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)

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

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

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

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

Примерный перечень вопросов для подготовки к экзамену

Примеры теоретических и теоретико-практических вопросов к экзамену

1. Опишите, на каких законодательных актах основа законодательная база аудита информационной безопасности в РФ?
2. Опишите основные международные подходы к аудиту информационной безопасности.
3. Составьте список и охарактеризуйте наиболее часто применимые международные и отраслевые стандарты аудита информационной безопасности.
4. Опишите методы тестирования ИБ в информационной среде организации.
5. Назовите основные цели соответствия требованиям стандарта PCI DSS.
6. Перечислите тематические разделы требований в стандарте PCI DSS.
7. Опишите этапы процесса проведения оценки соответствия стандарту PCI DSS.
8. Перечислите этапы работ по проведению внешнего аудита ИБ.
9. Перечислите цели и задачи программы внешнего аудита ИБ.
10. Перечислите документы, анализируемые внешними аудиторами ИБ.
11. Опишите составные части отчета по внешнему аудиту ИБ.
12. Опишите показатели, используемые для оценки соответствия обеспечения ИБ организации требованиям СТО БР.
13. Опишите показатели, используемые для оценки соответствия обеспечения ИБ организации требованиям СТО БР.
14. Опишите показатели, используемые для оценки соответствия защиты информации финансовой организации требованиям ГОСТ Р 57580.1.
15. Назовите и кратко охарактеризуйте основные национальные и национальные отраслевые стандарты информационной безопасности.
16. Составьте план проверки обеспечения соблюдения мер идентификации и аутентификации в соответствии с PCI DSS.
17. Составьте план проверки организации на соблюдение базовых мер контроля доступа (согласно ГОСТ Р 57580.1-2017).
18. Только что организованная российская кредитная организация регионального значения наняла вас ка эксперта по ИБ, для того что вы создали список мер ИБ, который ей предстоит соблюдать. Составьте список законодательных актов, относящихся к ИБ под исполнение которых организация попадает.
19. Ваши друзья открыли ломбард и просят вас сказать им какие меры

безопасности они должны выполнять. Составьте список законодательных актов ИБ, под которые она попадает.

20. Составьте план аудита для российской компании с мультикультурным коллективом в период декабрь-январь.

Примеры практико-ориентированных (ситуационных) заданий

Задание № 1. Организация сохраняет магнитные носители с резервных копий в кабинете, размещенном непосредственно за помещением центра обработки данных. Консультант рекомендовал организации хранить резервные копии вне здания, в котором размещен центр обработки данных. Что консультант имел в виду, когда давал эту рекомендацию?

a) Катастрофа, которая может разрушить центр обработки данных также может разрушить резервную копию

b) В результате ротации резервной копии могут быть потеряны резервные копии, которые были выполнены несколько недель назад

c) Разрушение основной базы данных может потребовать быстрого восстановления данных с резервной копии

d) Физические средства защиты центра обработки данных недостаточны

Задание № 2. Какое из нижеприведенных положений наиболее важно с точки зрения управления непрерывностью бизнеса? Обоснуйте ваш выбор.

a) Резервный центр обработки данных защищен и размещен на необходимом расстоянии от основного центра обработки данных

b) Планы восстановления периодически проверяются

c) На резервном центре обработки данных доступно и протестировано аппаратное обеспечение средств резервного сохранения

d) Сетевые сервисы предоставляются различными провайдерами коммуникационных сервисов

Задание № 3. С какой из нижеперечисленных областей в наибольшей степени связана непрерывность функционирования бизнеса? Обоснуйте ваш выбор.

a) Бизнес процессы

b) Функционирование информационно-технологической инфраструктуры

c) Устойчивость к авариям

d) Восстановление данных

Задание № 4. Организация использует схему классификации, позволяющую определить критичность системы с точки зрения возможности аварийного восстановления. Основное приложение организации для ведения

электронной коммерции классифицировано как «Критическое». Как организация должна классифицировать DNS-сервера организации?

a) DNS-сервера должны быть классифицированы отдельно в соответствии с их критичностью

b) DNS-сервера не должны классифицироваться, так как они не содержат пользовательских данных

c) DNS-сервера должны быть классифицированы как не конфиденциальные, так как они не содержат пользовательских данных

d) DNS-сервера должны быть классифицированы как «Критические», так как пользователи с их помощью взаимодействуют с серверами электронной коммерции

Задание № 5. Аудитор выявил имеющую высокий риск уязвимость при тестировании средств защиты. Какие действия он должен предпринять в первую очередь? Обоснуйте ваш выбор.

a) Немедленно выполнить действия по уменьшению риска

b) Включить уязвимость в отчет и пометить тест как не прошедший проверку

c) Немедленно проинформировать представителей организации, аудит которой проводится

d) Немедленно проинформировать группу по аудиту.