

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.06
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии и методы социальной инженерии

(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: 4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	6	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	48,25	48,25
Самостоятельная работа	95,75	95,75
Контроль	-	-
Итого	144	144

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Целями освоения дисциплины «Технологии и методы социальной инженерии» являются овладение методами системного анализа процессов, тактик и техник нарушителей, с целью их выявления, последующей нейтрализации, основами нейролингвистического программирования, а также овладение навыками работы с пользователями информационных систем в области повышения осведомленности с методами работы социальных инженеров.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Основы управления информационной безопасностью;
- Комплексная безопасность.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

- Мониторинг событий информационной безопасности.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-9 Способен формулировать политики информационной безопасности	ПК-9.1 Использует принципы построения и развития социальной инженерии, основы теории системного подхода при решении задач защиты информации	Знать: - принципы построения и развития социальной инженерии, основы теории системного подхода при решении задач защиты информации; -основные особенности, принципы и методы социальной инженерии, показатели и критерии эффективности применения методов;
		Уметь: - находить и использовать информацию, необходимую для ориентирования в текущих задачах информационной безопасности
		Владеть: - основами социальной инженерии
	ПК-9.2 Умеет провести оценку проблемной ситуации в сфере социальной инженерии, выявить основные закономерности и тенденции применения форм и методов нарушителями	Знать: - основные тенденции совершенствования социальной инженерии
		Уметь: - провести оценку проблемной ситуации в сфере социальной инженерии
		Владеть: - методами работы нарушителей с целью их выявления и нейтрализации
	ПК-9.3 Владеет основами соц инженерии, методами работы нарушителей с целью их	Знать: - методы нарушителей по воздействию на объекты внимания.

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	выявления и нейтрализации	- техники СИ, виды атак
		Уметь: - установить и настроить DLP систему
		Владеть: - навыками применения DLP

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Сущность социальной инженерии 1.Понятие "социальная инженерия". 2.Цели, функции и структура социальной инженерии. 3.Методологические основы социальной инженерии 4.Методы и процедуры социальной инженерии 5.Атаки на пользователей. 6.Технологии, психология и меры противодействия 7. Нейролинвистическое программирование 8. Social Engineering и гуманитарная составляющая	5	6		-	
Модуль 1	Пр	Тема 1 Сущность социальной инженерии Разработать 5 техник манипулирования людьми	6	4			Отчет по практическому занятию №1
Модуль 1	Ср	Тема 1 Сущность социальной инженерии	6	17			
Модуль 1	Лек	Тема 2 Психотипы целей и как их распознать 1.Эпилептоид 2.Эмотив 3.Истероид 4.Шизоид	6	2			
Модуль 1	Пр	Тема 2 Психотипы целей и как их	6	4			Отчет по практическому занятию №2

		распознать Определение психотипа по постам в соцсетях					
Модуль 1	Ср	Тема 2 Психотипы целей и как их распознать	6	17			
Модуль 1	Лек	Тема 3 Техники социальной инженерии 1. Претекстинг 2. Фишинг 3. Троянский конь 4. Дорожное яблоко 5. Кви про кво 6. Обратная социальная инженерия 7. Ловля «на живца» 8. Искусство обмана	6	2		-	
Модуль 1	Пр	Тема 3 Техники социальной инженерии Определение технологических векторов цифровых атак на сотрудников	6	2			Отчет по практическому занятию №3
Модуль 1	Пр	Тема 3 Техники социальной инженерии Организация и проведение фишинговой атаки Использование GoFish для учений по фишингу	6	4			Отчет по практическому занятию №4
Модуль 1	Ср	Тема 3 Техники социальной инженерии	6	17			
Модуль 1	Лек	Тема 4 DLP и профайлинг 1. Невербальные коммуникации 2. Обзор решений противодействия утечкам информации 3. Типовая архитектура построения системы DLP 4. Особенности организационной работы при эксплуатации DLP 5. Обучение системы принципам	6	2			

		классификации информации 6.Ввод правил реагирования 7.Выполнение системой DLP операций контроля 8.Обработка инцидентов 9.Преимущества и ограничения DLP систем 10. Профайлинг					
Модуль 1	Пр	Тема 4 DLP и профайлинг Разработка плана противодействия утечкам информации	6	2			Отчет по практическому занятию №5
Модуль 1	Пр	Тема 4 DLP и профайлинг Установка и настройка DLP	6	4			Отчет по практическому занятию №,6
Модуль 1	Ср	Тема 4 DLP и профайлинг	6	17			
Модуль 1	Лек	Тема 5 Модель антифишинга 1. Технологические векторы цифровых атак на сотрудников 2. Психологические векторы атаки 3. Источники атаки 4. Персонификация атаки 5.Формат описания имитированной атаки 6. Классификация цифровых атак на сотрудников	6	2			
Модуль 1	Пр	Тема 5 Модель антифишинга Разработка сценария персональной атаки Претекстинг и легендирование. Вишинг. Кейс Безответственный админ	6	4			Отчет по практическому занятию №7
Модуль 1	Ср	Тема 5 Модель антифишинга	6	16			
Модуль 1	Лек	Тема 6 Социальная инженерия на практике 1. Физическая безопасность и социальная инженерия 2. Экономическая безопасность и социальная инженерия 3 Информационная безопасность и социальная инженерия	6	2		-	

