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

|  |
| --- |
| **«Защищенные информационные системы»** |

наименование дисциплины

|  |  |
| --- | --- |
| по образовательной программе высшего образования – программе | **магистратуры** |
|  | бакалавриата, специалитета, 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-2 | Способен разрабатывать технический проект системы (подсистемы либокомпонента системы) обеспечения информационной безопасности | ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем |
| ОПК-4 | Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок». | ИОПК-4.3. Формирует планы и проекты технических разработок защищённых информационных систем |

В результате изучения дисциплины обучающийся должен:

**Владеть:** навыками управления проектами систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; навыками разработки проектов и комплексов управления информационной безопасностью с учетом особенностей объектов защиты;

навыками сбора и обработки информации, разработки планов и программ научных исследований; навыками использования результатов обзора научно-технической литературы при решении вопросов информационной безопасности телекоммуникационных систем и сетей.

 **Уметь:** организовывать и осуществлять контроль за разработкой технических проектов систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; находить ведомственные документы в части проектирования подсистем и применения средств обеспечения информационной безопасности;

выбирать методы и средства решения задачи в рамках проводимого исследования, вырабатывать планы и программы проведения научных исследований и технических разработок.

**Знать:** методы разработки систем и комплексы управления информационной безопасностью с учетом особенностей объектов защиты; основные компоненты технического проекта; перечень необходимых исходных данных для проектирования подсистем либо компонентов системы;

методы сбора, обработки, анализа и систематизации научно-технической информации;

современную научно-техническую литературу, нормативные и методические документы по вопросам информационной безопасности.

**1.2. Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| № | Тема (раздел дисциплины) (в соответствии с РПД) | Код компетенции и индикаторы достижения компетенций |
|  | Введение в предмет «защищённые информационные системы» | ОПК-2, ИОПК-2.3. ОПК-4:ИОПК-4.3 |
|  | Интегральная безопасность информационных систем | ОПК-2, ИОПК-2.3. ОПК-4:ИОПК-4.3 |
|  | Безопасность хранения и передачи информации | ОПК-2, ИОПК-2.3. ОПК-4:ИОПК-4.3 |
|  | Методы проектирования и анализа информационных систем  | ОПК-2, ИОПК-2.3. ОПК-4:ИОПК-4.3 |
|  | Определение степени защищенности информационной системы | ОПК-2, ИОПК-2.3. ОПК-4:ИОПК-4.3 |
|  | Реализация программ информационной защиты и защиты информации  | ОПК-2, ИОПК-2.3. ОПК-4:ИОПК-4.3 |

**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 |

**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 зачету**

**ОПК-2: ИОПК-2.3.** **Способен разрабатывать технический проект системы (подсистемы либо**

**компонента системы) обеспечения информационной безопасности,**

1. Общие определения и характеристики информационных систем. Структура и классификация систем.
2. Понятие сложности, критерии и свойства. Критерии и свойства для информационной системы.
3. Вероятностная модель системы и пример пограничных состояний. Базовые информационные процессы в системах.
4. Основные принципы обеспечения информационной безопасности для информационных систем.
5. Методическая и нормативная база для построения защищенных систем.
6. Виды защищенных информационных систем в соответствии с требованиями ГОСТ.
7. Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ.
8. Понятие о задаче интегральной безопасности информационных систем.
9. Примеры задач интегральной безопасности.
10. Физическая безопасность информационных систем.
11. Безопасность сетей и телекоммуникационных устройств.
12. Безопасность ПО.
13. Обеспечение конфиденциальности, целостности и доступности данных.
14. Постановка задачи, её структура.
15. Частный, комплексный и интегральных подходы к решению проблемы передачи и хранения данных.
16. Постановка задачи проектирования и анализа информационной системы. 17. Модель системы с общим перекрытием.
17. Концептуальные требования направленные на обеспечение безопасности функционирования информационной системы.
18. Важнейшие принципы построения архитектуры ИС.

**ОПК-4: ИОПК-4.3. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок,**

1. Анализ безопасности ИС.
2. Постановка задачи защищённости ИС.
3. Наличие и полнота политики безопасности.
4. Гарантированность безопасности.
5. Трёхуровневая модель параметров оценки защищенности ИС.
6. Аудит сетей связи. Мониторинг функционирования, обнаружение атак и принятие адекватных мер противодействия.
7. Средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (File Encryption System – FES).
8. Средства авторизации и разграничения доступа к информационным ресурсам, а также защита от несанкционированного доступа к информации с использованием технологии токенов (смарт-карты, touch-memory, ключи для USB-портов и т.п.).
9. Средства защиты от внешних угроз при подключении к общедоступным сетям связи, а также средства управления доступом Интернета с использованием технологии межсетевых экранов (FireWall) и содержательной фильтрации (Content Inspection).
10. Политика реализации межсетевых экранов и их функциональные возможности. Классификация межсетевых экранов. Недостатки фильтрующего маршрутизатора (Filter Router - FR).
11. Шлюз сеансового уровня (Session Level Gateway - SLG). Шлюз уровня приложений (Application Layer Gateway - ALG). Преимущества ALG.
12. Что такое Антивирусы?
13. Средства обеспечения активного исследования защищенности информационных ресурсов с использованием технологии обнаружения атак (Intrusion Detection).
14. Инфраструктура открытых ключей (Public Key Infrastruture - PKI).
15. Средства обеспечения конфиденциальности, целостности, доступности и подлинности информации, передаваемой по открытым каналам связи с использованием технологии защищенных виртуальных частных сетей (VPN).
16. Четыре вида архитектуры организации защиты информации на базе применения технологии VPN. Классификация VPN.
17. Средства обеспечения централизованного управления системой ИБ в соответствии с согласованной и утвержденной политикой безопасности.
18. Информация и данные. Свойства информации. Функции информации.
19. Информационная безопасность и защита информации. Задачи информационной безопасности.
20. Направления информационной безопасности.
21. Составляющие информационной безопасности.
22. Нормативно-правовое обеспечение информационной безопасности. Основные документы.
23. Государственная тайна и ее защита.
24. Ответственность за нарушения в сфере информационной безопасности.
25. Защита персональных данных. Понятия и основные документы.
26. Регуляторы в области защиты персональных данных. Их функции и требования.
27. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
28. Угрозы и риски информационной безопасности. Источники угроз. Виды угроз.
29. Риски нарушения информационной безопасности. Систематизация рисков. Измерение рисков, шкалы рисков.
30. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь.
31. Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации.

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

| № | Содержание вопроса | Правильный ответ |
| --- | --- | --- |
| **ОПК-2.: ОПК-2: ИОПК-2.3 . Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности** |
|  | 1. Общие определения и характеристики информационных систем. Структура и классификация систем. | Информационная система - это система, предназначенная для сбора, обработки, хранения и передачи информации. Она состоит из аппаратных и программных компонентов, а также людей, которые используют эту систему. Информационные системы могут быть автоматизированными или ручными.Структура и классификация систем:Информационные системы могут быть классифицированы по различным признакам, таким как цель использования (управленческие, бухгалтерские, производственные), масштаб (локальные, глобальные), способу обработки данных (пакетные, онлайн), и др. Структура информационной системы включает в себя аппаратное обеспечение, программное обеспечение, базы данных, пользователей и процессы обработки информации. |
|  |  2. Понятие сложности, критерии и свойства. Критерии и свойства для информационной системы.  | Сложность информационной системы - это степень ее сложности, которая определяется количеством компонентов, взаимосвязей между ними и степенью детализации. Критерии сложности могут включать количество функций, объем данных, скорость обработки и другие параметры. Свойства информационной системы могут быть надежность, эффективность, масштабируемость и др. |
|  | 3. Вероятностная модель системы и пример пограничных состояний. Базовые информационные процессы в системах.  | Вероятностная модель системы используется для анализа вероятности возникновения определенных событий или состояний в системе. Пограничные состояния - это состояния системы, которые находятся на грани нормального и аварийного функционирования. Базовые информационные процессы включают в себя сбор данных, их обработку, хранение и передачу. |
|  | 4. Основные принципы обеспечения информационной безопасности для информационных систем. | Основные принципы обеспечения информационной безопасности включают конфиденциальность (защита от несанкционированного доступа), целостность (защита от изменения данных без разрешения), доступность (гарантирование доступа к данным при необходимости) и аутентификацию (проверка личности пользователей). |
|  | Методическая и нормативная база для построения защищенных систем.  | Для построения защищенных информационных систем используются различные методики и стандарты. Например, ISO/IEC 27001 - стандарт по управлению информационной безопасностью, GDPR - правила по защите персональных данных в Европейском союзе. Также существуют методические рекомендации от различных организаций и институтов по обеспечению безопасности информационных систем. |
|  | Виды защищенных информационных систем в соответствии с требованиями ГОСТ.  | Согласно требованиям ГОСТ, защищенные информационные системы могут быть классифицированы на следующие виды:- Защищенные от несанкционированного доступа системы (ЗНД);- Защищенные от несанкционированного доступа и утечки информации системы (ЗНДИ);- Защищенные от несанкционированного доступа, утечки и уничтожения информации системы (ЗНДУ). |
|  | Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ.  | Согласно требованиям ГОСТ, принципы защиты информации в автоматизированных системах включают:- Принцип минимизации доступа: предоставление доступа к информации только необходимым пользователям;- Принцип целостности: обеспечение непрерывности и недопуск изменения информации без разрешения;- Принцип конфиденциальности: обеспечение защиты информации от несанкционированного доступа;- Принцип доступности: гарантирование доступа к информации для авторизованных пользователей. |
|  | Понятие о задаче интегральной безопасности информационных систем.  | Задача интегральной безопасности информационных систем заключается в обеспечении комплексной защиты системы от различных угроз, включая атаки, вирусы, утечку информации, а также обеспечение непрерывной работы системы и защиту от несанкционированного доступа. |
|  | Примеры задач интегральной безопасности.  | Мониторинг и анализ событий в системе для выявления аномалий;- Резервное копирование данных для обеспечения их сохранности;- Управление доступом к данным и ресурсам с помощью авторизации и аутентификации пользователей. |
|  | Физическая безопасность информационных систем.  | Физическая безопасность информационных систем включает в себя меры по защите физического оборудования, серверов, центров обработки данных от несанкционированного доступа, кражи, пожаров и других физических угроз. Это может включать контроль доступа, видеонаблюдение, антикражные меры и другие технические средства для обеспечения безопасности. |
