

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 27.02.2025 15:40:33
Уникальный программный ключ:
ca953a0120d891083f939673078ef1a989dae18a

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)**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

(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)

1.1 К оценочным средствам текущего контроля успеваемости относятся:
- тестовые задания открытого и закрытого типов.

Промежуточная аттестация по дисциплине проводится в форме зачета, который выставляется по результатам прохождения всех видов текущего контроля успеваемости. При необходимости задания закрытого и открытого типов могут быть использованы для проведения промежуточной аттестации.

1.2 Критерии оценки результатов освоения дисциплины

2 Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено»,

3 «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

3.1 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 % правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ТЕСТОВЫЕ ЗАДАНИЯ ОТКРЫТОГО ТИПА:

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это_____

Ответ: «информационная война»

2. _____ в различных сферах деятельности - это подтверждение того, что заданные требования выполнены, через предоставление объективных свидетельств; оценка соответствия продукта, услуги или системы нормам, требованиям, спецификациям или установленным условиям;

Ответ: Верификация

3. _____ в технике или в системе менеджмента качества — доказательство того, что требования конкретного пользователя, продукта, услуги или системы удовлетворены

4. _____ - это информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

Ответ: Конфиденциальная информация

5. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это _____

Ответ: комплексное обеспечение информационной безопасности

6. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это _____

Ответ: пароль пользователя

7. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений называется

Ответ: целостностью

8. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми называется принципом

Ответ: разумной достаточности

9. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности называется

Ответ: политикой безопасности

10. _____ — это система объединенных компьютерных сетей и подключенных к ним промышленных объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека

Ответ: Промышленный Интернет вещей

11. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется _____

Ответ: сканером

12. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это _____

Ответ: Информационная безопасность

13. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы – это _____

Ответ: атака на автоматизированную систему

14. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ _____

Ответ: Государственная тайна

15. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов _____

Ответ: Безопасность АС

16. _____ совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

Ответ: Угроза

17. _____ блокирует нежелательный трафик

Ответ: Межсетевой экран

18. Аттестация _____ является обязательной для организаций, которые работают в ГИС, АСУ ТП, относятся к объектам КИИ, обрабатывают ПДн и государственную тайну

Ответ: ФСТЭК

19. Основные требования к содержанию системы защиты персональных данных, при автоматизированной обработке, определяют следующие документы:

Ответ: ФЗ 152; ППРФ 1119; Приказ ФСТЭК №21;

20. Пентест - _____

Ответ: Имитация целевых атак злоумышленников и выявление уязвимости инфраструктуры называется

21. ФСТЭК России. Методический документ. Методика оценки угроз безопасности информации (5 февраля 2021 г.) определяет:

Ответ: порядок разработки модели угроз

22. Средства защиты информации автоматизированной системы – _____

Ответ: совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

23. _____ набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных

Ответ: Компьютерная безопасность

24. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это _____

Ответ: Защита информации

Тестовые задания закрытого типа:

25. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано:

1. **Надёжность**

3. Контролируемость

2. Точность

4. Доступность

26. В классификацию вирусов по способу заражения входят

1. **Резидентные**

3. **Нерезидентные**

2. Файловые

4. Загрузочные

27. Основными компонентами парольной системы являются

1. **интерфейс администратора**

3. хранимая копия пароля

2. **база данных учетных записей**

4. все варианты верны

28. Информационная безопасность это:

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз

3. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**

2. Состояние, когда не угрожает опасность информационным системам

4. Политика национальной безопасности России

29. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:

Принцип гибкости системы:

- | | |
|--------------------------------------|-----------------------------------|
| 1. <i>Принцип непрерывной защиты</i> | 3. Принцип комплексности |
| 2. Принцип системности | 4. Принцип разумной достаточности |

30. К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики, сведения о семейном положении, сведения об имущественном или финансовом состоянии...»:

- | | |
|------------------------------------------------------------------------|----------------------------------------------|
| 1. Информация без ограничения права доступа | 3. Информация с ограниченным доступом |
| 2. Информация, распространение которой наносит вред интересам общества | 4. Объект интеллектуальной собственности |

1 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

В данном разделе по учебному плану типовые задания на контрольную работу, курсовую работу/курсовой проект, расчётно-графическую работу не предусмотрены.