		4. Договорные и юридические аспекты СИ 5.OSIN, Prntest и социальная инженерия 6. Меры противодействия социальной инженерии					
Модуль 1	Пр	Тема 6 Социальная инженерия на практике Кликджекинг. Кейс Ненадежный форум Спирфишинг Кейс Торговцы оружием	6	4			Отчет по практическому занятию №8
Модуль 1	Пр	Тема 6 Социальная инженерия на практике OSINT+ Pentest + SE. Кейс Массовая рассылка файлов Сетевое сканирование. Кейс тысячи продавцов	6	4			Отчет по практическому занятию №9
Модуль 1	Ср	Тема 6 Социальная инженерия на практике Претекстинг и легендирование. Вишинг. Кейс Безответственный админ	6	15,75			
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно))	5	0,25		-	Банк тестовых заданий /Вопросы к зачету
Итого:				144			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
Формы и методы обучения		
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-9	Протоколы практических заданий №1-9
		Вопросы к зачету №№1-45
		Темы для реферата
		Банк тестовых заданий №1-350

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1 Реферат «Профайлинг и методики выявления обмана»

Реферат «Искусство обмана»

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Разработать 5 техник манипулирования людьми
2	Определение психотипа по постам в соцсетях
3	Определение технологических векторов цифровых атак на сотрудников
4	Организация и проведение фишинговой атаки Использование GoFish для учений по фишингу
6	Установка и настройка DLP
7	Разработка сценария персональной атаки Претекстинг и легендирование. Вишинг. Кейс Безответственный админ
8	Кликджекинг. Кейс Ненадежный форум Спирфишинг Кейс Торговцы оружием
9	OSINT+ Pentest + SE. Кейс Массовая рассылка файлов Сетевое сканирование. Кейс тысячи продавцов

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты определяют психотип человека по анализу поведения в соцсетях, используют знания на фишинговых учениях, развертывают и настраивают DLP системы, прописывают политики их использования, развертывают приложения для имитации фишинговых атак, пишут сценарии их применения.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.

2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.4 Типовой пример тестового задания

Сущность социотипа Эмотив:

Выберите один или несколько вариантов ответа:

- 1) яркие эмоции
- 2) сопереживания
- 3) драматизация ситуации
- 4) впечатлительность
- 5) нерешительность

Критерии оценки:

Минимальное количество баллов 1. Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 5

№ п/п	Вопросы к зачету
1.	Сущность понятия "социальная инженерия"
2.	Цели, функции и структура социальной инженерии
3.	Каковы методологические основы социальной инженерии
4.	Виды атак на пользователей
5.	Привести пример технологии СИ
6.	Сущность нейролинвистического программирования
7.	Social Engineering и гуманитарная составляющая на примерах
8.	Примеры мер противодействия социальным инженерам
9.	Привести примеры телефонного мошенничества
10.	Привести примеры психологического воздействия на пользователя
11.	Виды технологических атак, описание каждой
12.	Как провести атаку через соцсети
13.	Как провести атаку через эл.почту

14.	Как провести атаку через мессенжеры
15.	Как провести атаку через мобильные устройства
16.	Как провести атаку в офисе
17.	Привести примеры и описать психологические векторы атак
18.	Источники атак. Описать каждый
19.	Суть персональной атаки, как проводится
20.	Описать формат имитированной атаки
21.	Анализ контроля доступа и внутренних правил
22.	Экспертная оценка нормативных и методических документов
23.	Приемы симуляции действий злоумышленника в конкурентной разведке
24.	Мероприятия по проверке возможности доступа к информации на рабочих местах
25.	Каковы юридические аспекты СИ
26.	Каковы психологические аспекты СИ
27.	Описать связку OSINT+ Pentest + SE
28.	Описать технику Претекстинг
29.	Описать технику Фишинг
30.	Описать технику Троянский конь
31.	Описать технику Дорожное яблоко
32.	Описать технику Кви про кво
33.	Описать технику Ловля «на живца»
34.	Привести примеры решений противодействия утечкам информации
35.	Типовая архитектура построения системы DLP. Обзор решений. Сравнение
36.	Юридические аспекты применения DLP
37.	Применение DLP для контроля рабочего времени
38.	Применение DLP для предотвращения утечек информации
39.	Назначение и ввод правил реагирования
40.	Суть профайлинга
41.	Описать сущность социотипа Эпилептоид
42.	Описать сущность социотипа Эмотив
43.	Описать сущность социотипа Истероид
44.	Описать сущность социотипа Шизоид
45.	Применение знаний о социотипов в соц.инженерии

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
		«зачтено»	55-100 баллов
6	Зачет (письменно/по накопительному рейтингу)	«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Попел А. Е.	Социальная инженерия: теория и практика	Уч пособие	2022	

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	В.В. Зотов	Социальная инженерия. Теория и практика	Хрестоматия	2019	
2	К. Д. Митник	Искусство обмана		2018	
3	Фомина Н.А.	Использование методов социальной инженерии при мошенничестве в социальных сетях	Учебное пособие	2019	

8.3. Перечень профессиональных баз данных и информационных справочных систем

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы	Столы-парты

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	обучающихся Д -409	двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф