Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

Перечень вопросов, заданий, тем для подготовки к текущему контролю

Основные формы для текущего контроля знаний:

— участие в дискуссиях при обсуждении вопросов на семинарах;

— подготовка и выступление (с представлением презентации) по проблемным темам дисциплины;

— тематический опрос на семинарах по обсуждаемым вопросам;

— выполнение аудиторных контрольных заданий

— подготовка докладов по тематике дисциплины и выступление на семинаре.

Примерный перечень вопросов для контрольной работы

1. Дать определение и характерные признаки информационного общества и показать противоречивость его развития.
2. Раскрыть понятие информационной безопасности как правового аспекта регулирования отношений доступа.
3. Показать и обосновать различие сущностей угроз информации и информационных угроз.
4. Показать взаимосвязь информационных рисков и рисков кредитно-финансовой деятельности и возможного ущерба от них.
5. Сформулировать понятия киберпространства и киберсреды, показать их общность и различие в практических приложениях.
6. Предложить методы и способы создания доверенной организационно-технологической среды обработки информации и условий защищённости на объектах информатизации.
7. Обосновать базовые функции защиты от НСД к информации при её автоматизированной обработке.
8. Показать основные уязвимости телекоммуникационной среды и связанные с ними способы обеспечения информационной безопасности сетей передачи данных.
9. Обосновать базовые положения эффективности использования криптографических средств для защиты информации в информационных технологиях.

10. Раскрыть проблему скрытного внедрения в программно-техническую и телекоммуникационную среду и её возможные деструктивные последствия.

11. Раскрыть природу возможной утечки информации по техническим и физическим каналам и предложить способы и методы предотвращения её утечки.

12. Выполнить сравнительный анализ технологий аутентификации по наличию знания, обладанию предметом и путём использования биометрических методов.

13. Выполнить сравнительный анализ технологий дискреционного, мандатного и ролевого управления доступом.

14. Пояснить проблемы доверенной программно-технической и телекоммуникационной среды в отечественной практике внедрения информационных технологий и способы обеспечения доверенности.

15. Рассмотреть и обосновать значимость проблемы компьютерных вирусов и технологий защиты от них.

16. Сформулировать основные положения системного подхода к обеспечению информационной безопасности автоматизированной обработки информации.

17. Раскрыть понятия целевой системы, большой системы, сложной системы и предложить примеры из области обеспечения информационной безопасности.

18. Сформулировать понятия дескриптивной и конструктивной задачи системного анализа и пояснить способы их решения на примерах из области обеспечения информационной безопасности.

19. Представить и обосновать СОИБ как целевую обеспечивающую систему в операционном окружении АИС.

20. Сформулировать понятие системных технологий обеспечения информационной безопасности и предложить их примеры.

21. Представить и пояснить структурно-функциональную схему комплексной системы защиты информации от НСД.

22. Пояснить постановку и обосновать необходимость применения архитектуры сегментации среды и технологий обработки и защиты данных по признаку безопасности.

23. Предложить варианты технологий и средств защиты информации при работе удалённых пользователей в сети.

24. Обосновать необходимость, представить схему и пояснить работу технологий защиты от атак из Интернет методом демилитаризованного зонирования.

25. Предложить и обосновать структуру КСЗИ.

26. Сформулировать и пояснить особенности технологий обеспечения информационной безопасности ситуационных центров (СЦ).

27. Обосновать выделение общесистемных компонентов информационной индустрии – объектов защиты информации корпораций.

28. Сформулировать функции и задачи комплексной системы защиты информации (КСЗИ) объектов информатизации корпорации.

29. Пояснить функции и структурное взаимодействие подсистем информационного обеспечения (ПОИБ) АСОД и систем обеспечения информационной безопасности (СОИБ) объектов информатизации.

30. Раскрыть технологии менеджмента информационного обеспечения корпорации.

