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

|  |
| --- |
| **«Интеграция систем обработки и защиты информации»** |

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 | **Основание (ПС)** \*для профессиональных компетенций |
| ОПК-2 | Способен разрабатывать технический проект системы (подсистемы либокомпонента системы) обеспечения информационной безопасности | ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемыИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем | 06.033 Специалист по защите информации в автоматизированных системах  |
| ПК-4. | Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных | ИПК-4.3. Разрабатывает архитектуру системы защиты информации автоматизированных систем, а также интеллектуальных и информационно-аналитических систем в частности |  |

В результате изучения дисциплины обучающийся должен:

**владеть**: Умением проводить анализ рисков безопасности и разрабатывать соответствующие стратегии защиты..Навыками применения технических мер безопасности в разработке информационных систем; Методиками анализа угроз и рисков информационной безопасности.

**уметь:** Разрабатывать архитектуру системы защиты информации с учетом специфики деятельности организации. Проводить анализ уязвимостей информационных систем и разрабатывать меры по их устранению. Разрабатывать технический проект системы обеспечения информационной безопасности; Проектировать компоненты и подсистемы защищенных информационных систем

**знать:** Принципы построения архитектуры систем защиты информации. Основные угрозы и уязвимости, с которыми сталкиваются информационные системы. Принципы построения защищенных информационных систем; Технические меры обеспечения информационной безопасности;

**1.2. Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| № | Тема (раздел дисциплины) (в соответствии с РПД) | Код компетенции |
|  | Тема 1. Разработка и реализация комплексных систем защиты информации, включающих в себя технические, организационные и правовые меры | ОПК-2ИОПК-2.2ИОПК-2.3ПК-4 ИПК-4.3 |
|  | Тема 2. Исследование методов и технологий интеграции различных систем обработки и защиты информации, в том числе с использованием облачных технологий |
|  | Тема 3. Анализ рисков информационной безопасности и разработка стратегий их минимизации |
|  | Тема 4. Оценка эффективности систем обработки и защиты информации и разработка рекомендаций по их оптимизации |
|  | Тема 5. Исследование вопросов международного сотрудничества в области информационной безопасности и интеграции систем обработки и защиты информации |

**1.3. Система оценивания по дисциплине**

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – зачет.

|  |  |
| --- | --- |
| **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 |

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами

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

**Перечень вопросов и заданий для подготовки к зачету**

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

1. Понятие интегрированной корпоративной информационной системы.
2. Основные типы интеграционных задач
3. Методология «открытых систем» и проблема интеграции.
4. Базовые модели интеграции (передача файлов, обмен сообщениями, удаленный вызов процедуры, использование общей базы данных) и их сильные и слабые стороны.
5. Уровни интеграции корпоративных приложений
6. Проблема стандартизации. Основные организации, занимающиеся утверждением стандартов.
7. Сценарии интеграции данных. Получение данных для хранилищ данных и систем бизнес-аналитики (технология ETL).
8. Платформы для интеграции корпоративной информации (Oracle Data Integrator, Informatica power center, IBM Information Server).
9. Технологии Big Data и проблема интеграции.
10. Опишите самый современный подход интеграции бизнес процессов
11. Чего помогает добиться Композитное (составное) приложение
12. Как называется система позволяющая наращивать и записывать в себя информацию и выстраивающая интеграционную систему
13. Управления рисками информационной безопасности
14. Основные источники угроз и виды нарушений в области информационной безопасности.
15. Процесс управления непрерывностью. Преимущества и проблемы процесса.
16. Процесс управления безопасностью. Цели и преимущества процесса
17. Основные положения стандарта BS7799
18. Основные положения стандарта ISO 17799.
19. Система информационной безопасности предприятия (задачи системы, объекты защиты) Основные источники угроз и виды нарушений в области информационной безопасности.
20. Цели и задачи интеграции систем обработки и защиты информации
21. Что такое ИСОЗИ и какие принципы лежат в её основе?
22. Какие методы и технологии используются для защиты информации в интегрированных системах?
23. Как обеспечить совместимость между различными системами обработки и защиты информации?
24. Какие роли и обязанности возлагаются на интегратора систем обработки и защиты информации?
25. Какие технологии шифрования применяются для защиты информации в интегрированных системах обработки и защиты?
26. Как происходит интеграция систем мониторинга и аудита в информационной безопасности?
27. Как происходит проектирование и настройка интегрированных систем обработки и защиты информации?
28. Какие меры предпринимаются для обеспечения защиты от DDoS-атак в интегрированных системах обработки и защиты информации?

**ПК-4:ИПК-4.3. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных.**

1. Как обеспечить безопасность при передаче данных между различными подсистемами в интегрированных системах?
2. Какие методы аутентификации и авторизации используются в интегрированных системах обработки и защиты информации?
3. Каким образом осуществляется интеграция различных уровней защиты в информационных системах?
4. Какие протоколы и стандарты используются при интеграции систем обработки и защиты информации?
5. Какие меры предпринимаются для обеспечения безопасности в случае вывода из эксплуатации информационных систем или оборудования?
6. Какие методы и технологии используются для обнаружения и предотвращения утечек конфиденциальной информации в интегрированных системах обработки и защиты информации?
7. Какие методы обеспечения целостности данных используются в интегрированных системах обработки и защиты информации?
8. Каким образом осуществляется резервное копирование и восстановление данных в интегрированных системах обработки и защиты информации?
9. Какие методы используются для защиты от атак на прикладные уровни в интегрированных системах обработки и защиты информации?
10. Как осуществляется мониторинг и анализ сетевого трафика в интегрированных системах обработки и защиты информации?
11. Каким образом осуществляется контроль и защита информации при передаче
12. Понятие интегрированной корпоративной информационной системы. Концепция ERP (Enterprise Resource Planning)
13. Типовая архитектура ERP-систем. ERP-система как центр интеграционного решения.
14. Как оценить уровень риска при использовании интегрированных систем?
15. Принципы построения архитектуры систем защиты информации.

