МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

_____ 202_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Введение в специальность»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ А.Г. Остапенко

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Цель изучения дисциплины «Введение в специальность» – формирования целостной картины проблематики инфобезопасности, включая привитие будущим специалистам базовых знаний и умений в области анализа защищенности (уязвимостей) и обеспечения безопасности автоматизированных информационных систем и сетей.

1.2. Задачи освоения дисциплины

1. Освоение научно-методических основ кибер-безопасности, вовлечение будущих специалистов в проблематику сетевых войн и защиты современного (мультисетевого) пространства социотехнических систем.

2. Адекватное восприятие студентами сущности и важности проблемы обеспечения информационной безопасности личности, общества и государства через изучение основ и эффектов коммуникативного воздействия на психику индивида и социальной группы, включая привитие информационного иммунитета и снижение рисков вербовки студенческой молодежи в деструктивные культы и террористические организации.

3. Через ознакомление с цифровыми технологиями и методами социальной инженерии демонстрация преимуществ национальных демократических, культурных и духовно-нравственных ценностей и традиций и тем самым - снижение рисков участия студенческой молодежи в операциях кибер-преступных группировок и спровоцированных злоумышленниками противоправных акциях протеста (цветных революциях).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Введение в специальность» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б.1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Введение в специальность» направлен на формирование следующих компетенций:

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.2 Способен участвовать в работах по моделированию защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации	знать принципы построения компьютерных систем и сетей, модели безопасности компьютерных систем, виды политик безопасности компьютерных систем и сетей
	знать национальные, межгосударственные и международные стандарты в области защиты информации
	уметь анализировать возможные уязвимости информационных систем
	уметь определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети
	уметь выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации
	уметь оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите
	владеть навыками формализации предложений по устранению выявленных уязвимостей компьютерных сетей
ПК-7.3 Способен принимать участие в разработке предварительных проектных решений по защите информации в автоматизированых системах	знать нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
	знать основные методы управления проектами в области информационной безопасности
	знать уязвимости информационных систем
	знать методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее
	уметь проводить анализ угроз безопасности информации и разрабатывать модели угроз безопасности информации
	владеть навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Введение в специальность» составляет 5 зачетных единиц.

Распределение трудоемкости дисциплины по видам занятий

Очная форма обучения

Вид учебной работы	Всего часов	Семестры	
		1	2
Аудиторные занятия (всего)	108	36	72
В том числе:			
Лекции	108	36	72
Практические занятия (ПЗ)	0	0	0
Лабораторные работы (ЛР)	0	0	0
Самостоятельная работа	72	36	36
Курсовой проект(работа) (есть, нет)		нет	есть
Контрольная работа (есть, нет)		нет	нет
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)		зачет	зачет с оценкой
Общая трудоемкость час	180	72	108
зач. ед.	5	2	3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Учебный стандарт и план специальности в условиях цифровой трансформации и сетевой организации пространства	Значение автоматизированных систем для обеспечения информационной безопасности личности, общества и государства. Основные определения.	4	0	0	0	4
2	Проблема обеспечения безопасности автоматизированной информационной системы и сети	Цифровая трансформация и структура современной корпорации, модель корпоративной автоматизированной информационной системы, сети (АИС), оценка стоимости информационных ресурсов (ПКО). Модель угроз. Формирование требований к системе обеспечения информационной безопасности в автоматизированных системах корпорации. Организационно-технические мероприятия по защите информации при ее обработке, хранении и передаче в АИС.	16	0	0	0	16
3	Модели атакуемых автоматизированных сетей	Традиционная формализация описания сетей, взвешенные сети: матрицы и метрики, конфликтология взвешенных сетей, стратегические цели и тактические приемы сетевого противоборства, особенности сетевого терроризма.	10	0	0	0	10
	Эпидемические	Формализация описания сетевых структур и	6	0	0	0	6

