Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Иркутский национальный исследовательский технический университет»

Институт информационных технологий и анализа данных

Центр компетенций по кибербезопасности

УТВЕРЖДАЮ:
Директор института ИТ и АД
_____ / А.С. Говорков
28 марта 2022 г.

Фонд оценочных средств

Технологии защиты информации в автоматизированных информационных системах

10.04.01 Информационная безопасность

Безопасность киберфизических систем

Форма обучения: Очная

Составитель программы:

Маринов А.А. _____ / “ 28 ” марта 20 22 г.

Год набора – 2022

Иркутск 2022

1. Показатели и критерии оценивания компетенций на этапах их формирования

Индикатор достижения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания промежуточной аттестации
УК-2.2. Планирует необходимые ресурсы, в том числе с учетом их заменимости; разрабатывает план реализации проекта с использованием инструментов планирования; осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта	Формирует этапы решения защиты информации в АСУ с использованием инструментов планирования.	1. Разрабатывает этапы решения защиты информации. 2.Производит разбор задачи с указанием этапов и конечных целей защиты информации в автоматизированных информационных системах.	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий
УК-6.2. Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям	Формирует способы совершенствования собственной деятельности по выбранным критериям и обоснованно определяет их приоритетность.	Эффективно планирует и организует свою деятельность. Ставит личные цели и обоснованно определяет их приоритетность. Является инициатором запросов недостающих знаний и понимает их значимость. Участвует в рефлексии на позиции соорганизатора.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.
ОПК-1.2. Владеет техниками освоения новых методов, позволяющих решать профессиональные задачи,	Формирует решения профессиональных задач с их оценкой и критическим анализом информации.	1. Разрабатывает этапы решения поставленной задачи, выделяя ее основные составляющие. 2. Производит разбор задачи с указанием этапов и конечных целей	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.

самостоятельно использовать потенциал интегрированных знаний для освоения новых областей и совершенствования уровня своей квалификационной подготовки		используя новые методы(обработки и защиты информации), позволяющие решать профессиональные задачи. 3. Анализирует пути решения задачи с их оценкой и критическим анализом недостатков и достоинств.	Вид промежуточной аттестации – экзамен.
ОПК-2.1. Организует и осуществляет контроль за проектированием сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты	Осуществляет контроль за системой менеджмента информационной безопасности	Способен продемонстрировать специализированные знания в области проектирования сложных систем: государственных система защиты информации (ГИС); объектов КИИ; область применения проектируемой системы ИБ.	Опрос, собеседование, практикоориентированные задания, тесты письменные и/или компьютерные, дискуссия. Вид промежуточной аттестации – зачет.
ОПК-4.1. Разрабатывает программы и методики испытаний средстви систем обеспечения информационной безопасности	Эффективно использует методы разработки защиты информации, а также этапы внедрения системы защиты информации	Способен продемонстрировать специализированные знания в области разработки систем обеспечения информационной безопасности: программ и методик испытаний информационных систем	Устное собеседование по теоретическим вопросам и индивидуальные практические задания, дискуссия. Вид промежуточной аттестации – зачет.

1. Оценочные средства для проведения текущего контроля

1.1. Оценочные средства для проведения текущего контроля в 2_ семестре

Перечень тестовых заданий

УК-2.2

1. Какие этапы включает в себя разработка решения по защите информации в автоматизированных информационных системах?

А) Анализ уязвимостей, разработка стратегии защиты, реализация мер безопасности

Б) Проведение аудита, установка антивирусного программного обеспечения, обучение персонала

В) Планирование бэкапов, проведение тестирования на проникновение, разработка политики безопасности

2. Какая из нижеперечисленных целей не является конечной целью разработки этапов защиты информации в автоматизированных информационных системах?

А) Обеспечение конфиденциальности, целостности и доступности информации

Б) Предотвращение любых атак на информационную систему

В) Минимизация рисков утечки и повреждения информации

3. Какой этап разработки решения по защите информации включает в себя оценку текущего состояния системы и выявление уязвимостей?