**Вопросы для подготовки к зачету с «ключами» правильных ответов**

| № | Содержание вопроса | Правильный ответ |
| --- | --- | --- |
| **ОПК -2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.**  |
|  | Понятие интегрированной корпоративной информационной системы. | Интегрированная корпоративная информационная система (ИКИС) - это комплекс программных и аппаратных средств, объединяющий различные подсистемы и приложения предприятия для обеспечения единой информационной среды и повышения эффективности бизнес-процессов. |
|  | Основные типы интеграционных задач | Основные типы интеграционных задач включают в себя синхронизацию данных между различными системами, автоматизацию бизнес-процессов, обеспечение единого доступа к информации, обмен сообщениями между приложениями и другие. |
|  | Методология «открытых систем» и проблема интеграции. | Методология "открытых систем" предполагает создание систем с открытыми интерфейсами, что упрощает интеграцию различных приложений и обеспечивает их взаимодействие. Проблема интеграции заключается в несовместимости различных стандартов и технологий. |
|  | Базовые модели интеграции (передача файлов, обмен сообщениями, удаленный вызов процедуры, использование общей базы данных) и их сильные и слабые стороны. | Базовые модели интеграции включают передачу файлов, обмен сообщениями, удаленный вызов процедуры и использование общей базы данных. Каждая модель имеет свои сильные и слабые стороны, например, передача файлов проста в реализации, но не обеспечивает мгновенного обновления данных. |
|  | Уровни интеграции корпоративных приложений | Уровни интеграции корпоративных приложений могут быть представлены как технические (интеграция на уровне данных), так и бизнес-ориентированные (интеграция на уровне процессов). |
|  | Проблема стандартизации. Основные организации, занимающиеся утверждением стандартов. | роблема стандартизации в интеграции систем связана с необходимостью согласования форматов данных, протоколов обмена и других параметров. Организации, занимающиеся утверждением стандартов, включают ISO, ANSI, W3C и др. |
|  | Сценарии интеграции данных. Получение данных для хранилищ данных и систем бизнес-аналитики (технология ETL). | Сценарии интеграции данных включают получение данных для хранилищ данных и систем бизнес-аналитики с использованием технологии ETL (Extract, Transform, Load), которая позволяет извлекать данные из различных источников, преобразовывать и загружать их в целевую систему. |
|  | Платформыдляинтеграциикорпоративнойинформации (Oracle Data Integrator, Informatica power center, IBM Information Server). | Платформы для интеграции корпоративной информации, такие как OracleDataIntegrator, InformaticaPowerCenter, IBMInformationServer, предоставляют средства для автоматизации процессов интеграции данных и приложений. |
|  | Технологии Big Data и проблема интеграции. | Технологии Big Data представляют собой методы обработки больших объемов данных различных типов. Проблема интеграции заключается в необходимости сочетания Big Data технологий с существующими информационными системами предприятия. |
|  | Опишите самый современный подход интеграции бизнес процессов | Самый современный подход к интеграции бизнес-процессов включает использование цифровых технологий, автоматизацию процессов, аналитику данных и возможности машинного обучения для оптимизации бизнес-процессов и принятия управленческих решений. |
|  | Чего помогает добиться Композитное (составное) приложение | Композитное (составное) приложение помогает добиться гибкости и масштабируемости системы за счет комбинирования различных компонентов и сервисов. |
|  | Как называется система позволяющая наращивать и записывать в себя информацию и выстраивающая интеграционную систему | Система, позволяющая наращивать и записывать в себя информацию и выстраивающая интеграционную систему, может называться Центром Интеграции Данных (Data IntegrationHub) или Центром Интеграции Приложений (Application IntegrationHub). |
|  | Управления рисками информационной безопасности | Управление рисками информационной безопасности включает определение угроз, оценку уязвимостей, разработку мер по защите информации и мониторинг защиты для предотвращения инцидентов. |
|  | Основные источники угроз и виды нарушений в области информационной безопасности. | Основные источники угроз в области информационной безопасности включают в себя хакерские атаки, вирусы, фишинг, утечки данных, несанкционированный доступ к информации и другие виды нарушений. |
|  | Процесс управления непрерывностью. Преимущества и проблемы процесса. | Процесс управления непрерывностью (Business Continuity Management) направлен на обеспечение бесперебойного функционирования бизнес-процессов в случае чрезвычайных ситуаций. Преимущества процесса - минимизация потерь и повышение устойчивости предприятия. |
|  | Процесс управления безопасностью. Цели и преимущества процесса  | Процесс управления безопасностью (Security Management) направлен на обеспечение конфиденциальности, целостности и доступности информации предприятия. Цели - защита от угроз и минимизация рисков. |