4	модели автоматизированных сетей	процессов, компьютерные вирусы и эпидемии в информационно-телекоммуникационных сетях, вирусный контент и эпидемии в социальных сетях.					
5	Информационная безопасность и социальная инженерия в автоматизированных сетях	Основы информационно-психологического воздействия и управления социумом, контент как инструмент психологического воздействия и управления в информационном обществе, социальные сети как пространство распространения контентов влияния, информационно-психологические метрики контентов и интернет-ресурсов, управление информационно-психологическими рисками в целях обеспечения безопасности личности и социума.	20	0	0	0	20
6	Автоматизированные сети и деструктивный контент	Социальные сети как среда распространения контента, информационное обеспечение для описания процессов распространения контента в социальных сетях, методическое обеспечение для описания процессов распространения контента в социальных сетях, оценка и регулирование рисков распространения деструктивных контентов в социальных сетях.	16	0	0	0	16
7	Мониторинг безопасности автоматизированных сетей	Мониторинг и управление рисками социо-информационного пространства в целях обеспечения региональной и национальной безопасности, инструментальные и методические особенности контент-мониторинга социальных сетей, выявление деструктивных контентов в социальных сетях, риск-метрология для контент-мониторинга, мониторинг регионального интернет-пространства в контексте обеспечения социальной безопасности.	20	0	0	0	20
8	Перспективы цифровой трансформации и обеспечения безопасности автоматизированных сетей и систем на основе средств искусственного интеллекта	Базовые понятия информационной безопасности, методы защиты информации. Роль ИИ в кибербезопасности, оценка алгоритмов машинного обучения Обнаружение аномалий и атак в сетевом трафике. Применение МО для обнаружения сетевых атак и аномалий, межсетевые экраны и системы обнаружения вторжений Идентификация. Биометрия. Основы биометрии, виды аутентификации и задача отбора признаков. Состязательные атаки на биометрические системы	4	0	0	0	4
9	Картографирование защищаемого кибер-сетевого пространства	Киберпространство как объект защиты и картографического исследования. Концептуальные основы картографии защищаемого киберпространства Информационная карта как основа картографирования защищаемого киберпространства. Вербальная модель процесса информационно-картографического исследования. Инструментальные основы картографии защищаемого киберпрострастваа. Реализация методологии картографирования защищаемого киберпространства в условиях информационного противоборства	4	0	0	0	4
10	Особенности обеспечения безопасности интернета вещей	Анализ безопасности технологий интернета вещей. Классификация угроз IoT. Примеры угроз для устройств интернета вещей в различных сферах	4	0	0	0	4
11	Результаты и перспективы реализации проекта «Безопасный интернет»		4	0	0	0	4
12	Риск-мониторинг Интернет-ресурса		0	0	0	72	72
		Итого	**108**			**72**	**180**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы во 2 семестре.

Примерная тематика курсовой работы: «Риск-мониторинг интернет-ресурса»

Задачи, решаемые при выполнении курсового проекта:

- парсинг заданного ресурса на предмет выявления деструктивов, их классификация;
- измерение параметров деструктивов и формирование базы их данных;
- оценка рисков и выработка рекомендаций по противодействию деструктивам.

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

Учебным планом по дисциплине не предусмотрено выполнение контрольных работ.

Курсовая работа реализуется в рамках проекта «Безопасный интернет» (рег. № АААА-А18-118050700061-7)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-7.2	знать принципы построения компьютерных систем и сетей, модели безопасности компьютерных систем, виды политик безопасности компьютерных систем и сетей	знание принципов построения компьютерных систем и сетей, модели безопасности компьютерных систем, виды политик безопасности компьютерных систем и сетей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знать национальные, межгосударственные и международные стандарты в области защиты информации	знание национальных, межгосударственных и международных стандартов в области защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать возможные уязвимости информационных систем	умение анализировать возможные уязвимости информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети	умение определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации	умение выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите	умение оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками формализации предложений по	владение навыками формализации предложений по	Выполнение работ в срок, предусмотренный	Невыполнение работ в срок, предусмотренный

	устранению выявленных уязвимостей компьютерных сетей	устранению выявленных уязвимостей компьютерных сетей	в рабочих программах	в рабочих программах
ПК-7.3	знать нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	знание нормативных правовых актов, методических документов, национальных стандартов в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знать основные методы управления проектами в области информационной безопасности	знание основных методов управления проектами в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знать уязвимости информационных систем	знание уязвимостей информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знать методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее	знание методов и технологий защиты информации от несанкционированного доступа и специальных программных воздействий на нее	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь проводить анализ угроз безопасности информации и разрабатывать модели угроз безопасности информации	умение проводить анализ угроз безопасности информации и разрабатывать модели угроз безопасности информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач	владение навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются во 2 семестре:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ПК-7.2	Определяет основные угрозы безопасности информации и формализует модели нарушителя в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Разрабатывает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
ПК–7.3	Осуществляет сбор и систематизация (анализ и оценка) сведений об угрозах НСД к сетям электросвязи	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Реализует проведение анализа структурных и функциональных схем, защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Участвует в разработке программно-аппаратных средств защиты информации в компьютерных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень вопросов для подготовки к зачету