А) Планирование мер безопасности

Б) Анализ уязвимостей

В) Разработка стратегии защиты

4. Какая из нижеперечисленных мер не относится к этапам решения по защите информации в автоматизированных информационных системах?

А) Установка антивирусного программного обеспечения

Б) Разработка политики безопасности

В) Развертывание новой версии операционной системы

Правильный ответ: В) Развертывание новой версии операционной системы

5. Какой из нижеперечисленных методов не является частью разработки этапов защиты информации в автоматизированных информационных системах?

А) Метод анализа иерархий (МАИ)

Б) SWOT-анализ

В) Метод дерева решений для выбора наиболее эффективных мер по обеспечению безопасности

УК-6.2

6. Какие этапы включает в себя эффективное планирование и организация деятельности в области информационной безопасности?

А) Анализ уязвимостей, разработка стратегии защиты, реализация мер безопасности

Б) Проведение аудита, установка антивирусного программного обеспечения, обучение персонала

В) Планирование бэкапов, проведение тестирования на проникновение, разработка политики безопасности

7. Что включает в себя постановка личных целей и определение их приоритетности в области информационной безопасности?

А) Участие в рефлексии на позиции соорганизатора

Б) Формирование запросов недостающих знаний и понимание их значимость

В) Определение конкретных задач и их приоритетов для достижения целей

8. Какие методы могут быть использованы для формирования запросов недостающих знаний и понимания их значимости в области информационной безопасности?

А) Метод анализа иерархий (МАИ)

Б) SWOT-анализ

В) Метод дерева решений для выбора наиболее эффективных мер по обеспечению

безопасности

9. Что включает в себя эффективное участие в рефлексии на позиции соорганизатора в области информационной безопасности?

А) Анализ уязвимостей, разработка стратегии защиты, реализация мер безопасности

Б) Проведение аудита, установка антивирусного программного обеспечения, обучение персонала

В) Рассмотрение собственной роли и ответственности в организации обеспечения информационной безопасности

10. Какие этапы помогают определить приоритетность целей в области информационной безопасности?

А) Планирование бэкапов, проведение тестирования на проникновение, разработка политики безопасности

Б) Определение конкретных задач и их приоритетов для достижения целей

В) Установка антивирусного программного обеспечения

ОПК-1.2

1. Что включает в себя процесс разработки стратегии информационной безопасности?

А) Анализ уязвимостей, разработка стратегии защиты, реализация мер безопасности

Б) Установка антивирусного программного обеспечения

В) Периодическое изменение паролей

2. Какие методы можно использовать для определения приоритетов в области информационной безопасности?

А) Организация собраний безопасности

Б) Определение конкретных задач и их приоритетов для достижения целей

Г) Установка брандмауэра на всех компьютерах в сети

3. Какой метод анализа можно применить для оценки важности различных аспектов информационной безопасности?

А) Метод анализа иерархий (МАИ)

Б) Применение случайных методов

В) Опрос сотрудников об их представлениях о безопасности

4. Что включает в себя самооценка в области информационной безопасности?

А) Изучение новых технологий

Б) Регулярное обновление паролей

В) Рассмотрение собственной роли и ответственности в организации обеспечения информационной безопасности

5. Что является ключевым шагом для достижения целей в области информационной безопасности?

