МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Институт прикладной математики и компьютерных наук
Кафедра «Информационная безопасность»

Утверждено на заседании кафедры
«Информационная безопасность»
«21» января 2021г., протокол №5

Заведующий кафедрой ИБ
_____ А.А.Сычугов

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫЕ МАТЕРИАЛЫ) ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Организационное и правовое обеспечение информационной безопасности

основной профессиональной образовательной программы
высшего образования – программы специалитета
по специальности:
10.05.03 Информационная безопасность автоматизированных систем
с профилем:
Защищенные автоматизированные системы управления

Форма обучения: *очная*

Идентификационный номер образовательной программы: 100503-01-21

Тула 2021 год

ЛИСТ СОГЛАСОВАНИЯ
фонда оценочных средств (оценочных материалов)

Разработчик(и):

Баранова Е.М., доцент каф. ИБ, доцент, канд. техн. наук _____
(ФИО, должность, ученая степень, ученое звание) *(подпись)*

1. Описание фонда оценочных средств (оценочных материалов)

Фонд оценочных средств (оценочные материалы) включает в себя контрольные задания и (или) вопросы, которые могут быть предложены обучающемуся в рамках текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю). Указанные контрольные задания и (или) вопросы позволяют оценить достижение обучающимся планируемых результатов обучения по дисциплине (модулю), установленных в соответствующей рабочей программе дисциплины (модуля), а также сформированность компетенций, установленных в соответствующей общей характеристике основной профессиональной образовательной программы.

Полные наименования компетенций представлены в общей характеристике основной профессиональной образовательной программы.

2. Оценочные средства (оценочные материалы) для проведения текущего контроля успеваемости обучающихся по дисциплине (модулю)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ОПК-6

1. Система защиты информации должна быть рассмотрена как состоящая из следующих подсистем:

а) подсистемы управления доступом
б) подсистемы, анализирующей угрозы и уязвимости
в) подсистемы регистрации и учета
г) криптографической подсистемы
д) подсистемы обеспечения целостности

2. Какие документы потребуются для защиты конфиденциальной информации?

а) ФЗ №152 «О персональных данных»
б) ФЗ №187 «Критическая информационная инфраструктура…»
в) РД «Классы защищенности АС…»
г) ФЗ № 98 «О коммерческой тайне…»
д) Методика построения модели угроз ФСТЭК

3. Перечислите угрозы, непосредственным источником которых являются штатные программно-аппаратные средства информационной системы:

а) неквалифицированное использование или ошибочный ввод параметров программ
б) аварийное завершение системных процессов
в) инициализация баз данных
г) отказы и сбои в работе операционной системы, СУБД и прикладных программ
д) форматирование или реструктуризацию носителей информации, удаление данных

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ОПК-8.2

1. Укажите документы, на базе которых осуществляется защита информации, обрабатываемая в Информационных системах персональных данных.
2. Укажите возможные категории персональных данных.
3. Укажите возможные категории нарушителей режима эксплуатации информационной системы персональных данных.
4. Представьте определение типовой модели угроз информационной системы персональных данных.

5. Каким образом определяется перечень возможных угроз, характерных для информационной системы персональных данных?

3. Оценочные средства (оценочные материалы) для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ОПК-6

1. Укажите угрозы, непосредственным источником которых является среда, в которой эксплуатируется информационная система на основе базы данных

а) деструктивные функции программного обеспечения, функционирующего параллельно с эксплуатируемой информационной системой

б) внезапное и длительное отключение систем электропитания

в) природные катастрофы

г) техногенные катастрофы

д) всплески природных электромагнитных излучений

2. К угрозам нарушения информационной безопасности данных, отображаемой на терминале пользователя или принтере следует отнести:

а) изменение информации в оперативной памяти, используемой СУБД для кэширования данных

б) изменение информации в оперативной памяти, используемой операционной системой для кэширования данных

в) ложная сессия

г) изменение информации в оперативной памяти, используемой прикладными программами в процессе организации и выполнения сессии взаимодействия с сервером баз данных и прослушивающим процессом

д) изменение элементов данных, выводимых на терминал или принтер пользователя за счет перехвата потока

3. Угрозы, вызванные воздействием на систему баз данных и ее компоненты объективных физических процессов или стихийно развивающихся природных явлений – это…

а) наиболее вероятностные угрозы

б) неидентифицируемые угрозы

в) искусственные угрозы

г) случайные угрозы

д) естественные угрозы

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ОПК-8.2

1. Что такое политика безопасности организации? Как она проектируется?

2. Какие автоматизированные системы помогут реализовать модели угроз и нарушителей?

3. Какие функции выполняют программы ГРИФ и КОНДОР?

4. Укажите, какие компании на российском рынке выпускают сертифицированное программное обеспечение для защиты информации?

5. Что позволяет реализовать технология SecretNet?

4. Оценочные средства (оценочные материалы) для проведения промежуточной аттестации обучающихся (защиты курсовой работы (проекта)) по дисциплине (модулю)

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.