебник / А.И. Кострикин. - М.: МЦНМО, 2009. - Ч. 3. Основные структуры алгебры. - 272 с. - ISBN 978-5-94057-455-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=62951
10. Шевелев, Ю.П. Дискретная математика. [Электронный ресурс] — Электрон. дан. — СПб.: Лань, 2016. — 592 с. — Режим доступа: http://e.lanbook.com/book/71772 — Загл. с экрана.
11. Дискретная математика. Углубленный курс: учебник / Т.С Соболева; Под ред. А.В. Чечкина. - М.:КУРС, НИЦ ИНФРА-М, 2016. - 278 с.: 60x90 1/16. - (Бакалавриат) (Переплёт 7БЦ) ISBN 978-5-906818-11-9 http://znanium.com/go.php?id=520541
12. Храмова Т.В. Дискретная математика. Элементы теории графов [Электронный ресурс]: учебное пособие/ Т.В. Храмова.— Электрон. текстовые данные.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2014.— 43 с.— Режим доступа: http://www.iprbookshop.ru/45466.html.— ЭБС «IPRbooks»
13. Математическая логика и теория алгоритмов: учебник / А.В. Пруцков, Л.Л. Волкова. — М.: КУРС: ИНФРА-М, 2017. — 152 с. http://znanium.com/go.php?id=773373
14. Судоплатов, С.В. Математическая логика и теория алгоритмов :

учебник / С.В. Судоплатов, Е.В. Овчинникова. - 3-е изд. - Новосибирск : НГТУ, 2012. - 254 с. - (Учебники НГТУ). - ISBN 978-5-7782-1838-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=135676

15. Балдин, К.В. Теория вероятностей и математическая статистика: учебник / К.В. Балдин, В.Н. Башлыков, А.В. Рукосуев. - 2-е изд. - М. : Издательско-торговая корпорация «Дашков и К°», 2016. - 472 с. : ил. - Библиогр.: с. 433-434. - ISBN 978-5-394-02108-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=453249
16. Колемаев, В.А. Теория вероятностей и математическая статистика: учебник / В.А. Колемаев, В.Н. Калинина. - М. : Юнити-Дана, 2015. - 352 с. : табл. - ISBN 5-238-00560-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=436721
17. Шилова З.В. Теория вероятностей и математическая статистика [Электронный ресурс]: учебное пособие/ З.В. Шилова, О.И Шилов.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 158 с.— Режим доступа: http://www.iprbookshop.ru/33863.html.— ЭБС «IPRbooks»
18. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ С.А. Нестеров.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 с.— Режим доступа: http://www.iprbookshop.ru/43960.html.— ЭБС «IPRbooks»
19. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие /Ю.Н. Сычев.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2010.— 328 с.— Режим доступа: http://www.iprbookshop.ru/10746.html.— ЭБС «IPRbooks»
20. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров.— Электрон. текстовые

данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html.— ЭБС «IPRbooks»

21. Сальникова Н.А. Информатика. Основы информатики. Представление и кодирование информации. Часть 1 [Электронный ресурс]: учебное пособие/ Н.А. Сальникова.— Электрон. текстовые данные.— Волгоград: Волгоградский институт бизнеса, Вузовское образование, 2009.— 94 с.— Режим доступа: http://www.iprbookshop.ru/11321.html.— ЭБС «IPRbooks»
22. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»
23. Чепурнова Н.М. Правовые основы информатики [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по направлению «Прикладная информатика»/ Н.М. Чепурнова, Л.Л Ефимова.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 295 с.— Режим доступа: http://www.iprbookshop.ru/34498.html.— ЭБС «IPRbooks»
24. Методы и алгоритмы обработки данных : учебное пособие / А.А. Григорьев. — М.: ИНФРА-М, 2017. — 256 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/22119. http://znanium.com/go.php?id=545998
25. Шишов О.В. Современные технологии и технические средства информатизации: учебник. — М.: ИНФРА-М, 2017. — 462 с. — (Высшее образование: Бакалавриат). http://znanium.com/go.php?id=653093
26. Компьютерные науки. Деревья, операционные системы, сети / И.Ф. Астахова, И.К. Астанин, И.Б. Крыжко. - М.: ФИЗМАТЛИТ, 2013. - 88

с.: 60x90 1/16. (обложка) ISBN 978-5-9221-1449-3 http://znanium.com/go.php?id=428176

27. Самуйлов С.В. Базы данных [Электронный ресурс]: учебно-методическое пособие для выполнения лабораторной и контрольной работы/ С.В. Самуйлов.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2016.— 50 с.— Режим доступа: http://www.iprbookshop.ru/47276.html. — ЭБС «IPRbooks»
28. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В. Прохорова.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.html .— ЭБС «IPRbooks»
29. Торстейнсон, П. Криптография и безопасность в технологии. NET. [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш. — Электрон. дан. — М.: Издательство "Лаборатория знаний", 2015. — 428 с. — Режим доступа: http://e.lanbook.com/book/70724 — Загл. с экрана.
30. Сысоев Д.В. Введение в теорию искусственного интеллекта [Электронный ресурс]: учебное пособие/ Д.В. Сысоев, О.В. Курипта, Д.К. Проскурин.— Электрон. текстовые данные.— Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 171 с.— Режим доступа: http://www.iprbookshop.ru/30835.html .— ЭБС «IPRbooks»
31. Информационные системы и технологии управления: учебник / под ред. Г.А. Титоренко. - 3-е изд., перераб. и доп. - М. : Юнити-Дана, 2015. - 591 с. : ил., табл., схемы - (Золотой фонд российских учебников). - ISBN 978-5-238-01766-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115159
32. Разработка моделей криптографической защиты информации : монография / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко,

Ю.И. Титаренко; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова», Министерство образования и науки РФ. - Ульяновск : УлГПУ, 2013. - 128 с. : схем. - Библиогр.: с. 108-112. - ISBN 978-5-86045-640-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=278070

33. Сотов А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации [Электронный ресурс]: монография/ А.И. Сотов.— Электрон. текстовые данные.— М.: Русайнс, 2015.— 128 с.— Режим доступа: http://www.iprbookshop.ru/48904.html .— ЭБС «IPRbooks»
34. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092
35. Борисова И.В. Цифровые методы обработки информации [Электронный ресурс]: учебное пособие/ И.В. Борисова.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2014.— 139 с.— Режим доступа: http://www.iprbookshop.ru/45061.html.— ЭБС «IPRbooks»
36. Гуц, А.К. Теория игр и защита компьютерных систем: методические указания / А.К. Гуц, Т.В. Вахний; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования. «Омский Государственный университет им. Ф.М. Достоевского». - Омск : Омский государственный университет, 2013. -

160 с. : ил.,табл., схем. - ISBN 978-5-7779-1655-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=237190

37. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ В.В. Креопалов.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 с.— Режим доступа: http://www.iprbookshop.ru/10871.html .— ЭБС «IPRbooks»