МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса»

(ФГБОУ ВО «ПВГУС»)

|  |  |  |  |
| --- | --- | --- | --- |
| УТВЕРЖДЕНО |  | | |
| на заседании Высшей школы интеллектуальных систем и кибертехнологий | | | |
|  | | | |
| Протокол от | 02.12.2022г. | № | 4 |

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств) для проведения промежуточной аттестации

по дисциплине

|  |
| --- |
| **«Технологии обеспечения информационной безопасности»** |

наименование дисциплины

|  |  |
| --- | --- |
| по образовательной программе высшего образования – программе | магистратуры |
|  |  |

|  |
| --- |
| **«Информационная безопасность интеллектуальных и информационно-аналитических систем»** |

наименование образовательной программы

|  |
| --- |
| **10.04.01 «Информационная безопасность»** |
| шифр, наименование направления подготовки / специальности |

|  |  |
| --- | --- |
| Составитель | Мунирова Юлия Сергеевна, старший преподаватель, Высшая школла интеллектуальных систем и кибертехнологий |
|  | ФИО, должность, структурное подразделение,  ученая степень, ученое звание |

Тольятти

2022

**1. Паспорт фонда оценочных средств (далее – ФОС)**

**1.1. Планируемые результаты обучения по дисциплине**

|  |  |  |
| --- | --- | --- |
| Код компетенции | Наименование компетенции | Код и наименование индикаторов достижения компетенции |
| ОПК-1 | Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание | ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации  ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации |
| ОПК-2 | Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности | ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы  ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем |

В результате изучения дисциплины обучающийся должен:

**владеть:** инструментарием формирования требований к системе обеспечения информационной безопасности, навыками проектирования подсистемы обеспечения информационной безопасности

**уметь:** разрабатывать проект технического задания на создание системы обеспечения информационной безопасности, разрабатывать технический проект системы (подсистемы, либо компонента системы) обеспечения информационной безопасности

**знать:** требования к системе обеспечения информационной безопасности; методы концептуального проектирования технологий систем обеспечения информационной безопасности

**1.2. Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| № | Тема (раздел дисциплины)  (в соответствии с РПД) | Код компетенции и индикаторы достижения компетенций |
|  | Тема 1. Понятие системы, технологии функционирования. Сложные системы. Технология обеспечения информационной безопасности. | ОПК-1  ИОПК-1.1  ИОПК-1.2  ОПК-2  ИОПК-2.2  ИОПК-2.3 |
|  | Тема 2. Проектирование и совершенствование технологии обеспечения информационной безопасности. Этапы. Цели и задачи. Требования. Методы и способы. проектирования |
|  | Тема 3. Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем |
|  | Тема 4. Технология создания защищенных систем. Анализ требований, угроз, уязвимостей объекта защиты. |
|  | Тема 5. Особенности построения защищенных информационных систем |
|  | Тема 6. Вычисление структурно-топологических характеристик систем управления |

**1.3. Система оценивания по дисциплине**

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – экзамен.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Шкалы оценки уровня  сформированности результатов обучения | | Шкала оценки уровня освоения дисциплины | | |
| Уровневая шкала оценки компетенций | 100 бальная шкала, % | 100 бальная шкала, % | 5-балльная шкала,дифференцированная оценка/балл | недифференцированная оценка |
| допороговый | ниже 61 | ниже 61 | «неудовлетворительно» / 2 | не зачтено |
| пороговый | 61-85,9 | 61-69,9 | «удовлетворительно» / 3 | зачтено |
| 70-85,9 | «хорошо» / 4 | зачтено |
| повышенный | 86-100 | 86-100 | «отлично» / 5 | зачтено |

**2. Перечень оценочных материалов для проведения промежуточной аттестации**

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

**Перечень вопросов для подготовки к экзамену**

**ОПК-1: ИОПК-1.1, ИОПК-1.2. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.**

1. Что такое информация, субъекты информационных отношений?

2. Дайте определение Информационной технологии.

3. Компьютерная система-это…

4. Элементы и подсистемы, управление и информация, самоорганизация.

5. Раскройте терм информационная безопасность

6. Определение автоматизированной системы

7. Свойства информации

8. Что такое уязвимость?