А) Покупка нового оборудования

Б) Определение конкретных задач и их приоритетов для достижения целей

В) Установка дополнительных защитных программных средств

ОПК-2.1

1. Какие основные достоинства информационной безопасности в современном мире?
а) Защита персональных данных пользователей от несанкционированного доступа;
б) Повышение уровня конкурентоспособности предприятий и организаций;
в) Снижение риска финансовых потерь вследствие кибератак;

2. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:
а) Информация
б) Информационные технологии
в) Информационная система
г) Информационно-телекоммуникационная сеть
д) Обладатель информации

3. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:
а) Источник информации
б) Потребитель информации
в) Уничтожитель информации
г) Носитель информации
д) Обладатель информации

4. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:
а) База данных
б) Информационная технология
в) Информационная система
г) Информационно-телекоммуникационная сеть
д) Медицинская информационная система

5. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это:
а) Электронное сообщение
б) Распространение информации
в) Предоставление информации
г) Конфиденциальность информации

6. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:
а) Уничтожение информации
б) Распространение информации
в) Предоставление информации
г) Конфиденциальность информации
д) Доступ к информации

7. Возможность получения информации и ее использования это:
а) Сохранение информации
б) Распространение информации
в) Предоставление информации
г) Конфиденциальность информации
д) Доступ к информации

8. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:

а) Электронное сообщение
б) Информационное сообщение
в) Текстовое сообщение
г) Визуальное сообщение
д) SMS-сообщение

ОПК-4.1

9. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

а) Информационная система персональных данных
б) База данных
в) Централизованное хранилище данных
г) Система Статэкспресс
д) Д) Сервер

10. К сведениям конфиденциального характера, согласно указу президента рф от 6 марта 1997 г., относятся:

а) Информация о распространении программ
б) Информация о лицензировании программного обеспечения
в) Информация, размещаемая в газетах, Интернете
г) Персональные данные
д) Личная тайна

11. Отношения, связанные с обработкой персональных данных, регулируются законом…

а) «Об информации, информационных технологиях»
б) «О защите информации»
в) Федеральным законом «О персональных данных»
г) Федеральным законом «О конфиденциальной информации»
д) «Об утверждении перечня сведений конфиденциального характера»

12. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. Д это:

а) «Исправление персональных данных»
б) «Работа с персональными данными»
в). «Преобразование персональных данных»
г). «Обработка персональных данных»
д). «Изменение персональных данных»

13. Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных:

а). Выделение персональных данных
б). Обеспечение безопасности персональных данных
в). Деаутентификация
г). Деавторизация
д). Деперсонификация

14. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на:

а) Многопользовательские

б) Однопользовательские
в) Без разграничения прав доступа
г) С разграничением прав доступа
д) Системы, не имеющие подключений

15. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:
а) Авторизация
б) Аутентификация
в) Обезличивание
г) Деперсонализация
д) Идентификация

Перечень кейсовых заданий (задания с развернутым ответом)

№ задания	Содержание задания	Коды компетенций
1	Методы деструктивного воздействия на информационные ресурсы	УК-6
2	Принципы защиты информационных ресурсов от деструктивного воздействия	УК-6
3	Разработка планов реализации проекта с использованием инструментов планирования	УК-2
4	Влияние деструктивного воздействия на информационные ресурсы на эффективность структур управления	ОПК-1
5	Методы обнаружения деструктивного воздействия на информационные ресурсы	ОПК-1
6	Риски для структур управления предприятием в результате деструктивного воздействия	ОПК-1
7	Методы восстановления после деструктивного воздействия: обсуждение процедур и технологий для быстрого восстановления работоспособности информационных ресурсов и структур управления предприятием после инцидентов безопасности	ОПК-1
8	Анализ (обработка) организационно-распорядительных документов, в зависимости от уровня защищенности, а также функциональных особенностей информационной системы	ОПК-4
9	Моделирование динамических систем с использованием дифференциальных уравнений	ОПК-2
10	Методы статистического анализа данных с использованием современных интеллектуальных технологий	ОПК-2
11	Решение профессиональных задач с использованием современных интеллектуальных технологий	ОПК-2
12	Методы машинного обучения и их применение в научных и инженерных задачах	ОПК-2
13	Численное моделирование физических процессов с использованием методов конечных элементов	ОПК-4
14	Решение нестандартных профессиональных задачи с применением технологий разработки программного обеспечения.	ОПК-2

