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)

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

(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)

Примерные оценочные средства для текущего контроля успеваемости

Контрольная работа №1

1. Описать стуктуру основных средств защиты информации на предприятии.
2. Дать характеристику основных криптографической защиты.
3. Выбрать средство криптографической защиты на рабочем месте и обьяснить свой выбор

Контрольная работа №2

1. Выбрать приложение криптографической защиты на рабочем месте и обьяснить выбор (по параметрам).
2. Описать структуру открытой системы и разработать модель защиты информации в такой системе.
3. Описать модель безопасного межсетевого взаимодействия в корпорации.

Контрольная работа №3

1. Перечислить основные причины возникновения уязвимостей в применяемом программном обеспечении.
2. Для чего создаются виртуальные частные сети и какие для этого используются типы программных средств.
3. Модель программно-аппаратной защиты рабочего места от разрушающих воздействий.

Примерные оценочные средства для контроля самостоятельной работы студентов.

1. Знание теоретических основ учебной дисциплины.

Студент демонстрирует глубокое знание теории, а также умение увидеть и показать междисциплинарные связи.

Студент хорошо владеет теорией вопроса по каждой дисциплине, видит их взаимосвязь и взаимообусловленность.

Студент, раскрывая проблемы, затрудняется с изложением теории, может раскрыть содержание лишь при наводящих вопросах.

Студент не понимает проблемы, механически повторяет некоторые положения теории, не видит взаимосвязи институтов изученной учебной дисциплины.

2. Умение применять теоретические знания при решении практических задач.

Студент свободно иллюстрирует теоретические положения уместными и обоснованными примерами из своей практики или из заимствованного опыта. Студент иллюстрирует ответ немногочисленными примерами и испытывает затруднения при их обосновании.

Студент может подкрепить теоретические положения примерами только после наводящих вопросов, допуская при этом ошибки.

Студент демонстрирует неумение применять теоретические знания для решения практических задач.

2. Владение профессиональной терминологией.

Студент демонстрирует свободное владение понятийным аппаратом учебной дисциплины.

Студент хорошо владеет профессиональной терминологией, в случае ошибки в употреблении термина способен сам исправить её.

Студент слабо владеет профессиональной терминологией, допускает неточности в интерпретации понятий.

Студент не владеет профессиональной терминологией.

3. Аргументация.

Студент использует различные операции логического вывода: анализ, синтез, обобщение, сравнение и др. Свободно владеет аргументацией.

Студент предъявляет достаточно стройный, лаконичный и четкий ответ, но допускает незначительные ошибки при аргументировании своей позиции.

Студент демонстрирует недостаточно аргументацию, нарушает логику изложения.Студент демонстрирует полное отсутствие аргументации, грубые ошибки логического вывода.

Типовые контрольные вопросы и задания для проведения промежуточной аттестации:

Примерные вопросы, выносимые на экзамен

1) Цели и задачи ПА обеспечения информационной безопасности (ИБ).
2) Место ПА защиты информации в системе комплексной защиты информации объектов автоматизации (ОА).
3) Предмет, цели, задачи, содержание курса, его роль и место в подготовке специалистов по ком¬плексной защите ин-формации.
4) Критерии оценки информационной безопасности ОА.
5) Типовые пути утечки информации и угрозы безопасности ОА.
6) Службы защиты информации: обеспечение, аутентичность субъектов информационного взаимодействия, управление доступом,
7) Службы защиты информации: обеспечение секретности, конфиденциальности и целостности информации.
8) Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
9) Основные этапы проектирования систем комплексной защиты информации.
10) Основные подходы к ПА защите данных от несанкционированного доступа (НСД).
11) Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам.
12) Идентификация, аутентификация, авторизация.
13) Аутентификация субъекта. Парольные схемы защиты.
14) Симметричные и несимметричные методы аутентификации субъекта.
15) Аутентификация объекта. Разграничение и контроль доступа к информации.
16) Защита сетевого файлового ресурса.
17) Фиксация доступа к файлам, доступ к данным со стороны процесса. Способы фиксации факта доступа.
18) Контроль и управление доступом средствами операционной системы (ОС).
19) Стойкость шифра.
20) Симметричные криптосистемы. Алгоритмы шифрования.
21) Асимметричные криптосистемы.
22) Система открытого распределения ключей Диффи–Хеллмана.
23) Криптосистема RSA.
24) Система шифрования ElGamal.
25) Криптосистемы на основе эллиптической кривой.
26) Защита файлов от изменения.
27) Цифровая (электронная) подпись.