|  | Безопасность сетей и телекоммуникационных устройств.  | Могут включать следующее:- Использование сильных паролей и регулярное их обновление.- Шифрование данных при передаче через сети.- Установка и регулярное обновление антивирусного ПО и брандмауэров.- Ограничение доступа к сетевым ресурсам на основе принципа "минимум привилегий".- Мониторинг сетевого трафика для выявления подозрительной активности.- Регулярное обновление программного обеспечения и патчей для закрытия уязвимостей.- Обучение сотрудников о правилах безопасности и социальной инженерии. |
|  | Модель системы с общим перекрытием. | Модель системы с общим перекрытием предполагает наличие общих элементов или функций между различными компонентами системы, что позволяет им работать взаимосвязанно и эффективно. |
|  | Обеспечение конфиденциальности, целостности и доступности данных.  | Для обеспечения конфиденциальности, целостности и доступности данных необходимо использовать соответствующие меры безопасности, такие как шифрование данных, установка антивирусного ПО, регулярное резервное копирование информации, контроль доступа к данным и мониторинг сетевой активности. |
|  | Постановка задачи, её структура.  | Постановка задачи включает определение целей проекта, выделение этапов работы, определение ресурсов и сроков выполнения. Структура задачи может включать в себя формулировку проблемы, анализ требований, разработку плана действий, реализацию и контроль результатов. |
|  | Частный, комплексный и интегральных подходы к решению проблемы передачи и хранения данных.  | Частный подход к решению проблемы передачи и хранения данных ориентирован на решение конкретной задачи или проблемы. Комплексный подход предполагает использование нескольких методов и технологий для достижения цели. Интегральный подход включает в себя объединение различных аспектов для создания единой системы решения проблемы. |
|  | Постановка задачи проектирования и анализа информационной системы.  | Постановка задачи проектирования и анализа информационной системы включает определение требований к системе, анализ бизнес-процессов, моделирование данных и проектирование архитектуры системы. |
|  | Концептуальные требования направленные на обеспечение безопасности функционирования информационной системы.  | включают в себя защиту от несанкционированного доступа, обеспечение целостности данных, управление доступом к информации и резервное копирование данных |
|  | Важнейшие принципы построения архитектуры ИС.  | Важнейшие принципы построения архитектуры информационной системы включают модульность, расширяемость, гибкость, надежность, безопасность и эффективность работы системы |
| **ОПК-4: ИОПК-4.3. . Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок** |
|  | Что включает в себя анализ безопасности ИС.  | Анализ безопасности информационной системы включает в себя оценку уязвимостей, угроз и рисков, разработку мер по обеспечению безопасности, тестирование системы на проникновение и мониторинг безопасности в реальном времени. |
|  | Постановка задачи защищённости ИС.  | включает в себя определение угроз, уязвимостей и рисков, анализ потенциальных угроз, разработку мер по обеспечению безопасности, реализацию защитных механизмов и контроль за их эффективностью. |
|  | Наличие и полнота политики безопасности.  | определяются установленными правилами, процедурами и мерами по обеспечению безопасности, а также степенью их соответствия требованиям безопасности. Полнота политики безопасности означает наличие всех необходимых компонентов для обеспечения безопасности информационной системы. |
|  | Гарантированность безопасности.  | предполагает обеспечение непрерывной защиты от угроз и атак, а также возможность быстрого обнаружения и реагирования на инциденты безопасности. |
|  | Трёхуровневая модель параметров оценки защищенности ИС.  | включает оценку технических, организационных и процедурных аспектов безопасности. Технические параметры оценивают технологии и механизмы защиты, организационные параметры оценивают политику безопасности и управление рисками, а процедурные параметры оценивают процессы обеспечения безопасности. |
|  | Аудит сетей связи. Мониторинг функционирования, обнаружение атак и принятие адекватных мер противодействия. | Аудит сетей связи включает в себя проверку соответствия сетевых конфигураций установленным стандартам безопасности, обнаружение уязвимостей и рисков, анализ трафика с целью выявления аномалий и атак, а также принятие мер по предотвращению или прекращению атак и нарушений безопасности. Мониторинг функционирования сетей связи предполагает непрерывное отслеживание сетевой активности, обнаружение аномалий и инцидентов безопасности, а также реагирование на них с использованием адекватных мер по противодействию. |