1. Как с помощью графов определить автоматизированную информационную сеть(АИС)?
2. Дайте определение цикла и цепи АИС.
3. Определите контур и путь АИС.
4. Как задаётся матрица инциденции АИС.
5. Определите звёздную матрицу АИС.
6. Как задаётся матрица смежности АИС?
7. Что такое наполнитель АИС?
8. Как формируется матрица взвешенности АИС?
9. Каковы матрицы усреднённой и экстремальной взвешенности АИС?
10. Дайте определение статического и динамического ресурса АИС.
11. Как найти статический и динамический потенциал в АИС?
12. Что такое диаметр АИС?
13. Как определяется сетевая плотность?
14. Каковы шаги моделирования атакуемых взвешенных АИС
15. Какова процедура репрезентативной выборки из АИС?
16. Определите особенности моделирования диффузии контента в АИС.
17. Определите понятие сетевой конфликт.
18. Определите особенности дискретных моделей многослойного риск-анализа.
19. Как определяется эпистойкость АИС?
20. Перечислите основные разновидности моделей инфицирования.
21. Классифицируйте АИС по их назначению.
22. Как оцениваются веса рёбер и вершин АИС различного типа?
23. Классифицируйте разновидности наполнителей в соответствии с типами их АИС.
24. Перечислите метрика центрированности вершин АИС.
25. Каковы метрики групп и смешивания вершин АИС?
26. Классифицируйте АИС по их топологии.
27. Дайте классификацию для специализированных АИС.
28. Как оценить степень взвешенной центральности АИС и степень центральности всей АИС?
29. Как рассчитать плотность взвешенной центральности и центральности как посредничества?
30. Какова оценка взвешенной эквивалентности вершин АИС?
31. Классифицируйте стадии конфликта.
32. Как оценивается глубина конфликта?
33. Классифицируйте разновидности сетевого конфликта.
34. Классифицируйте этапы развития сетевого конфликта.
35. Какова классификация стратегий сетевого противоборства?
36. Классифицируйте тактические приёмы сетевого противоборства.
37. Какова классификация сценариев террористических атак?
38. Какова классификация вредоносных кодов вирусного характера?
39. Какова классификация антивирусного программного обеспечения?
40. Классифицируйте многообразие компьютерных червей.

41. Что обычно подразумевается под социальной системой?
42. Какова совокупность признаков социальной системы?
43. Дайте определение процессу внушения.
44. Определите понятие имидж.
45. В чём состоит сущность понятия пропагандистский миф?
46. Определите понятие стереотип.
47. Дайте определение понятию конформизм.
48. Определите понятие блеф
49. Дайте определение процессу информационного управления.
50. Определите понятие пропаганда.
51. Определите сущность человеческой коммуникации.
52. Дайте определение понятию контент.
53. Определите триаду: генератор, сообщение, получатель информации.
54. Как следует формировать контент?
55. В чём состоит «визуальный поворот» в восприятии информации?
56. Перечислите опасности при массовой информационно-психологической зависимости от социальных сетей.
57. Определите специфику фейковых новостей.
58. Дайте определение объекта информационно-психологического противоборства.
59. Определите понятие «виртуальные коалиции».
60. Определите особенность онлайн-сообществ.
61. Определите понятие контентные войны.
62. В чём сущность дифференциальных и интегральных метрик контента.
63. Определите понятие «деструктивный контент».
64. Дайте определение понятиям «лайк» и «дизлайк».
65. Что такое репост?
66. Определите понятие комментарий.
67. Что такое мониторинг контента.
68. Определите время жизни контента.
69. Как определяются периоды спада и роста популярности контента?
70. Определите понятия социальной сети и её пользователя
71. Классифицируйте виды внушения
72. Дайте классификацию эффектам информационно-психологического воздействия.
73. Классифицируйте средства информационно-психологического воздействия.
74. Дайте классификацию способам информационно-управляющего воздействия.
75. Классифицируйте приёмы организации лжи и обмана.
76. Дайте классификацию приёмов манипулирования информацией.
77. Классифицируйте способы информационно-психологического воздействия.
78. Дайте классификацию закономерностей манипулятивного информационно-психологического воздействия на массовое сознание
79. Классифицируйте мероприятия по нейтрализации деструктивного информационно-психологического воздействия.
80. Дайте классификацию средств информационно-психологического противодействия.
81. Как классифицируют контент по степени его уникальности?
82. Классифицируйте контенты с точки зрения их применения