28) Хэш-функции.
29) Эффективность реализации алгоритмов.
30) Эквивалентность прямого и обратного преобразований.
31) Характеристики стойкости алгоритмов.
32) Производительность и простота реализации.
33) Техническая реализация несимметричных криптосистем.
34) Реализация модулярных операций,
35) Реализация RSA криптосистем
36) Реализация криптосистем на основе эллиптических кривых.
37) Аппаратные компоненты криптозащиты данных.
38) Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.
39) Необходимые и достаточные функции ПА средств криптозащиты.
40) Специализированная компьютерная система безопасности.
41) Криптографический сопроцессор.
42) Стандарт FIPS PUB 140-2 и IBM 4758.
43) Аппаратура IBM 4758.
44) Программное обеспечение низкоуровневой начальной загрузки и диагностики.
45) Электронные ключи.
46) Ключ Touch Memory (iButton),
47) Однонаправленный интерфейс MicroLAN.
48) Радиочастотные идентификаторы (RFID).
49) Стандарты для RFID технологии,
50) элементы спецификации стандарта ISO 14443,
51) новые риски технологии RFID.
52) Смарт-карты.
53) Микропроцессорные смарт-карты.
54) Активация смарт карт.
55) Ответ на сброс (последовательность ATR).
56) Структура сообщения APDU.
57) Защищенная передача данных.
58) Физическая защита. Сценарии атаки, цели защиты, требования защиты, противодействие вмешательству.
59) Физический криптоанализ.
60) Модель противника, побочный канальный криптоанализ, канальный анализ на основе дефектов, некоторые виды физических канальных атак на RFID.
61) Защита во встроенных системах.
62) Информационно-технологическая защита.
63) Технологии встроенной защиты.
64) Элементы защиты флэшинга ПО.
65) Классы защиты встроенных электронных модулей.
66) Защита данных в мобильных беспроводных сетях.
67) Механизмы защиты WLAN на основе WEP.
68) IEEE 802.1X аутентификация.
69) Протокол TKIP.
70) Стандарт защиты IEEE 802.11i.
71) Взлом пароля точек доступа WiFi.
72) Дискреционный метод организации разграничения доступа.
73) Мандатный метод организации разграничения доступа.
74) Контроль целостности информации.
75) Имитозащита информации.
76) Криптографические методы контроля целостности.

77) Защищенные ОС.
78) Средства защиты ПО от несанкционированной загрузки.
79) ПА защита ПО от несанкционированного копирования, пароли и ключи.
80) Организация хранения ключей.
81) Защита ПО от излучения, отладки, дизассемблирования, трассировки по прерываниям.
82) Защита информации на машинных носителях, остатков информации.
83) Классификация способов НСД и жизненный цикл атак.
84) Способы противодействия несанкционированному межсетевому доступу.
85) Функции межсетевого экранирования.
86) Особенности межсетевого экранирования на различных уровнях модели OSI.
87) Режим функционирования межсетевых экранов и их основные компоненты.
88) Маршрутизаторы.
89) Шлюзы сетевого уровня.
90) Основы сетевого и межсетевого взаимодействия.
91) Схемы сетевой защиты на базе межсетевых экранов.
92) Применение межсетевых экранов для виртуальных корпоративных сетей.
93) Критерии оценки межсетевых экранов.
94) Построение защищенных виртуальных сетей.
95) Способы создания защищенных вир¬ту¬аль¬ных каналов.
96) Обзор протоколов.
97) Инфраструктура на основе криптографии с открытыми ключами (ИОК).
98) Цифровые сертификаты. Управление цифровыми сертификатами.
99) Компоненты ИОК и их функции.
100) Центр Сертификации.
101) Центр Регистрации.
102) Конечные пользователи.
103) Сетевой справочник.
104) Электронная почта и документооборот.
105) Web-приложения.
106) Стандарты в области ИОК.
107) Стандарты PKIX.
108) Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
109) Управление ключами.
110) Политика безопасности.
111) Шаблоны.
112) Сетевая политика безопасности.
113) Эшелонированная оборона.
114) Управление рисками. Понятия.
115) Процесс оценки рисков.
116) Уменьшение рисков.
117) Аудит информационной безо¬пас¬ности.
118) Определения, терминология.
119) Сценарий атаки.
120) Пассивная и активная разведка.
121) Выбор эксплойта.
122) Взлом целевой системы.
123) Загрузка кода.
124) Сокрытие следов взлома.
125) Примеры атак.
126) Классификация удалённых атак. Списки терминов, категорий, матричные схемы, процессы, онтология атак.

127) Фильтрация пакетов.
128) Межсетевые экраны уровня соединения,
129) Межсетевые экраны прикладного уровня,
130) Межсетевые экраны с динамической фильт¬рацией пакетов,
131) Межсетевые экраны инспекции состояний,
132) Межсетевые экраны уровня ядра.
133) Персональные и распределённые межсетевые экраны.
134) Обход межсетевых экранов. Постепенный подход. Туннелирование.
135) Требования и показатели защищённости.
136) Тестирование межсетевых экранов.
137) Модели систем обнаружения вторжений (CIDF, Деннинга).
138) Классификация систем обнаружения вторжений.
139) Обнаружение сигнатур, аномалий (методы Data Mining, технологии мобильных агентов, построения иммунных систем).
140) Генетические алгоритмы, нейронные сети.
141) Языки описания атак.
142) Методы обхода систем обнаружения вторжений.
143) Вспомогательные средства.
144) Тестирование систем обнаружения вторжений.
145) Системы предупреждения вторжений.
146) Туннелирование.
147) Протокол VPN канального уровня.
148) Протокол IPsec (обмена интернет – ключами, аутентификации заголовка, инкапсуляции содержимого пакета, IKE, совместное использование протоколов ESP и AH. Типы защищённых связей).
149) Протоколы VPN транспортного уровня.
150) Цифровые сертификаты.
151) Примеры отечественного построения VPN.
152) Компьютерные вирусы как класс разрушающих программных воздействий.
153) Необходимые и достаточные условия недопущения разрушающего воздействия.
154) Изолированная программная среда.
155) Направления и перспективы развития методов и средств ПА защиты информации и управления правами исполь-зования информационных ресурсов при передаче информации по каналам связи.
156) Современные системы ПА защиты информации на объектах информатизации.
157) Возможности современных ПА средств защиты.