

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:

Директор института прикладной
математики и компьютерных наук

А. В. Замятин

« 16 » Июня 20 23 г.

Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине
(Оценочные средства по дисциплине)

Социальная инженерия

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:

Анализ безопасности компьютерных систем

ОМ составил(и):
канд. техн. наук,
доцент кафедры компьютерной безопасности



В.А. Беляев

Рецензент:
д-р техн. наук, профессор,
профессор кафедры прикладной математики



В.И. Смагин

Оценочные средства одобрены на заседании учебно-методической комиссии
института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 08 июня 2023 г. № 02

Председатель УМК ИПМКН,
д-р техн. наук, профессор



С.П. Сущенко

Оценочные средства (ОС) являются элементом оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ОС разрабатываются в соответствии с рабочей программой (РП).

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

| Компетенция | Индикатор компетенции | Код и наименование результатов обучения (планируемые результаты обучения, характеризующие этапы формирования компетенций) | Критерии оценивания результатов обучения | |
|---|---|---|--|--|
| | | | Зачтено | Не зачтено |
| ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации | ИОПК-5.1 Обладает необходимыми знаниями нормативно-правовой базы, регламентирующей деятельность по защите информации. | ОР-5.1 Знать основные понятия в области информационной безопасности, математические основы методов анализа рисков; основные подходы к организации защиты от человеческого фактора, законодательство в области информационной безопасности. Уметь выявлять источники, риски и угрозы информационной безопасности, разрабатывать политику компании в соответствии со стандартами безопасности, использовать математические модели, алгоритмы для моделирования опасных ситуаций и анализа рисков. Владеть основами защиты интересов личности, общества и государства от возможных | Знает основные понятия в области информационной безопасности, математические основы методов анализа рисков; основные подходы к организации защиты от человеческого фактора, законодательство в области информационной безопасности. Умеет выявлять источники, риски и угрозы информационной безопасности, разрабатывать политику компании в соответствии со стандартами безопасности, использовать математические модели, алгоритмы для моделирования опасных ситуаций и анализа рисков. | Не знает основные понятия в области информационной безопасности, математические основы методов анализа рисков; основные подходы к организации защиты от человеческого фактора, законодательство в области информационной безопасности. Не умеет выявлять источники, риски и угрозы информационной безопасности, разрабатывать политику компании в соответствии со стандартами безопасности, использовать математические модели, алгоритмы для моделирования опасных ситуаций и анализа рисков. |

| | | | | |
|---|---|--|---|---|
| | | информационных атак, применением основных мер по ликвидации их последствий, способностью к общей оценке состояния информационной безопасности. | | |
| ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | ИОПК-6.1 Понимает нормативные правовые акты и нормативные методические документе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. | ОР-6.1 Знать основные понятия в области прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним. Уметь выявлять источники социальных проблем на производстве или в сфере взаимодействия с общественностью, применять инженерный подход в своей исследовательской и практической деятельности. Владеть основами исследования критических (экстремальных) ситуаций, применением экспериментов, теории игр, теории информации, тестирования с применением тренажёров и т. д. | Знает основные понятия в области прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним. Умеет выявлять источники социальных проблем на производстве или в сфере взаимодействия с общественностью, применять инженерный подход в своей исследовательской и практической деятельности. Владеет основами исследования критических (экстремальных) ситуаций, применением экспериментов, теории игр, теории информации, тестирования с применением тренажёров и т. д. | Знает основные понятия в области прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним. Не владеет основами исследования критических (экстремальных) ситуаций, применением экспериментов, теории игр, теории информации, тестирования с применением тренажёров и т. д. |
| ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в | ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием | ОР-16.1 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях | Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях | Не способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях |

| | | | | |
|---|---|---|---|--|
| компьютерных системах и сетях | штатных средств и методик. | | | |
| ОПК-18. Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы | ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности. | ОР-18.1 Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы | Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы | Не способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы |

2. Этапы формирования компетенций и виды оценочных средств

| № | Этапы формирования компетенций (разделы дисциплины) | Код и наименование результатов обучения | Вид оценочного средства (тесты, задания, кейсы, вопросы и др.) |
|----|--|---|--|
| 1. | Социальная инженерия (СИ) как наука. | ОР-5.1, ОР-6.1 | Вопросы теста, задания |
| 2. | Основные направления социальной инженерной деятельности. | ОР-5.1, ОР-6.1 | Вопросы теста, задания |
| 3. | Технологии защиты от социальных «хакеров». | ОР-5.1, ОР-6.1 | Вопросы теста, задания |
| 4. | Принципы оценки эффективности средств защиты. | ОР-5.1, ОР-6.1, ОР-16.1, 8.1, ОР-18.1 | Вопросы теста, задания |

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине (тесты, задания, задачи).

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине (вопросы к зачету, содержащие комплект контрольных вопросов и заданий для зачета).

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль по дисциплине проводится путём контроля посещаемости, проведения тестов по лекционному материалу и фиксируется в форме контрольной точки не менее одного раза в семестр.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Изучение курса завершается сдачей зачёта. Зачёт ставится при положительных результатах текущего контроля, положительных ответах на вопросы билета и сдаче реферата и доклада по одной из предложенных преподавателем тем. Методические материалы и требования к реферату включают критерии оценивания теоретических вопросов; процедуру формирования итоговой оценки, учитывающую оценки за каждую компетенцию.

Процедура формирования итоговой оценки включает степень самостоятельности студента при знакомстве с теоретической базой фундаментальных знаний по отдельным разделам социальной инженерии (по предложенной теме), полноту раскрытия темы, уровень обобщения собранного материала и отношение автора реферата к рассматриваемой проблеме и путям её решения.