83. Дайте классификацию коммуникативным ситуациям, оказывающим информационно-психологическое воздействие на человека.
84. Классифицируйте способы донесения информации в интернет пространстве.
85. Дайте классификацию типов восприятия человеком информации.
86. Классифицируйте ресурсы в формате 2.0.
87. Дайте классификацию психологических ресурсов.
88. Классифицируйте субъекты информационно-психологического противоборства.
89. Дайте классификацию основных форм организации общения с помощью Web-технологий.
90. Классифицируйте угрозы формирования у подростков, вовлечённых ы деструктивные течения, устойчивых поведенческих паттернов разрушительного типа.
91. Как оценить созвучность, тиражируемость, комментируемость и привлекательность контента?
92. Как измерить заметность и востребованность контента?
93. Как измеряется удельная мощность ареалов высокой, средней и низкой вовлеченности пользователей ресурса в содержание контента.
94. В чём состоит оценка рисков невертуальных деструктивных действий представителей ареалов низкой, средней и высокой вовлеченности.
95. Каковы дифференциальные метрики первичной реакции пользователей на контент.
96. Как измеряются дифференциальные метрики вторичной реакции пользователей на контент.
97. Как осуществить пошаговое сравнение параметров реакций пользователей на антагонистические контенты.
98. Как осуществить векторную оценку ресурсов на основе среднесуточных показателей реакции их пользователей?
99. Как и для чего следует осуществлять риск-ранжирование ресурсов?
100. Как осуществляется тематическая классификация контентов?
101. Дайте определение социальной системе и её информационно-психологическим признакам.
102. Каково позиционирование индивида в социуме?
103. Охарактеризуйте виды социального управления.
104. Какова иерархия уровней социального управления?
105. Охарактеризуйте компоненты социального управления.
106. Каковы категории социального управления?
107. Назовите формы социального управления.
108. Изобразите структуру социального управления в Российской Федерации.
109. Охарактеризуйте факторы, обуславливающие возрастание роли информационного управления социума.
110. Изобразите блок-схему обобщённого алгоритма информационного управления социумом.
111. Изобразите блок-схему обобщённого алгоритма информационно-психологического управления социумом.
112. Дайте определение внушению, как средству информационно-психологического воздействия.
113. Изобразите блок-схему классификации видов внушения.
114. Перечислите механизмы внушающего воздействия.

115. Имидж. Дайте определение.
116. Миф. Дайте определение.
117. Стереотип. Дайте определение.
118. Охарактеризуйте открытое и закрытое внушение.
119. В чем заключается контактное и дистантное внушение?
120. Кратковременное и длительное внушение. Дайте определение.
121. В чем состоит непосредственное и отсроченное внушение?
122. Эффект заражения. Как он достигается?
123. Эффект взрыва. Когда он наступает?
124. Эффект образа врага. В чем его сущность?
125. Эффект ореола. Каково его содержание?
126. Эффект реаптенса. В чем он состоит?
127. Эффект насыщения. Когда он возникает?
128. Эффект барлета. При каких условиях он возникает?
129. Эффект бумеранга. В чем его сущность?
130. Эффект края. В чем его сущность?
131. Эффект новизны. Каково его содержание?
132. Охарактеризуйте СМИ и социальные сети как средства ИПВ.
133. Виртуально-психологические средства. В чем заключается их специфика?
134. Психоаналитические средства. Охарактеризуйте их.
135. Нейролингвистические средства. В чем их специфика?
136. Энергоинформационные средства. Каково их устройство?
137. Психотропные средства. Как они воздействуют?
138. Психотропные средства. В чем их специфика?
139. Соматропнопсихо-информационные средства. В чем состоит их механизм воздействия?
140. Сенсорный и субсенсорный каналы человеческого восприятия. Охарактеризуйте их.
141. 25-й кадр. Какова его специфика?
142. В чем состоит манипуляционный способ информационно-психологического воздействия?
143. Охарактеризуйте уровни манипуляционного воздействия.
144. Прием информационной перегрузки. Каково его содержание?
145. Прием дозирования информации. Как он искажает картину реальности?
146. Большая ложь как прием информационно-психологического 64 воздействия.
147. Смешивание факторов как прием манипулирования информацией.
148. Прием выигрыша времени. Как он реализуется?
149. Прием скрытого удара. В чем его сущность?
150. Прием своевременной лжи. Как он реализуется?
151. Охарактеризуйте свойства психического вируса.
152. Перечислите комплексы внедрения психических вирусов.
153. В чем состоит сущность информационно-управляющего воздействия?
154. Перечислите способы информационно-управляющего воздействия?
155. Охарактеризуйте разновидности трансформирования.
156. В чем состоит прием дезинформирования? Охарактеризуйте его разновидности.
157. Метадезинформирование и его разновидности. Охарактеризуйте их.

