Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Комплексное обеспечение защиты информации объекта информатизации

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	116	116	116	116
Часы на контроль	36	36	36	36
Итого	216	216	216	216

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Лапсарь А.П.

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	приобретение знаний об основных типах технических и программных средств, используемых для защиты информации объекта информатизации, их технико-экономических характеристиках, принципах построения и функционирования, перспективах их развития, современного инструментария предназначенного для построения современных систем защиты информации объекта информатизации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

ОПК-2.1: Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;

ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

В результате освоения дисциплины обучающийся должен:

Знать:

способы подбора, изучения и обобщения научно-технической литературы; основное содержание нормативных и методических документов в области информационной безопасности (соотнесено с индикатором ОПК- 8.1);
методы анализа процесса функционирования объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз (соотнесено с индикатором ОПК- 2.1.1);
содержание и способы разработки комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности, их ;внедрения и сопровождения (соотнесено с индикатором ОПК- 2.3..1)

Уметь:

осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач в области информационной безопасности (соотнесено с индикатором ОПК- 8.2);
проводить анализ процесса функционирования объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба (соотнесено с индикатором ОПК- 2.1.2);
разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности (соотнесено с индикатором ОПК- 2.3.2)

Владеть:

подбора, изучения и обобщения научно-технической литературы, применения требований нормативных и методических документов в целях решения задач деятельности по обеспечению информационной безопасности (соотнесено с индикатором ОПК- 8.3);
проведения анализ функционального процесса объекта защиты и его информационных составляющих, выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба (соотнесено с индикатором ОПК- 2.1.3);
планирования, разработки внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности (соотнесено с индикатором ОПК - 2.3.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Построение комплексных систем защиты информации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	"Цель, задачи, содержание и структура дисциплины":место дисциплины в системе подготовки специалистов по защите информации. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.2	"Цель, задачи, содержание и структура дисциплины":место дисциплины в системе подготовки специалистов по защите информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.3	"Концепция создания защищенных информационно-телекоммуникационных систем":основные требования и принципы создания защищенных информационно-телекоммуникационных систем / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.4	"Концепция создания защищенных информационно-телекоммуникационных систем":основные требования и принципы создания защищенных информационно-	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4

	телекоммуникационных систем / Ср /				
1.5	"Этапы создания комплексной системы защиты информации":основные этапы создания комплексной системы защиты информации и их характеристика. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.6	"Этапы создания комплексной системы защиты информации":основные этапы создания комплексной системы защиты информации и их характеристика. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.7	"Научно-исследовательская разработка КСЗИ":принципы и этапы научно-исследовательских разработок КСЗИ. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.8	"Научно-исследовательская разработка КСЗИ":принципы и этапы научно-исследовательских разработок КСЗИ. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.9	"Моделирование КСЗИ": классификация и характеристика различных типом моделей, используемых при создании КСЗИ. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.10	"Моделирование КСЗИ": классификация и характеристика различных типом моделей, используемых при создании КСЗИ. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.11	"Специальные методы неформального моделирования": содержание и характеристика специальных методов неформального моделирования; метод экспертного оценивания. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.12	"Специальные методы неформального моделирования": содержание и характеристика специальных методов неформального моделирования; метод экспертного оценивания. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.13	"Декомпозиция общей задачи оценки эффективности функционирования КСЗИ":особености решения задач оценки эффективности функционирования КСЗИ на основе метода декомпозии общей задачи. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.14	"Декомпозиция общей задачи оценки эффективности функционирования КСЗИ":особености решения задач оценки эффективности функционирования КСЗИ на основе метода декомпозии общей задачи. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.15	"Выбор показателей эффективности и критериев оптимальности КСЗИ":принципы выбора и характеристика основных показателей эффективности;критерии оптимальности КСЗСИ / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.16	"Выбор показателей эффективности и критериев оптимальности КСЗИ":принципы выбора и характеристика основных показателей эффективности;критерии оптимальности КСЗСИ / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.17	"Математическая постановка задачи по разработке комплексной системы защиты информации":типы используемых математических моделей при разработке КСЗИ. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.18	"Математическая постановка задачи по разработке комплексной системы защиты информации":типы используемых математических моделей при разработке КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.19	"Подходы к оценке эффективности КСЗИ";характеристка основных подходов к оценке эффективности КСЗИ. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.20	"Подходы к оценке эффективности КСЗИ";характеристка основных подходов к оценке эффективности КСЗИ. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.21	"Официальный подход к оценке эффективности КСЗИ":нормативно-правовые требования к оценке эффективности КСЗИ. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.22	"Официальный и экспериментальный подходы к оценке эффективности КСЗИ":нормативно-правовые требования к оценке эффективности КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.23	"Экспериментальный подход к оценке эффективности КСЗИ":особенности реализации экспериментального подхода к оценке эфеективности КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.24	"Создание организационной структуры КСЗИ";.основные	7	2	ОПК-8,	Л1.1, Л1.2, Л2.1,

	элементы структуры КСЗИ; требования при создании организационной структуры КСЗИ. / Лек /			ОПК-2.1, ОПК-2.3	Л2.3
1.25	"Создание организационной структуры КСЗИ";.основные элементы структуры КСЗИ; требования при создании организационной структуры КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.26	Модели комплексной системы защиты информации, их преимущества и недостатки / Ср /	7	6	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.27	Определения состава защищаемой информации, с использованием LibreOffice. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.28	Инвентаризация информационных ресурсов, определение состава защищаемой информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.29	Классификация информации по видам тайны и степеням конфиденциальности. / Ср /	7	6	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.30	Определение состава машинных носителей защищаемой информации. / Ср /	7	6	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.31	Определение направлений и возможностей доступа нарушителей к защищаемой информации. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.32	Определение направлений и возможностей доступа нарушителей к защищаемой информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.33	Определение основных компонентов комплексной системы защиты информации. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.34	Оптимизация компонентов комплексной системы защиты информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.35	Методы оценки эффективности комплексной системы защиты информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.36	Оценка эффективности комплексной системы защиты информации неформализованными методами. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.37	Сущность и задачи комплексной системы защиты информации. Разработка модели КСЗИ. / Пр /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.38	Сущность и задачи комплексной системы защиты информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.39	Определения состава защищаемой информации. / Пр /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.40	Методика выявления состава носителей защищаемой информации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.41	Выявление способов воздействия на информацию. / Пр /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.42	Выявление способов воздействия на информацию. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.43	Построение многоуровневой модели нарушителя. / Пр /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.44	Построение модели нарушителя. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.45	Обеспечение информационной безопасности при вводе объектов в эксплуатацию. / Пр /	7	4	ОПК-8, ОПК-2.1,	Л1.1, Л1.2, Л2.1, Л2.3

				ОПК-2.3	
1.46	Факторы, влияющие на выбор компонентов КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.47	Классификация информационных систем и категорирование объекта информатизациии. / Пр /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.48	Классификация информационных систем и категорирование объекта информатизациии. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.49	"Применение КСЗИ по назначению":особенности применения КСЗИ при организации защиты информации на объектах информатизации. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.50	"Применение КСЗИ по назначению":особенности применения КСЗИ при организации защиты информации на объектах информатизации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.51	Организация предпроектного обследования объекта информатизации. / Пр /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
1.52	Организация предпроектного обследования объекта информатизации. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3

Раздел 2. Организация функционирования комплексных систем защиты информации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	"Техническая эксплуатация КСЗИ":основные этапы эксплуатации КСЗИ; требования при эксплуатации КСЗИ. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
2.2	"Техническая эксплуатация КСЗИ":основные этапы эксплуатации КСЗИ; требования при эксплуатации КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
2.3	"Планирование эксплуатации КСЗИ":цели планирования;виды планирования и их назначение;методы и формы контроля выполнения планов. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.4	"Планирование эксплуатации КСЗИ":цели планирования;виды планирования и их назначение;методы и формы контроля выполнения планов. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.5	"Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций";особенности управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. / Лек /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.6	"Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций";особенности управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.7	Сбор, обработка и изучение информации, необходимой для планирования КСЗИ. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л2.1, Л2.3
2.8	Сбор, обработка и изучение информации, необходимой для планирования КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.9	Межведомственный контроль функционирования КСЗИ. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.10	Внутриобъектовый контроль функционирования КСЗИ. / Ср /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.11	Основные стили управления КСЗИ. / Пр /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.12	Основные стили управления КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4