9. Основные принципы системного подхода при создании сложных систем.

10. Технология функционирования сложной системы.

11. Перечислите основные объекты информационной безопасности. Дайте их определения.

12. Понятия ущерба, риска и угрозы.

13. Основные угрозы безопасности информации АС и их классификация.

14. Каково назначение Политики информационной безопасности?

15. Для чего нужна стандартизация в сфере информационной безопасности?

16. Какую информацию относят к секретной, конфиденциальной?

17. Цели и задачи проектирования ИБ

18. Что такое система физической защиты объекта?

19. Перечислите основные риски ИБ. Дайте их определения.

**ОПК-2:ИОПК-2.2, ИОПК-2.3. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.**

20. Какие требования предъявляются к комплексной системе безопасности объекта?

21. В чем суть гарантированного уничтожения данных?

22. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

23. Охарактеризуйте понятие большие данные.

24. Какую информацию относят к секретной, конфиденциальной?

25. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?

26. Какие применяются методы защиты информации от промышленного шпионажа?

27. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?

28. Какие организационные меры обеспечения безопасности Вы знаете?

29. Какие технические меры обеспечения безопасности Вы знаете?

30. Основные принципы обеспечения ИБ

31. Основные функции системы безопасности.

32. Основные принципы политики ИБ.

33. Какое свойство информации является наиболее актуальным при обеспечении ИБ? Дайте его определение.

34. Свойство информации при котором невозможно ее искажение…

35. Охарактеризуйте ИБ поиска информации.

36. Охарактеризуйте ИБ обработки данных.

37. Охарактеризуйте эмерджентные технологии.

38. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

39. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

40. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

41. Укажите модель управления доступом, к которой относится основная теорема безопасности.

42. Какие виды информации существуют в зависимости от категории доступа к ней?

43. Защищаемая информация – это..

44. Правовые методы обеспечения ИБ

45. Способы представления информации о правах доступа.

46. Характеристика качества

47. Показатели и критерии эффективности

48. Методические вопросы оценки эффективности сложных систем.

49. Дайте определение понятию «ядро безопасности»

50. Кратко опишите архитектуру защищенной системы.