|  | Средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (File Encryption System – FES).  | File Encryption System (FES) - это технология защиты информации на файловом уровне, которая позволяет шифровать данные перед их сохранением на диске или другом носителе. Основной принцип работы FES заключается в том, что файлы преобразуются в зашифрованный формат с использованием специальных алгоритмов шифрования, что делает их недоступными для несанкционированного доступа. |
|  | Средства защиты от внешних угроз при подключении к общедоступным сетям связи, а также средства управления доступом Интернета с использованием технологии межсетевых экранов (FireWall) и содержательной фильтрации (Content Inspection).  | Средства защиты от внешних угроз при подключении к общедоступным сетям связи включают в себя использование межсетевых экранов (FireWall) и содержательной фильтрации (Content Inspection). Межсетевые экраны позволяют контролировать трафик между внутренней и внешней сетями, а также фильтровать содержимое пакетов данных для предотвращения атак. |
|  | Политика реализации межсетевых экранов и их функциональные возможности. Классификация межсетевых экранов. Недостатки фильтрующего маршрутизатора (Filter Router - FR).  | Политика реализации межсетевых экранов определяет правила и процедуры их использования, а также функциональные возможности, такие как блокирование определенных портов или протоколов, контроль доступа к ресурсам сети и т.д. Межсетевые экраны классифицируются по уровню защиты и функциональности. Недостатки фильтрующего маршрутизатора (Filter Router - FR) могут включать ограниченные возможности фильтрации и недостаточную защиту от сложных атак. |
|  | Шлюз сеансового уровня (Session Level Gateway - SLG). Шлюз уровня приложений (Application Layer Gateway - ALG). Преимущества ALG. | Шлюз сеансового уровня (Session Level Gateway - SLG) и шлюз уровня приложений (Application Layer Gateway - ALG) являются средствами защиты информационных систем от угроз. ALG имеет преимущества перед SLG, такие как более глубокая инспекция трафика на уровне приложений и более эффективное обнаружение атак. |
|  | Антивирусы - это | Антивирусы - это программное обеспечение, предназначенное для обнаружения, блокирования и удаления вредоносных программ, таких как вирусы, трояны, шпионские программы и другие угрозы, которые могут нанести вред компьютеру или информации. |
|  | Средства обеспечения активного исследования защищенности информационных ресурсов с использованием технологии обнаружения атак (Intrusion Detection).  | то специализированные системы, которые мониторят сетевой трафик и системные журналы на предмет необычной активности, аномалий и попыток несанкционированного доступа к информационным ресурсам. |
|  | Инфраструктура открытых ключей (Public Key Infrastruture - PKI).  | это набор технологий, стандартов и протоколов, который обеспечивает безопасное хранение, распространение и использование открытых ключей для шифрования данных, цифровой подписи и аутентификации в сети. |
|  | Средства обеспечения конфиденциальности, целостности, доступности и подлинности информации, передаваемой по открытым каналам связи с использованием технологии защищенных виртуальных частных сетей (VPN).  | это специальные сетевые технологии, которые позволяют создать зашифрованный туннель для безопасной передачи данных через открытые сети, обеспечивая конфиденциальность, целостность и аутентификацию информации. |
|  | Четыре вида архитектуры организации защиты информации на базе применения технологии VPN. Классификация VPN. | Классификация VPN:- Клиент-серверная архитектура VPN- Сайт-к-сайту архитектура VPN- Удаленный доступ к сети (Remote Access VPN)- Виртуальная частная сеть на основе шифрования (Encrypted VPN) |
|  | Средства обеспечения централизованного управления системой ИБ в соответствии с согласованной и утвержденной политикой безопасности. | программные и аппаратные средства, которые позволяют централизованно управлять политиками безопасности, мониторить события безопасности и реагировать на инциденты в информационной системе. |
|  | Информация и данные. Свойства информации. Функции информации. | Информация - это данные, обработанные и представленные в понятной форме для принятия решений. Свойства информации включают конфиденциальность, целостность и доступность. Функции информации - хранение, передача и обработка данных для достижения целей организации. |
|  | 38. Информационная безопасность и защита информации. Задачи информационной безопасности | комплекс мер и технологий, направленных на обеспечение конфиденциальности, целостности, доступности и аутентичности информации от различных угроз и рисков. Задачи информационной безопасности включают определение угроз, разработку политик безопасности, обучение персонала и реагирование на инциденты. |
|  | Направления информационной безопасности. | включают технические меры защиты (криптография, антивирусные программы), организационные меры (политики безопасности, обучение персонала), физические меры защиты (контроль доступа к помещениям) и правовые меры (законодательство о защите данных). |