|  | Основные положения стандарта BS7799  | Основные положения стандарта BS7799 (ISO/IEC 27001) - это международный стандарт по управлению информационной безопасностью, который определяет требования к созданию, внедрению, поддержке и улучшению системы управления информационной безопасностью. |
|  | Основные положения стандарта ISO 17799.  | Основные положения стандарта ISO 17799 (ISO/IEC 27002) - это международный стандарт по практическим аспектам управления информационной безопасностью, который содержит рекомендации по реализации мер по защите информации. |
|  | Система информационной безопасности предприятия (задачи системы, объекты защиты) Основные источники угроз и виды нарушений в области информационной безопасности. | Система информационной безопасности предприятия включает в себя задачи по защите конфиденциальности, целостности и доступности информации, а также объекты защиты - данные, программное обеспечение, аппаратное обеспечение и персонал предприятия. |
|  | Цели и задачи интеграции систем обработки и защиты информации | Цели и задачи интеграции систем обработки и защиты информации включают создание единой информационной безопасной среды, обеспечение целостности данных, защиту от несанкционированного доступа и обеспечение соответствия стандартам информационной безопасности. |
|  | Что такое ИСОЗИ и какие принципы лежат в её основе? | ИСОЗИ (интеграция систем обработки и защиты информации) - это подход к обеспечению безопасности информации, объединяющий процессы обработки данных и механизмы защиты. Его принципы включают комплексный подход к безопасности, прозрачность, согласованность, эффективность и гибкость. |
|  | Какие методы и технологии используются для защиты информации в интегрированных системах? | В интегрированных системах обработки и защиты информации используются методы шифрования данных, аутентификации пользователей, межсетевой безопасности, системы мониторинга и аудита, а также многоуровневые системы защиты от внешних и внутренних угроз. |
|  | Как обеспечить совместимость между различными системами обработки и защиты информации? | Совместимость между различными системами обработки и защиты информации обеспечивается путем использования стандартных протоколов и интерфейсов, а также разработкой единых методов интеграции и обмена данными. |
|  | Какие роли и обязанности возлагаются на интегратора систем обработки и защиты информации? | Интегратор систем обработки и защиты информации отвечает за проектирование, развертывание и поддержку интегрированных систем безопасности, включая выбор подходящих технологий, настройку систем, обучение персонала и обеспечение соответствия стандартам безопасности. |
|  | Какие технологии шифрования применяются для защиты информации в интегрированных системах обработки и защиты? | В интегрированных системах обработки и защиты информации применяются различные методы шифрования, включая симметричное и асимметричное шифрование, хэширование и цифровые подписи. |
|  | Как происходит интеграция систем мониторинга и аудита в информационной безопасности? | Интеграция систем мониторинга и аудита в информационной безопасности осуществляется путем сбора, анализа и отображения данных о событиях безопасности с различных источников в централизованной системе управления. Это позволяет оперативно реагировать на инциденты и анализировать тренды безопасности. |
|  | Как происходит проектирование и настройка интегрированных систем обработки и защиты информации? | Проектирование и настройка интегрированных систем обработки и защиты информации включает определение требований к безопасности, выбор подходящих технологий и решений, разработку архитектуры системы, настройку компонентов и проверку их работоспособности. |
|  | Какие меры предпринимаются для обеспечения защиты от DDoS-атак в интегрированных системах обработки и защиты информации? | Для защиты от DDoS-атак в интегрированных системах обработки и защиты информации используются меры, такие как фильтрация трафика, распределенное кеширование, использование CDN, а также системы обнаружения и предотвращения DDoS-атак. |
|  | **ПК-4. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных** |
|  | Как обеспечить безопасность при передаче данных между различными подсистемами в интегрированных системах? | Безопасность при передаче данных между различными подсистемами в интегрированных системах обеспечивается с помощью протоколов шифрования и аутентификации, защиты каналов связи, а также контроля целостности и конфиденциальности данных. |
|  | Какие методы аутентификации и авторизации используются в интегрированных системах обработки и защиты информации? | В интегрированных системах обработки и защиты информации могут использоваться методы аутентификации, такие как пароли, биометрическая идентификация, а также многофакторная аутентификация. Авторизация осуществляется на основе ролей и прав доступа пользователей к ресурсам системы. |