15	Текущие тенденции защиты информации в области АСУ	ОПК-2
16	Методы анализа уязвимостей информационных систем (подготовка результатов по технической защите информации)	УК-2
17	Технологии обнаружения и предотвращения атак	УК-2
18	Анализ современных стандартов информационной безопасности	ОПК-2
19	Роль человеческого фактора в информационной безопасности	УК-6
20	Этические аспекты в области информационной безопасности	УК-6
21	Разработка этапов построения системы (или подсистемы) информационной безопасности для защиты информации в АСУ	УК-2

2. Оценочные средства для проведения промежуточной аттестации

2.1. Оценочные средства для проведения экзамена по дисциплине

Перечень тестовых заданий

ОПК -1.2

Множественный выбор

1. Что такое "вирус" в контексте информационной безопасности?

а) Вредоносная программа, способная размножаться и повреждать информационные ресурсы +

б) Метод атаки на системы по несанкционированному доступу

в) Вид угрозы, связанный с физическими повреждениями информационного оборудования

г) Предупреждение или защита от угроз информационной безопасности

2. Какие объекты информатизации относятся к структурам управления?

а) Локальные компьютерные системы

б) Сетевое оборудование +

в) Информационные базы данных +

г) Все вышеперечисленное

3. Какое воздействие на объекты информатизации может привести к нарушению безопасности информации?

а) Вирусное заражение +

б) Несанкционированный доступ к рабочей станции (ПК)

в) Физическое повреждение оборудования +

г) Все вышеперечисленное

4. Какие угрозы нарушения безопасности информации могут быть реализованы путем деструктивного воздействия на информационные ресурсы?

а) Уничтожение данных

б) Изменение данных

в) Нарушение конфиденциальности информации

г) Все вышеперечисленное +

5. Какие специализированные знания необходимы для обеспечения безопасности информации?

а) Знание алгоритмов шифрования

б) Знание методов аутентификации пользователей
в) Знание законодательных актов в области информационной безопасности
г) Все вышеперечисленное +

6. Какие структуры управления очень чувствительны к нарушению безопасности информации?
а) Объекты и субъекты государственного управления и их система +
б) ФСТЭК
в) Пищевая промышленность
г) Все вышеперечисленное

7. Какая угроза нарушения безопасности информации является наиболее опасной?
а) Распространение вредоносного (шпионского) ПО
б) утечка конфиденциальной (чувствительной) информации +
в) Сетевые атаки
г) Все вышеперечисленное

Короткий ответ

8. Что такое деструктивное воздействие на информационную систему?...**(Это действия, направленные на нанесение ущерба информационным ресурсам предприятия)**

9. Какие угрозы представляет деструктивное воздействие для информационной системы?..**(Потеря данных, нарушение работы системы, утечка конфиденциальной информации)**

10. Какие последствия может иметь деструктивное воздействие на управление предприятием?...**(Финансовые потери, нарушение бизнес-процессов, потеря доверия клиентов и партнёров)**

11. Какие методы защиты от деструктивного воздействия могут быть использованы на предприятии?...**(Антивирусные программы, брандмауэры, системы резервного копирования данных)**

12. Какие технологии помогают обнаружить деструктивное воздействие на информационную систему?...**(Системы мониторинга сетевого трафика, антивирусные программы с функцией обнаружения вторжений)**

13. Какие законодательные акты регулируют вопросы безопасности информации на предприятии?...**(Законы о защите персональных данных, законы о кибербезопасности)**

14. Какие методы социальной инженерии могут быть использованы для деструктивного воздействия на информационную систему?...**(Фишинговые атаки, атаки через социальные сети, мошеннические звонки).**

ОПК -2.1

Множественный выбор

1. Какая программа используется для численного решения математических задач?
а) Microsoft Excel
б) MATLAB
в) Python +
г) SPSS

2. Какой метод используется для решения систем нелинейных уравнений?

