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)

МЕТОДЫ ВЫЯВЛЕНИЯ И АНАЛИЗА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(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)

Паспорт оценочных средств.

Направление подготовки (специальность): 10.04.01 Информационная безопасность

Дисциплина: Методы выявления и анализа инцидентов информационной безопасности

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства
1	**Отечественные и зарубежные стандарты и документы**	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе. Экзамен
2	**Предлагаемый подход к осуществлению** организации и управления	
3	**Перечень событий, относящихся к ИБ**	
4	**Определение состава событий ИБ**	
5	Определение правил сбора и корреляции событий ИБ	
6	Критерии классификации событий ИБ	

Типовые контрольные вопросы и задания для проведения промежуточной аттестации:

Типовые контрольные вопросы

1. Международные и зарубежные стандарты
2. Российские стандарты
3. Перечень событий, относящихся к ИБ
4. **Критерии отнесения событий ИБ к инцидентам**
5. **Источники событий ИБ**
6. **Способы оповещений о событиях ИБ**
7. Пример состава событий информационной безопасности, рекомендуемых к использованию для анализа с целью выявления нарушений в обеспечении информационной безопасности.
8. Типы (классы) технических средств, являющихся источниками, формирующими события информационной безопасности.
9. Правила сбора событий информационной безопасности
10. Сводная таблица событий и правил корреляции и отражения признаков нарушений ИБ в отчётах систем мониторинга
11. Вероятности нахождения сведений о конкретных классах событий ИБ
12. Требования к критериям классификации
13. известные подходы к классификации событий ИБ
14. Критерии классификаций событий ИБ в качестве свидетельств нарушения безопасности
15. Принципы классификации
16. Критерии классификации

Типовые задания

1. Выбор метода классификации и его обоснование

2. Строение классификатора инцидентов ИБ
3. Обработка инцидентов ИБ
4. Анализ действий работников при обработке инцидентов
5. Системы менеджмента инцидентов ИБ
6. Определение функций группы реагирования на инциденты ИБ
7. Выбор технических средств необходимых для использования в процессе менеджмента инцидентов ИБ
8. Выделение необходимых ресурсов и создание организационной структуры менеджмента инцидентов ИБ, включая группу реагирования на инциденты информационной безопасности
9. Контроль за выполнением требований нормативных документов организации в ходе обработки инцидентов
10. Цели хранения данных о событиях информационной безопасности, которые классифицированы в качестве свидетельств нарушений информационной безопасности
11. Применяемые способы сбора и хранения данных о событиях информационной безопасности, которые классифицированы в качестве свидетельств нарушений информационной безопасности

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования результатов.

Оценивание знаний студентов по дисциплине «Автоматизация процессов управления инцидентами информационной безопасности» осуществляется в ходе текущего контроля успеваемости и промежуточной аттестации в соответствии с балльно-рейтинговой системой.

Оценка знаний студентов включает:

1. Оценку работы студента в течение семестра – до 60 баллов.
2. Оценка знаний студента на промежуточной аттестации – до 40 баллов.

Промежуточная аттестация предусмотрена в форме экзамена, который проводится в виде устного собеседования по контрольным вопросам. Предлагается два теоретических вопроса.

Важнейшими критериями оценки знаний и умений являются:

– степень усвоения учебной программы;

– содержание ответа на контрольные вопросы: логичность и доказательность изложения;

– степень творчества и самостоятельности в раскрытии поставленных вопросов.

Содержание текущего контроля успеваемости.

Выполнение мероприятий учебной работы	**Удельный вес в баллах**	**Количество мероприятий**	**Всего баллов**
Работа на лекциях	до 1,3	7	до 9,0
Работа на семинарских и практических занятиях	до 3,0	7	до 21,0
		Итого:	**до 30,0**

Оценка знаний на экзамене.

	Удельный вес одного вопроса в баллах	**Количество вопросов**	**Всего баллов**
Ответ на экзамене	до 10,0	2	до 20,0
		Итого:	**до 50,0**

Критерии оценивания ответов на вопросы экзамена.

Для получения 9-10 баллов за ответ на один вопрос студент должен:

1. Исчерпывающе владеть терминологическим аппаратом по теме, ее метаязыком; видеть системные связи объекта с общим контекстом дисциплины и смежными вопросами.

2. Иметь системное представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть методикой анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки ответа с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Для получения 6-8 баллов студент должен:

1. В достаточной мере владеть терминологическим аппаратом по теме; видеть системные связи объекта со смежными вопросами.

2. Иметь общее представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть основными принципами методики анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Менее 6 баллов выставляется студенту в том случае, если он:

1. Не владеет терминологическим аппаратом по теме.

2. Не имеет представлений об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Не владеет принципами анализа объекта.

4. Не умеет выстраивать связные научные формулировки.