**Вопросы (задания) для подготовки к экзамену с «ключами» правильных ответов**

| № | Содержание вопроса | Правильный ответ |
| --- | --- | --- |
| **ОПК-1- Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание** | | |
|  | Что такое информация, субъекты информационных отношений? | . Информация - это сведения, данные или факты, которые передаются или получаются для обмена знаниями или для принятия решений. Субъекты информационных отношений - это лица или организации, которые участвуют в процессе обмена информацией. |
|  | Дайте определение Информационной технологии. | Информационная технология - это совокупность методов, процедур и инструментов, используемых для сбора, хранения, обработки, передачи и анализа информации. |
|  | Компьютерная система-это… | Компьютерная система - это совокупность аппаратных и программных средств, которые работают вместе для выполнения определенных задач. |
|  | Элементы и подсистемы, управление и информация, самоорганизация. | Элементы и подсистемы, управление и информация, самоорганизация являются основными компонентами сложных систем. |
|  | Раскройте терм информационная безопасность | Информационная безопасность - это состояние защищенности информации от несанкционированного доступа, разрушения, изменения или утечки. |
|  | Определение автоматизированной системы | Автоматизированная система - это система, в которой процессы управления и контроля осуществляются автоматически с помощью компьютеров и специализированного программного обеспечения. |
|  | Свойства информации | Свойства информации включают целостность (достоверность и полноту), конфиденциальность (ограниченный доступ), доступность (возможность получения информации в нужное время) и аутентичность (подлинность). |
|  | Что такое уязвимость? | Уязвимость - это слабое место в системе безопасности, через которое возможно нарушение конфиденциальности, целостности или доступности информации. |
|  | Основные принципы системного подхода при создании сложных систем. | Основные принципы системного подхода при создании сложных систем включают целостность, иерархичность, взаимосвязь элементов, обратную связь и самоорганизацию. |
|  | Технология функционирования сложной системы. | Технология функционирования сложной системы включает в себя определение целей, проектирование структуры системы, определение ролей и функций элементов системы, управление ресурсами и обеспечение взаимодействия между элементами. |
|  | Перечислите основные объекты информационной безопасности. Дайте их определения. | Данные: Основные элементы информации, подлежащие защите от несанкционированного доступа, изменений или утраты.  Информационные системы: Совокупность аппаратных и программных средств, а также процессов и людей, используемых для обработки, хранения и передачи информации.  Сети: Инфраструктура, обеспечивающая связь между информационными системами и устройствами, требующая защиты от несанкционированного доступа и других угроз.  Пользователи: Люди, которые имеют доступ к информационным ресурсам и могут представлять угрозу или служить защитой в контексте информационной безопасности. |
|  | Понятия ущерба, риска и угрозы. | Ущерб: Потенциальные или фактические негативные последствия нарушения безопасности.  Риск: Вероятность возникновения ущерба из-за уязвимостей и угроз.  Угроза: Потенциальное событие или действие, которое может нанести ущерб информационным ресурсам. |
|  | Основные угрозы безопасности информации АС и их классификация. | Вирусы: Вредоносное программное обеспечение, такое как вирусы, черви, троянские кони и шпионские программы.  Атаки в сети: Включают в себя атаки отказа в обслуживании (DDoS), перехват трафика (подслушивание), внедрение (взлом) и подделку данных.  Социальная инженерия: Обман людей для получения конфиденциальной информации или выполнения вредоносных действий.  Физические угрозы: Пожары, наводнения, кражи оборудования и другие физические события, которые могут привести к потере или повреждению данных и оборудования.  Классификация угроз информационной безопасности:  По источнику угроз (внутренние, внешние)  По типу угрозы (технические, не технические)  По методу атаки (активные, пассивные)  По цели атаки (конфиденциальность, целостность, доступность)  По уровню риска (низкий, средний, высокий) |
|  | Каково назначение Политики информационной безопасности? | Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов. |
|  | Для чего нужна стандартизация в сфере информационной безопасности? | Стандартизация информационной безопасности (ИБ) выгодна как для профессионалов, так и для потребителей продуктов и услуг в области информационной безопасности, поскольку позволяет определять оптимальный уровень заказа и стандартизации, обеспечивать взаимозаменяемость продуктов для обеспечения информационной безопасности, а также обеспечивать измеримость и повторяемость в разных странах и организациях достигнуты результаты. |
|  | Какую информацию относят к секретной, конфиденциальной? | Конфиденциальная информация — это сведения, доступ к которым ограничен законом РФ и которые не являются государственной тайной. Конфиденциальными могут считаться персональные данные отдельного гражданина, служебные и коммерческие тайны предприятия, а также секретные сведения в правоохранительной сфере |