|  | Составляющие информационной безопасности. | Составляющие информационной безопасности включают технические средства защиты (firewall, антивирусные программы), организационные меры (политики безопасности, процедуры доступа), человеческий фактор (обучение персонала, контроль действий) и правовые аспекты (законы о защите данных). |
|  | Нормативно-правовое обеспечение информационной безопасности. Основные документы. | Нормативно-правовое обеспечение информационной безопасности включает в себя ряд основных документов, определяющих правила и требования по защите информации. К ним относятся:- Федеральный закон "О защите информации" от 27 июля 2006 года;- Постановление Правительства РФ "Об утверждении Правил обработки персональных данных" от 1 ноября 2012 года;- Федеральный закон "О персональных данных" от 27 июля 2006 года;- ГОСТы и стандарты по информационной безопасности. |
|  | Составляющие информационной безопасности. | Информационная безопасность включает в себя несколько ключевых составляющих, которые помогают обеспечить защиту информации от угроз и рисков. Вот основные составляющие информационной безопасности: Конфиденциальность, Целостность, Доступность, Аутентификация, Надежность, Шифрование. |
|  | Государственная тайна и ее защита. | Государственная тайна - это сведения, составляющие государственную тайну, обладание которыми ограничено и регулируется законодательством. Защита государственной тайны осуществляется в соответствии с законодательством РФ, а также специальными инструкциями и правилами. |
|  | Ответственность за нарушения в сфере информационной безопасности. | может быть административной, уголовной или гражданско-правовой. Нарушения могут включать несанкционированный доступ к информации, утрату данных, утечку конфиденциальной информации и другие действия, противоречащие законодательству. |
|  | Защита персональных данных. Понятия и основные документы. | это комплекс мер и технологий, направленных на обеспечение конфиденциальности и безопасности информации о физических лицах. Основные документы в этой области включают Федеральный закон "О персональных данных", Постановление Правительства РФ "Об утверждении Правил обработки персональных данных" и другие нормативные акты. |
|  | Регуляторы в области защиты персональных данных. Их функции и требования. | Регуляторы в области защиты персональных данных в России включают в себя Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и Уполномоченного по правам человека в Российской Федерации. Их функции включают контроль за соблюдением законодательства о персональных данных, выдачу лицензий на обработку персональных данных и рассмотрение жалоб граждан. |
|  | Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных | Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных может быть административной, уголовной или гражданско-правовой. Нарушения могут повлечь штрафы, административные наказания или уголовную ответственность. |
|  | Угрозы и риски информационной безопасности. Источники угроз. Виды угроз. | Угрозы информационной безопасности могут иметь различные источники, такие как хакеры, вредоносное программное обеспечение, социальная инженерия, утечки данных, природные катастрофы и другие факторы. Виды угроз включают кибератаки, утечку данных, отказ в обслуживании (DDoS), фишинг и другие. |
|  | Риски нарушения информационной безопасности. Систематизациярисков. Измерение рисков, шкалы рисков. | Риски нарушения информационной безопасности могут быть систематизированы по различным критериям, таким как вероятность возникновения события, потенциальный ущерб от инцидента, степень защищенности системы и другие параметры. Измерение рисков может проводиться с использованием шкал рисков, которые оценивают вероятность и последствия инцидентов. |
|  | Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизацияпотерь. | Технологии оценки угроз, уязвимостей, рисков и потерь включают методики анализа рисков (Risk Analysis), оценку уязвимостей (Vulnerability Assessment), моделирование угроз (Threat Modeling) и другие подходы. Оптимизация потерь может проводиться путем принятия мер по снижению рисков, использованию защитных механизмов и резервированию информационных ресурсов. |
|  | Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации. | Экономические проблемы информационных ресурсов включают определение затрат на защиту информации, оценку экономической эффективности мер по обеспечению безопасности и выбор оптимальных стратегий защиты. Основные подходы к определению затрат на защиту информации включают методику Total Cost of Ownership (TCO), оценку затрат на реализацию технологий безопасности и расчет экономической эффективности мероприятий по защите информации. |