158. Каковы объекты информационно-психологического воздействия?
159. Перечислите контуры сознания.
160. Алгоритм воздействия на человеческое сознание с использованием контуров.
161. Для чего нужна коммуникация в живой природе?
162. В чем особенность человеческой коммуникации?
163. Зачем коммуникация необходима злоумышленникам?
164. Определите понятие «контент».
165. Как классифицируют контент по степени его уникальности?
166. Какие формы передачи контента всем известны? Охарактеризуйте их.
167. Какова направленность контентов с точки зрения их применения?
168. Охарактеризуйте коммуникативные ситуации межличностного общения.
169. Опишите коммуникационные ситуации, обусловленные нахождение личности в составе определенной общности людей.
170. Охарактеризуйте коммуникационные ситуации при воздействии СМИ.
171. Предпосылки возникновения средств массовой коммуникации.
172. Фейковые риски массовой коммуникации. В чем они состоят?
173. В чем состоит специфика формирования контента?
174. Перечислите простейшие рекомендации по созданию контента социальных сетей?
175. Перечислите принципы формирования Интернет-контента.
176. Назовите способы донесения информации до Интернет-аудитории.
177. Перечислите способы распространения контента в социальных сетях.
178. Сущность трансформации «от аудитории к пользователю».
179. Особенность трансформации «от формата к контенту».
180. Специфика трансформации «от мономедиа к мультимедиа».
181. Трансформация «от периодичности к доставке здесь и сейчас» и ее сущность.
182. Особенность трансформации «о дефиците к изобилию».
183. Специфика трансформации «от редактора к его отсутствию».
184. Трансформация «от распространения к доступу» и ее сущность.
185. Сущность трансформации «от автономности к интерактивности».
186. Особенность трансформации «от линейного повествования к гипертексту».
187. Специфика трансформации «от данных к знаниям».
188. Визуальный тип восприятия.
189. Кто такой аудиовизуал?
190. Как воспринимают мир кинестетики?
191. Кто такой человек-дигитал?
192. Глобальная деревня и ее информационная специфика.
193. Визуальный поворот в современном информационном обществе.
194. На что рассчитаны фейки и кому они нужны?
195. Сущность конспирологических фейков.
196. Для чего используют онлайновых комментаторов?
197. Назовите параметры скорости распространения и восприятия фейков.
198. Охарактеризуйте направленность фейков, предусматривающих ревизию итогов Второй мировой войны.
199. Как стремление предупредить об опасности приводит к распространению фейков, порождающих панику в условиях пандемии?

200. Представьте формализацию первичного эффекта инфицирования психологическим вирусом.
201. Как выглядит модель вторичного эффекта инфицирования психологическим вирусом?
202. Изобразите граф феерверкоподобного распространения психологического вируса.
203. Как измеряются риски неблагоприятного и шансы позитивного развития инфодемии?
204. Сущность современной информационной революции.
205. Каковы тренды развития глобальных социальных сетей?
206. В чем состоит актуальность информационного влияния и управления в социальных сетях?
207. Сформулируйте задачи информационного противоборства в условиях организации эпидемии в социальных сетях.
208. Приведите типологию ресурсов в формате Web 2.0.
209. Перечислите высокорейтинговые ресурсы.
210. Определите объект информационного противоборства.
211. Перечислите классы объектов информационного противоборства.
212. Перечислите сегменты информационно-психологического пространства, которые могут стать объектами противоборства.
213. Перечислите субъекты информационного противоборства.
214. Перечислите психологические ресурсы.
215. Укажите признаки субъекта информационного противоборства.
216. Укажите роль в информационной борьбе владельцев открытых информационно-телекоммуникационных сетей.
217. Обозначьте роль транснациональных корпораций в информационно-психологическом пространстве.
218. Перечислите характеристики социальных сетей, в которых наиболее остро проявляется информационное противоборство.
219. Охарактеризуйте виртуальные коммуникации как субъекты геополитической конкуренции.
220. В чем состоит социально-техническая специфика сообществ социальных сетей?
221. Перечислите наиболее распространённые формы организации общения с использованием Web-технологий.
222. Назовите наиболее общие черты сетевых сообществ.
223. Как сетевые сообщества могут быть использованы с точки зрения воспитания умений?
224. Какие могут быть у подростка мотивы злоупотребления интернет-пространством?
225. Какие существуют направления психологической профилактики интернет-зависимости?
226. Назовите устойчивые поведенческие паттерны разрушительного типа, формируемые у зависимых пользователей в социальных сетях.
227. Назовите причины востребованности социальных сетей для проведения психологических операций.
228. Перечислите факторы, обуславливающие информационное влияние в ходе контент-противоборства в социальных сетях.
229. Назовите правила проведения контентных войн.