|  | Каким образом осуществляется интеграция различных уровней защиты в информационных системах? | Интеграция различных уровней защиты в информационных системах осуществляется путем объединения различных технологий и методов защиты на разных уровнях сети и приложений. Это включает в себя защиту на физическом уровне, сетевую безопасность, защиту операционной системы и приложений. |
|  | Какие протоколы и стандарты используются при интеграции систем обработки и защиты информации? | При интеграции систем обработки и защиты информации часто используются протоколы и стандарты, такие как IPsec, SSL/TLS, LDAP, Kerberos, OAuth, SAML и другие. Эти протоколы обеспечивают безопасную передачу данных, аутентификацию и авторизацию пользователей, а также управление доступом. |
|  | Какие меры предпринимаются для обеспечения безопасности в случае вывода из эксплуатацииинформационных систем или оборудования? | Для обеспечения безопасности в случае вывода из эксплуатации информационных систем или оборудования принимаются меры, такие как удаление конфиденциальной информации, физическое уничтожение носителей данных, отключение от сети и отмена доступа сотрудников. |
|  | Какие методы и технологии используются для обнаружения и предотвращения утечек конфиденциальной информации в интегрированных системах обработки и защиты информации? | Для обнаружения и предотвращения утечек конфиденциальной информации в интегрированных системах обработки и защиты информации используются методы шифрования данных, системы обнаружения утечек информации (DLP), контроль доступа на основе политик, а также мониторинг и аудит действий пользователей. |
|  | Какие методы обеспечения целостности данных используются в интегрированных системах обработки и защиты информации? | В интегрированных системах обработки и защиты информации используются методы обеспечения целостности данных, такие как хэширование, цифровые подписи, контроль целостности файлов и транзакционные журналы. Эти методы позволяют обнаруживать и предотвращать несанкционированные изменения данных. |
|  | Каким образом осуществляется резервное копирование и восстановление данных в интегрированных системах обработки и защиты информации? | Резервное копирование и восстановление данных в интегрированных системах обработки и защиты информации осуществляется путем создания резервных копий данных на регулярной основе, использования специализированного программного обеспечения для автоматизации процесса резервного копирования и восстановления данных в случае потери или повреждения. |
|  | Какие методы используются для защиты от атак на прикладные уровни в интегрированных системах обработки и защиты информации? | Для защиты от атак на прикладные уровни в интегрированных системах обработки и защиты информации используются методы, такие как фильтрация трафика на прикладном уровне, аудит безопасности приложений, использование механизмов шифрования и цифровой подписи. |
|  | Как осуществляется мониторинг и анализ сетевого трафика в интегрированных системах обработки и защиты информации? | Мониторинг и анализ сетевого трафика в интегрированных системах обработки и защиты информации осуществляется с помощью специализированных систем мониторинга трафика, анализаторов событий безопасности (SIEM), детекторов аномалий и других средств для выявления потенциальных угроз. |
|  | Каким образом осуществляется контроль и защита информации при передаче  | Контроль и защита информации при передаче в интегрированных системах обработки и защиты информации осуществляется через использование шифрования трафика (SSL/TLS), виртуальных частных сетей (VPN), механизмов аутентификации пользователей и мониторинга сетевой активности. |
|  | Понятие интегрированной корпоративной информационной системы. Концепция ERP (Enterprise Resource Planning) | Интегрированная корпоративная информационная система (ИКИС) представляет собой комплекс программных и аппаратных средств, объединенных для обеспечения эффективного управления бизнес-процессами организации. Концепция ERP (EnterpriseResourcePlanning) является одним из подходов к построению ИКИС, направленнымнаинтеграциювсехпроцессов и ресурсовпредприятия. |
|  | Типовая архитектура ERP-систем. ERP-система как центр интеграционного решения.  | Типовая архитектура ERP-систем включает модули для управления финансами, управления персоналом, управления закупками, управления производством и другие функциональные области. ERP-система выступает как центральное интеграционное решение, объединяющее все бизнес-процессы и данные организации. |
|  | Как оценить уровень риска при использовании интегрированных систем? | Уровень риска при использовании интегрированных систем можно оценить через анализ потенциальных угроз и уязвимостей системы, вероятность и возможные последствия инцидентов безопасности, соответствие стандартам безопасности и другие факторы. |
|  | Принципы построения архитектуры систем защиты информации. | Принципы построения архитектуры систем защиты информации включают комплексный подход к безопасности, учет специфики организации, применение слоя защиты на разных уровнях системы, использование шифрования данных и другие принципы. |