а) Метод Ньютона +
б) Метод Монте-Карло
в) Метод Гаусса
г) Метод Симпсона

3. Какой метод используется для аппроксимации функций?
а) Метод Ньютона
б) Метод Монте-Карло
в) Метод Гаусса
г) Метод наименьших квадратов +

4. Какой метод используется для решения задачи о распределении вероятностей?
а) Метод Эйлера
б) Метод Монте-Карло +
в) Метод Гаусса
г) Метод Симпсона
5. Какая программа используется для визуализации математических моделей?
а) Microsoft Excel
б) MATLAB +
в) Python
г) SPSS

6. Какой метод используется для решения задачи нахождения корней уравнения?
а) Метод Ньютона +
б) Метод Монте-Карло
в) Метод Гаусса
г) Метод Симпсона

7. Какой метод используется для решения задачи определения экстремума функции?
а) Метод Ньютона +
б) Метод Монте-Карло
в) Метод Гаусса
г) Метод Симпсона

Короткий ответ

8. Зачем применяют математические методы в информационной безопасности?...**(Для анализа сложных систем, разработки криптографических алгоритмов, исследования уязвимостей)**

9. Какие математические методы используются для защиты информации?...**(Теория чисел, дискретная математика, теория вероятностей, линейная алгебра).**

10. Какие эксперименты могут быть проведены в области информационной безопасности?...**(Тестирование криптографических алгоритмов, анализ уязвимостей сетевых протоколов, оценка надежности систем защиты)**

11. Какие математические методы используются для анализа уязвимостей в информационной системе?...**(Методы формальной верификации, анализ графов, моделирование угроз)**

12. Какие роли играют математические модели в обеспечении информационной безопасности?...**(Предсказание рисков, определение оптимальных стратегий защиты, оценка эффективности мер по обеспечению безопасности)**

13. Какие методы математического анализа применяются для обнаружения аномалий в

сетевом трафике?...**(Методы статистики, машинного обучения, временных рядов)**

14. Какие математические методы помогают в разработке криптографических алгоритмов?...**(Теория чисел, комбинаторика, алгебраическая геометрия, теория сложности вычислений)**.

ОПК -4.1

Множественный выбор

1. Какой тип угрозы информационной безопасности связан с недостатками программных систем?
а) Физические угрозы
б) Человеческие угрозы
в) Технические угрозы +
г) Природные угрозы

2. Какая из следующих мер защиты помогает предотвратить несанкционированный доступ к информации?
а) Бронирование
б) Антивирусная защита
в) Бэкап
г) Фаервол +

3. Какая из следующих атак носит характер внутренней угрозы?
а) DDO атака
б) Фишинг
в) Инсайдерская атака +
г) SQL-инъекция

4. Какая из следующих методик используется для обеспечения конфиденциальности данных?
а) Шифрование +
б) Бэкапирование
в) Хеширование
г) Фильтрация трафика

5. Какие недостатки могут быть связаны с применением информационной безопасности?
а) Потенциальные затраты на внедрение и поддержание систем информационной безопасности;
б) Ограничение доступа к информации для сотрудников;
в) Возможность возникновения ложных срабатываний систем защиты;
г) Все вышеперечисленные недостатки связаны с применением информационной безопасности. +

6. С какими методологическими принципами научного исследования связан анализ информации о современных технологиях информационной безопасности?
а) Системность – рассмотрение безопасности информации как комплексного процесса;
б) Объективность – нейтральное и беспристрастное исследование;
в) Репрезентативность – использование достоверных и репрезентативных данных при анализе;
г) Все вышеперечисленные принципы связаны с анализом информации о современных технологиях информационной безопасности.+

Короткий ответ

7. Какие основные источники информации по исследованиям в области информационной безопасности?...**(Научные журналы, конференции, отчеты организаций, блоги экспертов, академические ресурсы)**

8. Какие ключевые слова следует использовать при поиске информации по исследованиям в области информационной безопасности?...**(Кибербезопасность, криптография, уязвимости, защита данных, кибератаки, информационная безопасность)**