230. Для чего используется искажение реальности в социальных сетях?
231. Назначение перегрузки пользователя социальных сетей информационным мусором.
232. Определите основной принцип проведения контентных войн.
233. В результате чего эпидемия коронавируса достигается статуса пандемии?
234. Охарактеризуйте тематическое пространство инфодемии.
235. Какие риски породила инфодемия?
236. В чем состоят шансы, индуцированные инфодемией?
237. Какова графовая формализация инфодемии?
238. Что произошло в массовом обществе с появлением сети Интернет?
239. Приведите характеристики «виртуальной толпы».
240. Перечислите принципы, на которые полагался Йозеф Геббельс в своей деятельности.
241. Какова цель информационного конфликта, и с помощью какого инструмента она достигается?
242. Понятие троллинг.
243. Какие люди могут стать троллями?
244. Перечислите разновидности троллинга.
245. Приведите классификацию троллинг-мотивов.
246. Какие выделяют категории троллей?
247. Какие существуют программы для автоматической публикации контента?
248. Перечислены возможности сети Интернет троллинга.
249. Понятие «цветные революции».
250. В чем суть «цветных революций»?
251. На какие инфраструктурные категории подразделяются «цветные революции»?
252. На какие уровни люди могут разделяться до начала протестных акций?
253. Роль символики в «цветных революциях».
254. В силу чего молодежь является идеальным инструментом для революционных действий?
255. Какие задачи выполняет молодежь в «цветных революциях»?
256. Какие факторы выделяют для успешного проведения «цветной революции»?
257. Какие этапы «цветной революции» выделяет Джин Шарп в своих работах?
258. Социальные сети как инструмент реализации «цветных революций»
259. Почему необходимо измерять параметры не только контентов, но и Интернет-ресурсов?
260. В чем сущность дифференциальных и интегральных метрик?
261. Охарактеризуйте ареалы низкой, средней и высокой вовлеченности пользователей в содержание контента.
262. Как измеряются созвучность, тиражируемость, комментиремость и привлекательность контента?
263. Приведите выражения для расчета заметности и востребованности контента в ресурсе.
264. Как измеряется удельная мощность ареалов высокой, средней и низкой вовлеченности пользователей ресурса в содержание контента?
265. Приведите выражения для оценки рисков невиртуальных деструктивных действий представителей низкой, средней и высокой вовлеченности.