Примерные темы докладов по тематике дисциплины:

1. Требования, методические подходы и технологии обеспечения доверенной организационно-технологической среды и условий защищённости на объектах информатизации.
2. Перспективы развития и повышения эффективности технологий аутентификации при автоматизированной обработке.
3. Анализ методов и методик выявления вирусного заражения программно-технической среды при функционировании АС и тенденций развития антивирусных средств.
4. Сравнительный анализ эффективности использования криптографических систем с открытым и закрытым ключом в АИС.
5. Перспективные направления развития средств мониторинга вторжений в программно-техническую среду АС и выявления кибератак.
6. Общие проблемы, новые задачи и технологии обеспечения информационной безопасности при использовании виртуальных сред и ресурсов.
7. Системная инженерия и подходы её использования при реализации технологий обеспечения информационной безопасности.
8. Системный подход и комплексная защита от несанкционированного доступа к информации в автоматизированных информационных системах.
9. Комплексные системы и технологии защиты информации объектов информатизации.

10. Концепция построения системы управления информационной безопасностью в корпоративном информационном пространстве.

11. Обоснование архитектурных решений по построению сегментации среды автоматизированной обработки информации по признаку безопасности.

12. Анализ, классификация и характеристика технологий и средств обеспечения информационной безопасности в телекоммуникационных системах.

13. Анализ подходов и технологий защиты информации от утечки по техническим каналам.

14. Политика использования Интернет на объекте информатизации в условиях обработки конфиденциальной информации.

15. Технологии обеспечения информационной безопасности в системах «облачных вычислений».

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Департамента информационной безопасности.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе «2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, знаний и умений

Таблица 6

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные и индикаторами достижения компетенций	Типовые контрольные задания
ПКН-1 Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационно	**Индикатор 1** Использует отечественные и зарубежные стандарты в области обеспечения информационной безопасности.	**Знать** требования и критерии отечественных и зарубежных стандартов оценки ИБ конкретных объектов **Уметь** выявлять угрозы и оценивать уязвимости ИБ с учётом конкретной специфики инфраструктуры объекта информатизации.	**Задание** Подобрать отечественные и зарубежные стандарты в области обеспечения ИБ для конкретного объекта

й безопасности конкретных объектов			
	Индикатор 2 Разрабатывает требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности.	**Знать** требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности **Уметь** разрабатывать требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности.	**Задание** Предложить перечень требований к системе обеспечения ИБ и разработать критерии оценки ее эффективности
	Индикатор 3 Демонстрирует навыки разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.	**Знать** нормативные требования и рекомендации по обеспечению информационной безопасности при информатизации и автоматизации деятельности организации. **Уметь** на основании результатов обследования и нормативных требований разрабатывать модели угроз и нарушителей для автоматизированных систем и комплексов, в целом для ОИ; формировать базовые положения политики информационной безопасности.	**Задание** Предложить методику разработки, структуру и состав политики информационной безопасности на объектах информатизации деятельности.
ПКН-2 Способность проектировать системы обеспечения информационной безопасности конкретных объектов	**Индикатор 1** Использует методы проектирования технологий обеспечения информационной безопасности, принципы построения и функционирования, принципы построения компьютерных систем и сетей, методы и методики оценки безопасности программно-аппаратных	**Знать** проблемы, уязвимости и угрозы, связанные с обеспечением информационной безопасности при функционировании организаций; направления, практики и технологии реализации основных функций назначения по защите информации и нейтрализации угроз ИБ. **Уметь** выбирать оптимальный набор методов и средств реализации технологий обеспечения информационной безопасности для конкретных объектов информатизации и автоматизированных систем.	**Задание** Определить набор типовых угроз безопасности информации при функционировании организаций и предложить оптимальный соответствующий им набор технологий нейтрализации.

	средств защиты информации, методы оценки эффективности политики безопасности, национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации.		
	Индикатор 2 Определяет параметры функционирования программно-аппаратных средств защиты информации, разрабатывает методики оценки защищенности программно-аппаратных средств защиты информации с целью определения уровня обеспечиваемой ими защищенности и доверия.	**Знать** регламенты работ и функции жизненного цикла проектируемых и эксплуатируемых автоматизированных систем; подходы и методы оценки защищенности программно-аппаратных средств защиты информации. **Уметь** осуществлять постановку задач анализа и обоснования оптимальности технологий и эффективности систем и средств обеспечения ИБ в соответствии с нормативными и методическими требованиями и регламентами.	**Задание** Предложить этапы жизненного цикла автоматизированных информационных систем в соответствии со стандартами и сформулировать возможный набор проектно-эксплуатационных и проектно-экономических задач на каждом этапе.
	Индикатор 3 Оценивает работоспособность применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.	**Знать** методику оценки работоспособности применяемых программно-аппаратных средств защиты информации **Уметь** проводить оценку работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.	**Задание** Провести анализ существующих методик оценки работоспособности применяемых программно-аппаратных средств защиты информации и на его основе предложить свою

