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)

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

(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)

1. Паспорт оценочных средств

Направление подготовки (специальность): 10.04.01 Информационная безопасность
Дисциплина: Б1.Б.04 Защищенные информационные системы

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства
1	Комплексный подход к организации защищенных информационных систем. Основные понятия защищенных информационных систем.	Реферат, экзамен
2	Общие принципы построения защищенных информационных систем. Архитектура информационных систем на основе баз данных	Реферат, экзамен
3	Технологии проектирования баз данных. Разграничения доступа к ресурсам информационной системы	Реферат, экзамен
4	Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных	Реферат, экзамен
5	Способы хранения конфиденциальной информации. Основные направления защиты информации. Организационные меры защиты информации в организации.	Реферат, экзамен
6	Программно-аппаратные средства обеспечения информационной безопасности информационных систем.	Реферат, экзамен
7	Классификация firewall′ов. Их политики. Типы окружений firewall′ов. Политика безопасности firewall′а. Системы обнаружения атак. Безопасное использование службы доменных имен (DNS). Обеспечение безопасности WEB –серверов. Безопасность WEB – ориентированного контента. Технологии аутентификации и шифрования	Реферат, экзамен

2. Виды контроля по периодам обучения

2.1 Материалы для проведения текущего контроля:
Текущий контроль не предусмотрен программой.

2.2 Материалы для проведения промежуточной аттестации:
3 семестр.
Вид промежуточной аттестации – экзамен
Форма проведения – устный опрос

Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Типовые контрольные вопросы:

1. Понятие «информационная система».
2. Концепция безопасности информационной системы.
3. Цели обеспечения информационной безопасности.
4. Санкционированный и несанкционированный доступ.
5. Угрозы безопасности и каналы реализации угроз.
6. Уровни защиты информации.
7. Стандарты безопасности.
8. Классы защищенности информационных систем.
9. Нормативная база Российской Федерации.
10. Современная доктрина информационной безопасности Российской Федерации.
11. Трехуровневая архитектура информационных систем на основе баз данных.
12. Модели данных. Структура данных. Целостность реляционных данных.
13. Основные этапы проектирования баз данных.
14. Технологии проектирования на основе нормализации.
15. Технологии проектирования на основе модели «Сущность-связь».
16. Основные понятия систем разграничения доступа.
17. Сущность и определение политики безопасности.
18. Основные типы политик безопасности: мандатные, ролевые, контроля целостности информационных ресурсов, избирательного разграничения доступа.
19. Субъектно-объектная модель информационной системы.
20. Угрозы целостности информации. Способы противодействия.
21. Понятие и основные свойства транзакций. Механизм блокировок.
22. Декларативная и процедурная ссылочные целостности.
23. Способы поддержания ссылочной целостности. Триггеры и правила.
24. Угрозы конфиденциальности информации**.**
25. Средства идентификации и аутентификации в СУБД.
26. Средства управления доступом. Виды привилегий. Использование механизма ролей. Метки безопасности.
27. Использование представлений для обеспечения конфиденциальности информации.
28. Положение о конфиденциальной информации в электронном виде.
29. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов.
30. Способы хранение конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация.
31. Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей.
32. Классификация внутренних нарушителей: неосторожные, манипулируемые, саботажники, нелояльные, мотивированные извне. Другие градации.
33. Кадровая политика. Определение прав локальных пользователей. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации.

Типовые задания:

1. Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.
2. Классификация. Установление TCP – соединения. Пакетные фильтры, набор правил.
3. Пограничные роутеры. Stateful Inspection и Host-based firewall′ы. Персональные firewall′ы и их персональные устойства.