266. Как на i-ом шаге мониторинга оценить созвучность, тиражируемость, комментируемость и привлекательность контента?
267. Приведите дифференциальные метрики первичной реакции пользователей на контент.
268. Охарактеризуйте дифференциальные метрики вторичной реакции пользователей на контент.
269. Укажите аналитические выражения дифференциальных метрик риска невиртуальных деструктивных действий пользователей.
270. Приведите метрики пошагового сравнения восприимчивости антагонистических контетов.
271. Охарактеризуйте метрики пошагового сравнения параметров первичной реакции пользователей ресурса на антагонистические контенты.
272. Укажите аналитические выражения метрики пошагового сравнения параметров вторичной реакции пользователей ресурса на антагонистические контенты.
273. Как осуществляется оценка рисков невиртуальных деструктивных действий пользователей, вовлеченных в содержание антагонистических контентов?
274. В чем состоит векторная ресурсов на основе среднесуточных показателей реакций их пользователей?
275. Как и для чего следует осуществлять риск-ранжирование ресурсов?
276. Для чего и как реализуется тематическая классификация ресурсов?
277. Почему руководство Китая предусматривает модернизацию политики и духовности в соответствии с идеологией Конфуцианства?
278. В чем состоит китайская модель «гигантского муравейника»?
279. Каково значение социально-ходовых связей для китайцев?
280. Гуманность и просветление как психологические категории управления в Поднебесной.
281. Конфуцианство как основа единения общества КНР.
282. В чем видится назначение проекта «Золотой щит»?
283. Каков функционал подсистемы «Великий файрвол»?
284. Насколько эффективен «Золотой Щит» в борьбе с кибертерроризмом?
285. Каковы цели внедрения системы социального кредита в КНР?
286. Какие личные данные китайцев используются в системе социального кредита?
287. Как осуществляется информационный контроль в Синьцзян-Уйгурской провинции КНР?
288. Перечислите технические методики, используемые в управлении китайским населением.
289. Как вычисляется и используется в Китае коэффициент благонадежности?
290. Как устраняется анонимность в китайском Интернет-пространстве?
291. О чем говорят результаты апробации системы социального кредита?
292. В чем видится самоокупаемость технологий информационно-психологического контроля, разработанных в КНР?
293. Каково информационно-психологическое назначение Интернет-троллинга?
294. Какова сущность автопостинга?
295. Перечислите и охарактеризуйте известные «армии троллей».
296. Каковы общие принципы мониторинга социальных сетей?
297. Охарактеризуйте структуру мониторинга контентов.

298. Каков функционал модуля сканирования пабликов и выделения контентов?
299. Охарактеризуйте модуль выявления и классификации контентов.
300. Каков функционал модуля оценки параметров и построения характеристик контентов?
301. Как осуществляется формирование базы данных контентов?
302. Какова структура управления, актуализации и пользования базой данных контентов?
303. Каковы негативы и позитивы изоляции социо-информационного пространства КНР?
304. Цифровизация и наблюдение за гражданами: каковы позитивы и негативы?
305. Каков функционал троллинга в информационном управлении обществом?
306. В чем заключается региональный аспект информационного управления?
307. Опишите проект «Золотой щит».
308. На каких составляющих базируется «Золотой щит»?
309. Что представляет собой технология DPI?
310. Что представляет собой технология Connection probe?
311. Что представляет собой технология SVM?
312. В чем суть функции «Золотого щита»?
313. Приведите виды правонарушений в процессе функционирования «Золотого щита».
314. Какие результаты дало использование «Великого китайского файрвола» в борьбе с Интернет-преступностью?
315. Что такое китайская парадигма?
316. В чем состоит суть «коэффициента благонадежности»?
317. Из чего следует психологическая составляющая системы управления
318. населением правительством КНР?
319. Как влияют системы социального кредита на общество?
320. Какие технические методики используются для управления населением?
321. Укажите цели и задачи противодействия информационно-психологическим атакам.
322. Опишите средства и систему информационно-психологического противодействия.
323. Предметная область корпораций и компаний (КК).
324. Миссия КК.
325. Функции КК.
326. Задачи КК в строительстве.
327. Задачи КК в приборо- и машиностроении.
328. Функции управления в КК.
329. Жизненный цикл проекта / изделия КК.
330. Управление жизненным циклом объектов промышленного назначения.
331. Информационные потоки КК.
332. Организационная структура управления КК.
333. Типовые организационные структуры КК.
334. Функции структурных подразделений КК.
335. Математическая модель структуры КК.
336. Нормативные документы для КК.