|  | Цели и задачи проектирования | системы, способной выполнять требуемые функции и операции.  Обеспечение эффективности: Минимизация затрат ресурсов (времени, денег, энергии) при выполнении задач.  Обеспечение надежности: Гарантирование стабильной работы системы в различных условиях и ситуациях.  Задачи:  Анализ требований: Выявление и формализация требований к системе.  Выбор технологий: Определение технологий и инструментов, необходимых для реализации системы.  Разработка и тестирование: Создание и проверка компонентов системы на соответствие требованиям и спецификациям. |
|  | Что такое система физической защиты объекта? | Система физической защиты – это совокупность ресурсов, средств и методов, обеспечивающих предотвращение, обнаружение и ликвидацию угроз физической целостности объекта защиты |
|  | Перечислите основные риски ИБ. Дайте их определения. | Основные риски информационной безопасности:  Случайные. Объединяют непредвиденные события, когда происходит стечение обстоятельств, приводящее к неблагоприятным последствиям. Примеры: выход из строя технического оборудования, ЧС, перебои электроэнергии, повреждение коммуникационных каналов, поломка блокирующих устройств, ограничивающих доступ к информации.  Субъективные. Возникают из-за ошибок и неправильных действий персонала при обработке, хранении информации. Примеры: пренебрежение внутренними правилами и регламентом безопасности в компании: нарушение режима тайны, несанкционированный доступ к сведениям, нарушение правил передачи информации, использование незащищенных информационных каналов.  Объективные. Возникают в ходе использования защитных систем и сопутствующего технического оборудования. Примеры: проникновение в информационную систему вредоносного ПО, внедрение следящего, шпионского оборудования |
| **ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо**  **компонента системы) обеспечения информационной безопасности** | | |
|  | Какие требования предъявляются к комплексной системе безопасности объекта? | Целостность: Система должна обеспечивать целостность защищаемых объектов, т.е. предотвращать несанкционированные изменения или повреждения данных или ресурсов.  Конфиденциальность: Она должна обеспечивать конфиденциальность информации, предотвращая несанкционированный доступ к ней.  Доступность: Система должна быть доступной для использования, когда это необходимо, предотвращая атаки или сбои, которые могут привести к недоступности.  Аутентификация и авторизация: Требуется обеспечение идентификации пользователей (аутентификации) и управление их доступом к ресурсам (авторизации), чтобы предотвратить несанкционированный доступ.  Мониторинг и аудит: Необходим контроль за действиями пользователей и системы с возможностью регистрации событий для последующего анализа и реагирования на инциденты безопасности |
|  | В чем суть гарантированного уничтожения? | Суть гарантированного уничтожения состоит в том, чтобы обеспечить необратимое и полное уничтожение конфиденциальной информации или материалов до такой степени, чтобы они не могли быть восстановлены или использованы каким-либо способом. |
|  | Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании? | Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа. |
|  | Охарактеризуйте понятие большие данные. | Большие данные-это область, которая рассматривает способы анализа, систематического извлечения информации из наборов данных или иного взаимодействия с ними, которые слишком велики или сложны для работы с традиционным прикладным программным обеспечением для обработки данных. |
|  | Какую информацию относят к секретной, конфиденциальной? | Конфиденциальная информация, как и государственная тайна, относится к информации ограниченного доступа. Согласно указу Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», к видам информации конфиденциального характера относятся: персональные данные, коммерческая тайна, служебная тайна, профессиональная тайна, тайна следствия и судопроизводства. |
|  | Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности? | Недостаток обучения по безопасности: Непонимание важности правил безопасности.  Необоснованный интерес к конфиденциальной информации: Интерес к данным вне обычных обязанностей.  Изменения в поведении или финансовом положении: Необъяснимые изменения могут указывать на внешние мотивы.  Избегание проверок безопасности: Отказ от сотрудничества или скрытие информации.  Частые нарушения правил безопасности: Игнорирование правил или повторные |
|  | Какие применяются методы защиты информации от промышленного шпионажа? | Шифрование данных.  Использование средств антивирусной защиты.  Ограничение доступа к конфиденциальной информации.  Мониторинг сетевой активности и обнаружение аномалий.  Обучение сотрудников по правилам безопасности. |
|  | Какие цели и задачи проведения тренингов по безопасности для сотрудников организации? | - Повышение осведомленности сотрудников о рисках информационной безопасности.  - Обучение правилам работы с конфиденциальной информацией.  - Подготовка к действиям в случае кибератак или утечки данных.  - Снижение вероятности социальной инженерии и фишинга. |
|  | Какие организационные меры обеспечения безопасности Вы знаете? | - Разработка политики информационной безопасности.  - Аудит безопасности систем и процессов.  - Установление ролей и полномочий пользователей.  - Контроль доступа к информации.  - Обеспечение физической безопасности помещений и оборудования |
|  | Какие технические меры обеспечения безопасности Вы знаете? | - Установка брандмауэров и антивирусного программного обеспечения.  - Использование систем мониторинга и обнаружения вторжений.  - Шифрование данных при передаче и хранении.  - Резервное копирование данных.  - Обновление программного обеспечения и патчей безопасности. |