			методику оценки для конкретного объекта информатизации
ПКН-3 Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	**Индикатор 1** Применяет нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации.	**Знать** нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа **Уметь** организовать разработку проекта и приёмо-сдаточные работы по завершению этапов проектирования в соответствии с нормативными требованиями.	**Задание** Подобрать набор базовых нормативно-методических документов и национальных стандартов в области защиты информации ограниченного доступа
	Индикатор 2 Использует необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	**Знать** регламентирующие деятельность по защите информации нормативно-правовые акты, действующие в организации **Уметь** применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	**Задание** На примере конкретного объекта информатизации подобрать локальные нормативно-правовые акты, регламентирующие деятельность по защите информации.
	Индикатор 3 Составляет организационно-распорядительные документы, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	**Знать** алгоритм разработки организационно-распорядительных, нормативных и методических документов, регламентирующих деятельность по защите информации в организации. **Уметь** разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	**Задание** Предложить свой проект организационно-распорядительного документа по обеспечению информационной безопасности на примере конкретного объекта

Примерные теоретические вопросы к зачету

1. Сформулировать и обосновать понятие информационного общества, проблемы и вызовы, связанные с информационной безопасностью.
2. Проанализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества.
3. Обосновать сущность обеспечения информационной безопасности как правовой аспект регулирования отношений доступа в среде обработки информации и информационного взаимодействия.
4. Рассмотреть модель отношений угроз информации, информационных угроз, информационных рисков и рисков основной деятельности институтов кредитно-финансовой деятельности.
5. Представить и охарактеризовать основные предметные направления реализации технологий обеспечения информационной безопасности в киберпространстве.
6. Предложить решения по обеспечению доверенной организационно-технологической среды и условий защищённости на объектах информатизации.
7. Определить методы и технологии защиты информации при электронном документообороте.
8. Обосновать и дать характеристику базовым функциям назначения по защите информации от несанкционированного доступа (НСД) в автоматизированных информационных системах.
9. Сформулировать проблемы и определить функции назначения по обеспечению информационной безопасности в телекоммуникационной среде при информационном взаимодействии.
10. Определить и обосновать целесообразность и эффективность применения криптографических средств защиты информации в технологиях автоматизированной обработки информации.
11. Перечислить и обосновать основные каналы и способы скрытного внедрения в программно-техническую среду компьютерных и телекоммуникационных систем.
12. Проанализировать природу формирования и извлечения информации по техническим каналам, виды технических и физических каналов утечки информации при её автоматизированной обработке.
13. Выполнить анализ и сравнить по критериям эффективности и технологичности дискреционное, мандатное и ролевое управление доступом.

14. Рассмотреть виды компьютерных вирусов и предложить технологии и средства защиты от вирусов и антивирусную политику на объекте информатизации.

15. Определить основные технологии и средства защиты информации в телекоммуникационных сетях и при сетевой организации автоматизированной обработки информации.

16. Предложить структуру, состав и технологии систем обнаружения вторжений.

17. Дать характеристику и обосновать необходимость системного подхода для обеспечения информационной безопасности при автоматизированной обработке информации.

18. Сформулировать подходы системной инженерии к созданию систем обеспечения информационной безопасности, обосновать целесообразность и эффективность их применения.

19. Обосновать достоинства и недостатки защиты информации в автоматизированных информационных системах, основанной на архитектуре сегментации среды обработки по признаку конфиденциальности (*выделение контуров безопасности*).

20. Предложить и обосновать структуру комплексной системы защиты информации (КСЗИ) объекта информатизации.

1.