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)

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(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. Виды контроля по периодам обучения

**Материалы для проведения контроля:**

1. Наименование оценочного средства (в соответствии с паспортом фонда оценочных средств) – **контрольная работа**
2. Перечень вопросов (заданий)

**Тематика контрольных работ:**

**1**. Политика использования компьютеров интранета в организации.
**2**. Политика использования паролей в организации.
**3**. Политика использования алгоритмов шифрования в организации.
**4**. Примеры угроз ИБ.
**5**. Примеры уязвимостей объектов ИБ.
**6**. Аспекты ИБ в управлении непрерывностью бизнеса.
**7**. Инструментальные средства управления рисками ИБ.
**8**. Основные документы процесса управления рисками ИБ операционного уровня.
**9**. Возможные критерии оценивания рисков ИБ и принятия рисков ИБ.
**10**. Политика антивирусной защиты в организации.
**11**. Политика удаленного доступа к интранету.
**12**. Политика работы с конфиденциальной информацией.
**13**. Политика для веб-сервера.
**14**. Политика отправки электронной почты за пределы интранета.
**15**. Политика для межсетевых экранов.
**16**. Политика подключения новых устройств к интранету.
**17**. Учет вопросов ИБ при работе с персоналом.
**18**. Управление логическим доступом к активам организации.
**19**. Управление защищенной передачей данных и операционной деятельностью.
**20**. Модели организационного управления ИБ.

**Материалы для проведения аттестации:**

1. Вид аттестации (**экзамен**)
2. Форма проведения (**устный опрос**)
3. Перечень тем, вопросов, практических заданий, выносимых на экзамен:

1. Эволюция определений информационной безопасности. Содержание терминов «безопасность информации», «защита информации» и «информационная безопасность».
2. Этапы обеспечения информационной безопасности организации.
3. Сущность системного подхода к исследованию объектов и управлению организацией.
4. Определение и содержание процессного подхода к анализу деятельности организации.
5. Основные свойства информации как предмета защиты. Характеристики секретной и конфиденциальной информации.
6. Понятие объекта угроз ИБ, целей и источников угроз защищаемой информации.
7. Основные составляющие процесса управления инцидентами ИБ в организации.

8. Основные преимущества использования циклической модели PDCA управления деятельностью организации.

9. Основные направления деятельности законодательных органов РФ относящиеся к вопросам ИБ.

10. Характеристика статей Уголовного кодекса непосредственно связанных с ИБ.

11. Понятие «Политика безопасности». Содержание списка решений верхнего уровня Политики безопасности.

12. Управления рисками. Уровень и процедура управления рисками.

13. Технические аспекты управления ИБ.

14. Каналы несанкционированного доступа к информации. Типичные причины их появления.

15. Основные категории технических каналов утечки информации.

16. Назначение и направления деятельности ФСТЭК России.

17. Понятия «идентификации» и «аутентификации». Причины, затрудняющие надежную идентификацию.

18. Направления деятельности органов стандартизации РФ применительно к решению задач управления ИБ.

19. Кадровые аспекты управления ИБ.

20. Роль и место аудита в системе сервисов безопасности организации.

21. Задачи и возможности современных средств биометрической «идентификации» и «аутентификации».

**Критерии и показатели оценки**

| **Критерии** | **Оценка** | | | |
|---|---|---|---|---|
| | **«отлично»** | **«хорошо»** | **«удовлетворительно»** | **«неудовлетворительно»** |
| 1.Знание теоретических основ дисциплины. | Студент демонстрирует глубокое знание теоретических основ и принципов, базовых понятий, которые используются при управлении информационной безопасностью. | Студент достаточно хорошо владеет знаниями теоретических основ и принципов, базовых понятий, которые используются при управлении информационной безопасностью. | Студент затрудняется с изложением теории, поверхностно ориентируется в базовых понятиях, которые используются при управлении информационной безопасностью. | Студент не понимает поставленной проблемы, не знает теоретических основ и принципов управления информационной безопасностью. |
| 2. Умение иллюстрировать теоретические знания на конкретных практических примерах. | Студент уверенно иллюстрирует теоретические положения обоснованными примерами. | Студент иллюстрирует ответ немногочисленными 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, допускает неточности в интерпретации понятий и определений в данной предметной области. | Студент не владеет профессиональной терминологией и не разбирается в понятийном аппарате дисциплины. |

**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».