4. Прокси-сервер прикладного уровня. Выделеные прокси-серверы. Гибридные технологии firewall′ов.
5. Трансляция сетевых адресов (NAT).Статическая и скрытая трансляция NAT.
6. Принцип построения окружения firewall′a. DMZ –сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация.
7. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети. Расположение VPN-серверов.
8. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях.
9. Внешне доступные серверы. VPN и Dial-in серверы.
10. Внутренние серверы. DNS –серверы. SMTP – серверы.
11. Политика firewall′a. Реализация его набора правил. Тестирование политики firewall′a.
12. Возможные подходы к эксплуатации firewall′a. Сопровождение firewall′a и управление им.
13. Физическая безопасность окружения firewall′a. Администрирование firewall′a. Встраивание firewall′ов в ОС.
14. Стратегия восстановления после сбоев. Возможность создания логов firewall′a. Инциденты безопасности. Создание backup′ов firewall′ов.
15. Понятие системы обнаружения атак (IDS). Типы и базовая структура IDS.Совместное расположение Host и Target.
16. Разделение Host и управления. Полностью распределенное управление. Network-based IDS, Host-based IDS, Application-based IDS.
17. Анализ, выполняемый IDS.Определение злоупотреблений. Активные и пассивные ответные действия. Использование SNMP TRAPS.
18. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.
19. Безопасность DNS.Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности. Основные механизмы безопасности для сервисов DNS.
20. Данные DNS и ПО DNS. Name-серверы, Авторитетные и кэширующие Name-серверы. Resolver′ы.
21. Транзакции DNS. Запрос/ответ DNS. Зонная пересылка. Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.
22. Причины уязвимости WEB – сервера. Планирование развертывания WEB – сервера. Безопасное инсталлирование и конфигурирование используемой ОС.
23. Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на уровне ОС. Альтернативные платформы для web - сервера. Использование Appliances для web – сервера.
24. Специально усиленные ОС и web –серверы. Тестирование безопасности ОС. Безопасное инсталлирование и конфигурирование web – сервера. Соответствующий список действий.
25. Разграничение доступа для ПО web – сервера. Управление доступом к директории содержимого web – сервера.
26. Публикации информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
27. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности web-содержимого.
28. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP - адресе. Basic и Digest аутентификации.
29. SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS.

30. Список действий при использовании технологий аутентификации и шифрования. Wirewall прикладного уровня для Web: ModSecurity.

3.Критерии и показатели оценивания результатов обучения

3.1 Планируемые результаты обучения по дисциплине:

Таблица № 1

Результаты освоения образовательной программы *(Код и формулировка компетенций)*	**Уровень освоения компетенции** *(например, первый – базовый или пороговый, второй – углубленный, третий – продвинутый, при наличии)*	**Перечень планируемых результатов обучения по дисциплине** *(в целях формирования названной компетенции)*
ОК-2 способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	базовый	**Знать:** информационные технологии; профессиональные термины и понятия. **Уметь:** приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения. **Владеть:** методами поиска и обработки информации в новой предметной области.
ПК-2 способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	базовый	**Знать:** методы и технологии программирования и методы разработки эффективных алгоритмов решения прикладных задач; основные программные средства системного, прикладного и специального назначения; **Уметь:** выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; **Владеть:** навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и системы программирования для решения профессиональных задач; профессиональной терминологией.
ПК-3 способность администрировать подсистемы информационной безопасности объекта защиты	углубленный	**Знать:** методы разработки эффективных алгоритмов решения прикладных задач; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления базами данных; принципы построения информационных систем; структуру систем документационного обеспечения; эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; **Уметь:** выбирать необходимые инструментальные средства для решения профессиональных задач; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; **Владеть:** методами и средствами выявления угроз безопасности автоматизированным системам; методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; профессиональной терминологией;
ПК-4 способность участвовать в работах по реализации политики информационной	базовый	**Знать:** принципы и методы организационной защиты информации; основы реализации политики информационной безопасности; основные нормативные правовые акты в области ИБ и ЗИ; принципы организации информационных систем в соответствии с требованиями по защите информации;

безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		**Уметь:** формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; **Владеть:** навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; практическими навыками по реализации политики информационной безопасности.
ПК-7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования	базовый	**Знать:** нормативно-правовые документы по обеспечению информационной безопасности в России и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем; **Уметь:** анализировать и оценивать угрозы информационной безопасности объекта; интерпретировать и обобщать данные, формулировать выводы и рекомендации для проектирования подсистем и средств обеспечения информационной безопасности; **Владеть:** навыками обоснования, выбора, реализации и контроля результатов соответствующих проектных решений;
ПК-14 способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	базовый	**Знать:** основные понятия и методы в области управленческой деятельности; принципы и методы организационной защиты информации; основные принципы организации коллективной разработки автоматизированных информационных систем и технологий, модели жизненного цикла изделий программных и их разновидности; **Уметь:** оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; работать в коллективе; анализировать возможные конфликтные ситуации и искать пути к их разрешению; **Владеть:** методами организации и управления деятельностью служб защиты информации на предприятии; способами работы в коллективе, приемами цивилизованной дискуссии и навыками творческой работы в коллективе, способностью к критике и самокритике, терпимостью, способностью работать в коллективе.
ПК-15 способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	базовый	**Знать:** состав работ по вводу в эксплуатацию новых систем и средств обеспечения ИБ; методы концептуального проектирования технологий обеспечения информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; **Уметь:** организовывать работы по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организовать полный цикл работ по сдаче в эксплуатацию систем информационной безопасности; **Владеть:** навыками безопасного использования технических средств в профессиональной деятельности; навыками наладки и испытаний систем и средств обеспечения информационной безопасности.

2.1 Критерии и показатели оценки

Таблица № 2

Критерии	**Оценка**			
	«отлично»	**«хорошо»**	**«удовлетвори-тельно»**	**«неудовлетвори-тельно»**

1.Знание теоретических основ информационной безопасности	Студент демонстрирует глубокое знание теоретических основ и принципов, базовых понятий, информационной безопасности.	Студент достаточно хорошо владеет знаниями теоретических основ и принципов, базовых понятий, информационной безопасности.	Студент затрудняется с изложением теории, поверхностно ориентируется в базовых понятиях, которые используются при рассмотрении вопросов информационной безопасности.	Студент не понимает поставленной проблемы, не знает теоретических основ и принципов информационной безопасности.
2. Умение иллюстрировать теоретические знания на конкретных практических примерах.	Студент уверенно иллюстрирует теоретические положения обоснованными примерами.	Студент иллюстрирует ответ немного-численными конкретными примерами, испытывая затруднения при их подборе.	Студент может подкрепить теоретические положения примерами только после наводящих вопросов, допуская при этом ошибки.	Студент демонстрирует неумение проиллюстрировать теоретические положения практическими примерами.
3. Владение профессиональной терминологией.	Студент демонстрирует свободное владение понятийным аппаратом и умение быть корректным в употреблении терминологией.	Студент достаточно хорошо владеет профессиональной терминологией, в случае ошибки в употреблении термина способен исправить ее сам.	Студент слабо владеет профессиональной терминологией, до-пускает неточности в интерпретации понятий и определений в данной предметной области.	Студент не владеет профессиональной терминологией и не разбирается в понятийном аппарате дисциплины.

2.2 Порядок выставления общей оценки в рамках экзамена.

Общая оценка за ответ выставляется:

«отлично»:
а) ответы на два теоретических вопроса заслуживают оценки «отлично».

«хорошо»:
а) ответы на два вопроса заслуживают оценки «хорошо»;
б) один вопрос заслуживает оценки «отлично», второй – оценки «хорошо»;
в) ответ на один вопрос заслуживает оценки «отлично», а на второй – оценки «удовлетворительно».

«удовлетворительно»:
а) ответы на оба вопроса заслуживают оценки «удовлетворительно»;
б) ответы на один вопрос заслуживают оценки «хорошо», а на второй – «удовлетворительно».

«неудовлетворительно»:
а) ответы на оба вопроса не соответствуют необходимому объему знаний;
б) ответ на один вопрос заслуживает оценки «удовлетворительно», а на второй – «неудовлетворительно».