9. Как можно оценить достоверность и актуальность найденной информации по исследованиям в области информационной безопасности?...**(Проверка авторства и репутации авторов, анализ даты публикации, сравнение с другими источниками, оценка качества изложения)**

10. Какие онлайн-ресурсы предоставляют доступ к актуальной информации по исследованиям в области информационной безопасности?...**(IEEE Xplore, ACM Digital Library, Google Scholar, ResearchGate, arXiv)**

11. Какие методы анализа информации могут быть применены для извлечения значимых результатов и выводов из исследований по информационной безопасности?...**(Методы статистического анализа, контент-анализ, машинное обучение, анализ сетевых графов)**.

12. Какие организации и институты специализируются на исследованиях в области информационной безопасности?...**(CERT, SANS Institute, ENISA, Kaspersky Lab, Palo Alto Networks)**

13. Как можно быть в курсе последних новостей и обновлений в области информационной безопасности?...**(Подписаться на рассылки специализированных новостных порталов, следить за официальными блогами и социальными медиа крупных компаний в области кибербезопасности)**

Перечень кейсовых заданий (задания с развернутым ответом, например, вопросы к экзамену, зачету, защите курсовых проектов и т.п.)

№ задания	Содержание задания	Коды компетенций
1	Меры по обеспечению информационной безопасности объектов информатизации на предприятии	ОПК-1
2	Организация процесса реагирования на информационные инциденты, включая выявление, анализ и восстановление после нарушений безопасности в объектах информатизации	ОПК-1
3	Методы воздействия на структуры управления предприятия, путем деструктивного воздействия на информационные ресурсы и их последствия	ОПК-1
4	Меры безопасности для защиты структур предприятия от деструктивного воздействия на информационные ресурсы	ОПК-1

5	Риски деструктивного воздействия на процессы управление предприятием, путем совершения кибератак на информационные ресурсы.	ОПК-1
6	Влияние деструктивного воздействия на информационные ресурсы на принятие управленческих решений	ОПК-1
7	Наиболее опасные методы воздействия на информационные ресурсы и методы их предотвращения	ОПК-1
8	Последствия деструктивного воздействия на информационные ресурсы предприятия и стратегии минимизации рисков	ОПК-1
9	Применение современных математических методов от криптографических атак	ОПК-2
10	Применение математических методов для обнаружения аномального поведения в сетях и системах	ОПК-2
11	Применение математических моделей для оценки риска информационной безопасности	ОПК-2
12	Применение современных методов алгебры, графов и теории вероятностей для анализа сложных систем информационной безопасности	ОПК-2
13	Применение методов статистического анализа при проведении экспериментов с использованием прикладных программ	ОПК-2
14	Автоматизация эксперимента с использованием прикладных программ	ОПК-4
15	Использования прикладных программ для моделирования и визуализации эксперимента	ОПК-2
16	Применение методов оптимизации и параллельных вычислений при проведении экспериментов с использованием прикладных программ для ускорения процесса и улучшения точности результатов	ОПК-2
17	Методы и инструменты поиска уязвимостей в сетевых приложениях и операционных системах	ОПК-2
18	Применение литературы для отслеживания последних угроз информационной безопасности и обновлений безопасности	ОПК-4
19	Проведение анализа утечек данных и инцидентов в области информационной безопасности с использованием открытых источников информации	ОПК-4
20	Оценка надежности и безопасности сторонних программных продуктов перед их использованием в корпоративной среде	ОПК-4

21	Применение методов и инструментов для анализа логов и мониторинга сетевой активности с целью выявления потенциальных угроз безопасности	ОПК-4
22	Применение баз данных и ресурсов для исследования методов кибератак и техник обхода систем безопасности	ОПК-4
23	Применение методов анализа в выявлении скрытых угроз в сетевом трафике и защитите информации от утечек	ОПК-4
24	Применение современных методов и инструментов в области защиты данных и криптографии	ОПК-4