|  | Основные принципы обеспечения ИБ | - Принцип минимизации привилегий доступа.  - Принцип разделения ответственности.  - Принцип защиты по умолчанию.  - Принцип недоверия (Zero Trust).  - Принцип непрерывности защиты. |
|  | Основные функции системы безопасности. | - Идентификация и аутентификация пользователей  - Управление доступом и привилегиями  - Мониторинг и анализ безопасности  - Шифрование данных  - Защита от вредоносных программ  - Резервное копирование и восстановление данных  - Физическая безопасность |
|  | Основные принципы политики ИБ. | - Принцип неотъемлемости  - Принцип минимизации рисков  - Принцип защиты конфиденциальности  - Принцип целостности данных  - Принцип доступности информации |
|  | Какое свойство информации является наиболее актуальным при обеспечении ИБ? Дайте его определение. | Наиболее актуальным свойством информации при обеспечении информационной безопасности является целостность. Целостность информации означает, что данные не были изменены или повреждены незаконно или случайно. |
|  | Свойство информации при котором невозможно ее искажение… | Целостность информации — состояние информации, при котором отсутствует любое её изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. |
|  | Охарактеризуйте ИБ поиска информации. | Информационная безопасность (ИБ) поиска информации включает в себя меры и методы обеспечения защиты информации в процессе ее поиска с использованием информационных технологий. Основные аспекты ИБ поиска информации включают контроль доступа к поисковым системам, защиту конфиденциальности результатов поиска, обеспечение целостности и достоверности найденной информации, а также защиту от вредоносных программ и атак на процесс поиска. |
|  | Охарактеризуйте ИБ обработки данных. | Информационная безопасность (ИБ) обработки данных охватывает все меры и методы, направленные на защиту данных в процессе их преобразования, обработки и хранения с использованием информационных технологий. Ключевые аспекты ИБ обработки данных включают контроль доступа к данным, шифрование информации, мониторинг целостности данных, защиту от утечек и несанкционированного доступа, а также обеспечение соответствия законодательным требованиям по защите данных. Важно также обеспечить безопасность при передаче данных между системами и при их хранении на серверах или в облаке. |
|  | Охарактеризуйте эмерджентные технологии. | Эмерджентные технологии (от англ. "emerging technologies") - это новые и развивающиеся технологии, которые имеют потенциал изменить способы работы, общения, производства и другие аспекты жизни людей и бизнеса. Эти технологии обычно находятся на стадии активного исследования и разработки, и могут включать в себя такие области как искусственный интеллект, интернет вещей, блокчейн, квантовые вычисления, биотехнологии, нанотехнологии и другие. |
|  | При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности? | При использовании метода криптографии пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности. |
|  | Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)? | Метод физического преграждения пути злоумышленнику к защищаемой информации называется физической защитой. |
|  | Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств? | Средства защиты информации, предназначенные для выполнения функций защиты информационной системы с помощью программных средств, называются программными средствами защиты информации. |
|  | Укажите модель управления доступом, к которой относится основная теорема безопасности. | Модель Белла — Лападулы — модель контроля и управления доступом, основанная на мандатной модели управления доступом |
|  | Какие виды информации существуют в зависимости от категории доступа к ней? | В зависимости от категории доступа к ней, информацию можно разделить на общедоступную, конфиденциальную, секретную и строго секретную. |
|  | Защищаемая информация – это.. | Защищаемая информация - это информация, требующая особого режима защиты и обращения. |
|  | Правовые методы обеспечения ИБ | Правовые методы обеспечения информационной безопасности включают законодательные акты, нормативные документы и правила, регулирующие обращение и защиту информации. |
|  | Способы представления информации о правах доступа. | Способы представления информации о правах доступа могут включать матрицы доступа, списки контроля доступа (ACL), ролевые модели доступа. |
|  | Характеристика качества информации | Характеристика качества включает такие аспекты как надежность, доступность, конфиденциальность, целостность и другие свойства системы. |
|  | Показатели и критерии эффективности | Показатели и критерии эффективности могут включать время реакции на инциденты, процент успешных атак, стоимость обеспечения безопасности и другие параметры |
|  | Методические вопросы оценки эффективности сложных систем. | Методические вопросы оценки эффективности сложных систем включают выбор критериев оценки, методики измерения и анализ результатов. |
|  | Дайте определение понятию «ядро безопасности» | Ядро безопасности - это основной компонент системы безопасности, обеспечивающий ее базовую защиту и функционирование. |
|  | Кратко опишите архитектуру защищенной системы | Архитектура защищенной системы включает в себя различные слои защиты (физический, сетевой, прикладной), механизмы контроля доступа, шифрование данных, мониторинг и другие элементы, обеспечивающие безопасность системы. |