337. Программное обеспечение для КК.
338. Стадии проектирования.
339. Корпоративная информационная система (КИС) КК – назначение.
340. Функциональная структура типовой КИС КК комплексного типа.
341. Принципы создания КИС.
342. Состав КИС проектной организации.
343. Формальные модели КИС.
344. Функциональная модель КИС.
345. Критические информационные ресурсы КК.
346. Информационная модель КИС.
347. Необходимость оценки стоимости информационных ресурсов КК.
348. Система идентификации проектных и иных документов.
349. Описание базового обозначения документации.
350. Факторы, требующие расширения базовой системы обозначений.
351. Идентификация электронных документов.
352. Классификация информационных ресурсов по способу оценки их стоимости.
353. Оценка НМА, созданных внутри компании.
354. Оценка угроз безопасности информации КК.
355. Основные виды угроз безопасности информации.
356. Угрозы конфиденциальности информации.
357. Угрозы целостности информации.
358. Угрозы доступности информации.
359. Источники угроз безопасности информации.
360. Внешние источники угроз.
361. Внутренние источники угроз.
362. Уровни возможностей внутреннего нарушителя.
363. Формирование требований к системе информационной безопасности в КК.
364. Цели и задачи СУИБ КК.
365. Объекты защиты в КИС КК.
366. Пути решения задач защиты информации.
367. Этапы создания СУИБ.
368. Исходные данные для разработки СУИБ.
369. Определение требований к СЗИ КИС КК.
370. Организационно-технические мероприятия по защите информации при ее обработке и передаче в информационных системах КК.
371. Система документов по защите информации.
372. Организационные мероприятия по защите информации в АРМ.
373. Организационные мероприятия по защите информации в локальных вычислительных сетях.
374. Организационные мероприятия по антивирусной защите.
375. Организация резервного копирования и восстановления.
376. Технические мероприятия по защите информации.
377. Порядок задания требований по защите информации.
378. Планирование работ по защите информации.
379. Контроль состояния защиты информации.
380. Администрирование безопасности информации.

7.2.6 Методика выставления оценки при проведении промежуточной аттестации

(Например: Зачет проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Учебный стандарт и план специальности в условиях цифровой трансформации и сетевой организации пространства	ПК-7.2, ПК-7.3	Тест
2	Проблема обеспечения безопасности автоматизированной информационной системы и сети	ПК-7.3	Тест
3	Модели атакуемых автоматизированных сетей	ПК-7.2	Тест
4	Эпидемические модели автоматизированных сетей	ПК-7.2	Тест
5	Информационная безопасность и социальная инженерия в автоматизированных сетях	ПК-7.2	Тест
6	Автоматизированные сети и деструктивный контент	ПК-7.2	Тест
7	Мониторинг безопасности автоматизированных сетей	ПК-7.2	Тест
8	Перспективы цифровой трансформации и обеспечения безопасности автоматизированных сетей и систем на основе средств искусственного интеллекта	ПК-7.3	Тест
9	Картографирование защищаемого кибер-сетевого пространства	ПК-7.3	Тест
10	Особенности обеспечения безопасности интернета вещей	ПК-7.3	Тест
11	Результаты и перспективы реализации проекта «Безопасный интернет»	ПК-7.3	Тест
12	Риск-мониторинг Интернет-ресурса	ПК-7.3	Тест

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсового проекта осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

№ п/п	Авторы, составители	Заглавие	Годы издания, вид издания
8.1.1.1	А.Г. Остапенко, Н.М. Радько, А.О. Калашников, О.А. Остапенко, Р.К. Бабаджанов	Теория сетевых войн: Эпидемии в телекоммуникационных сетях	2018, печат.
8.1.1.2	А.Г. Остапенко, Д.Г. Плотников, В.Б. Щербаков, А.О. Калашников, О.А. Остапенко	Теория сетевых войн: Атакуемые взвешенные сети	2018, печат.
8.1.1.3	А.Г. Остапенко, А.В. Паринов, А.О. Калашников, В.Б. Щербаков, А.А. Остапенко	Теория сетевых войн: социальные сети и деструктивный контент	2018, печат.
8.1.1.4	А.Г. Остапенко, Е.Ю. Чапурин, А.О. Калашников, О.А. Остапенко, Г.А. Остапенко	Теория сетевых войн: Социальные сети и риск-мониторинг	2019, печат.
8.1.1.5	А.Г. Остапенко Е.Б. Белов, А.О. Калашников, В.П. Лось, О.А. Остапенко	Теория сетевых войн: Социальные сети и психологическая безопасность	2020, печат.
8.1.1.6	А.Г. Остапенко, Е.Б. Белов, А.О. Калашников, В.П. Лось, А.А. Остапенко	Теория сетевых войн: Сетевая эпидемиология	2021, печат
8.1.1.7	А.Г. Остапенко, О.А. Остапенко, Н.М. Лантюхов, И.А. Боков, Д.А. Нархов	Методические указания к курсовым работам по дисциплине «Введение в специальность»	2021, печат

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем

8.2.1 Свидетельство №2017610047 о государственной регистрации программы для ЭВМ и «Netepidemic»

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория 407/5, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

10 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Введение в специальность» читаются лекции, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы. Освоение дисциплины оценивается на зачете.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад.
Подготовка к дифференцированному зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и решение задач на практических занятиях.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4