2.13	Анализ и использование результатов проведения контрольных мероприятий функционирования КСЗИ. / Пр /	7	4	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.14	Анализ и использование результатов проведения контрольных мероприятий функционирования КСЗИ. / Ср /	7	2	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.15	/ Экзамен /	7	36	ОПК-8, ОПК-2.1, ОПК-2.3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Смирнов А. А.	Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза: монография	Москва: ЮНИТИ-ДАНА: Закон и право, 2012	http://biblioclub.ru/index.php?page=book&id=448202 неограниченный доступ для зарегистрированных пользователей
Л1.2	Сердюк В. А.	Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие	Москва: Издательский дом Высшей школы экономики, 2015	http://biblioclub.ru/index.php?page=book&id=440285 неограниченный доступ для зарегистрированных пользователей
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2017	http://www.iprbookshop.ru/63594.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Креопалов В. В.	Технические средства и методы защиты информации: учебно-практическое пособие: учебное пособие	Москва: Евразийский открытый институт, 2011	https://biblioclub.ru/index.php?page=book&id=90753 неограниченный доступ для зарегистрированных пользователей
Л2.2		Информационная безопасность: журнал	Москва: Гротек, 2014	https://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей
Л2.3		Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: практикум	Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016	https://biblioclub.ru/index.php?page=book&id=458012 неограниченный доступ для зарегистрированных пользователей
Л2.4	Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: учебно-методическое пособие	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/77317.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Информационная справочная система "КонсультантПлюс"
База данных Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/
База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-8: способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности			
З. способы подбора, изучения и обобщения научно-технической литературы; основное содержание нормативных и методических документов в области информационной безопасности	основное содержание нормативных правовых актов и методических документов в области информационной безопасности	полнота и содержательность ответа, обоснованность выбора в ответах на вопросы опроса, на экзамене	Э (1-30) О (1-30)
У. осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач в области информационной безопасности	решение практических заданий формирования требований к обеспечению информационной безопасности организации	правильность выполнения задания, обоснованность применения информационных технологий для сбора информации при выполнении практических заданий	ПОЗЭ (1-10) ПЗ (1-8)
В. навыками подбора, изучения и обобщения научно-технической литературы, применения требований нормативных и методических документов в целях решения задач по обеспечению информационной безопасности	формирование требований по информационной безопасности на объекте защиты при выполнении практических заданий	правильность выполнения задания, обоснованность выбора и применения обязательных требований при выполнении практических заданий	ПОЗЭ (1-10) ПЗ (1-8)
ОПК-2.1: Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба			
З методы анализа процесса функционирования объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз	типы и виды угроз объектам информатизации и информационным системам	полнота и содержательность ответа умение приводить примеры при ответе на экзамене, опросе	Э (1-30) О (1-30)
У проводить анализ процесса функционирования объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	проводит анализ защиты информации при его функционировании (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты информации) при выполнении практических работ	правильность выполнения практического задания	ПОЗЭ (1-10) ПЗ (1-8)
В навыками проведения анализа функционального процесса объекта защиты и его информационных составляющих, выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	проводит аудит информационной безопасности объекта при выполнении практических работ	методика и результаты оценки угроз информационной безопасности соответствуют требованиям нормативных документов	ПОЗЭ (1-10) ПЗ (1-8)
ОПК-2.3: Ссособен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности			
З содержание и способы разработки комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности, их внедрения и сопровождения	меры по обеспечению информационной безопасности объекта защиты, обязанности должностных лиц по обеспечению информационной безопасности объекта защиты при подготовке к экзамену, опросу	полнота и содержательность ответа умение приводить примеры при ответе на экзамене, опросе	Э (1-30) О (1-30)
У разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	организация обеспечения безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности при выполнении практического задания	правильность выполнения практического задания	ПОЗЭ (1-10) ПЗ (1-8)

В навыками планирования, разработки внедрения и сопровождения комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	Организует планирование и реализацию актуальных мер по обеспечению информационной безопасности при выполнении практических работ	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПОЗЭ (1-10) ПЗ (1-8)

О – опрос, Э – вопросы для экзамена, ПЗ – практические задания, ПОЗЭ – практико-ориентиованные задания к экзамену

1.2 Шкалы оценивания:
Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:
84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к экзамену

1. Понятие и сущность КСЗИ.
2. Назначение КСЗИ.
3. КСЗИ как средство выражения концептуальных основ защиты информации.
4. Методологические основы организации КСЗИ.
5. Основные положения теории систем.
6. Характер и степень влияния различных факторов на организацию КСЗИ.
7. Методика определения состава защищаемой информации.
8. Работы по выявлению состава защищаемой информации.
9. Значение носителей защищаемой информации как объектов защиты.
10. Методика выявления состава носителей защищаемой информации.
11. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
12. Методика выявления способов воздействия на информацию.
13. Методика выявления каналов несанкционированного доступа к информации.
14. Оценка степени целостности информации в результате действий нарушителей различных категорий.
15. Факторы, влияющие на выбор компонентов КСЗИ.
16. Основные требования, предъявляемые к выбору методов и средств защиты.
17. Понятие модели объекта, основные виды моделей и их характеристика.
18. Характеристика основных стадий создания КСЗИ.
19. Определение состава кадрового обеспечения функционирования КСЗИ.
20. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ.
21. Понятие и цели управления КСЗИ. Сущность процессов управления КСЗИ.
22. Понятие и задачи планирования функционирования КСЗИ. Способы и методы планирования.
23. Понятие и виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ. Методы контроля.
24. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации.
25. Классификация подходов к оценке эффективности систем защиты информации.
26. Оценочный подход на основе формирования требований к защищенности объекта.
27. Сравнительный анализ подходов оценки эффективности систем защиты информации.
28. Классификационная структура методов и моделей оценки эффективности комплексной системы защиты информации.

29. Системы показателей защищенности (эффективности).
30. Метод оценки эффективности на основе структурных вопросников.

Практико-ориентированные задания к экзамену

1. Разработка модели КСЗИ.
2. Определения состава защищаемой информации.
3. Классификация информации по видам тайны и степеням конфиденциальности.
4. Определение состава носителей защищаемой информации.
5. Определение направлений и возможностей доступа нарушителей к защищаемой информации.
6. Определение компонентов комплексной системы защиты информации
7. Оценка эффективности комплексной системы защиты информации.
8. Построение модели нарушителя
9. Организация предпроектного обследования объекта информатизации
10. Контроль функционирования КСЗИ.

Критерии оценивания:

- 84-100 баллов – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированного задания, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целью обучения, правильные действия по применению навыком и умений при решении практико-ориентированного задания, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 баллов – наличие твердых знаний в объеме пройденного курса в соответствии с целью обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению навыком и умений при решении практико-ориентированного задания;
- 0-49 баллов – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированного задания, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Вопросы для опроса

1. Понятие и сущность КСЗИ.
2. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
3. КСЗИ как средство выражения концептуальных основ защиты информации.
4. Методика выявления состава носителей защищаемой информации.
5. Назначение КСЗИ.
6. Оценочный подход на основе формирования требований к защищенности объекта.
7. Классификация подходов к оценке эффективности систем защиты информации.
8. Понятие и виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ. Методы контроля.
9. Методологические основы организации КСЗИ.
10. Факторы, влияющие на выбор компонентов КСЗИ
11. Основные положения теории систем.
12. Характеристика основных стадий создания КСЗИ.
13. Характер и степень влияния различных факторов на организацию КСЗИ.
14. Системы показателей защищенности (эффективности).
15. Методика определения состава защищаемой информации.
16. Сравнительный анализ подходов оценки эффективности систем защиты информации.
17. Работы по выявлению состава защищаемой информации.
18. Метод оценки эффективности на основе структурных вопросников.

19. Основные требования, предъявляемые к выбору методов и средств защиты.
20. Понятие модели объекта, основные виды моделей и их характеристика.
21. Классификационная структура методов и моделей оценки эффективности комплексной системы защиты информации.
22. Значение носителей защищаемой информации как объектов защиты.
23. Методика выявления способов воздействия на информацию.
24. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации.
25. Определение состава кадрового обеспечения функционирования КСЗИ.
26. Понятие и цели управления КСЗИ. Сущность процессов управления КСЗИ.
27. Понятие и задачи планирования функционирования КСЗИ. Способы и методы планирования.
28. Оценка степени целостности информации в результате действий нарушителей различных категорий.
29. Методика выявления каналов несанкционированного доступа к информации.
30. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ.

Критерии оценивания:

- 2 балла выставляется обучающемуся, если изложенный материал фактически верен и логически обоснован.
- 1-0 баллов, если ответ неверный или имеет неточности.

Максимальное количество баллов за семестр: 36 баллов.

Практические задания

Практическое задание 1 Сущность и задачи комплексной системы защиты информации. Разработка модели КСЗИ.
Практическое задание 2 Определения состава защищаемой информации.
Практическое задание 3 Выявление способов воздействия на информацию.
Практическое задание 4 Построение многоуровневой модели нарушителя.
Практическое задание 5 Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
Практическое задание 6 Классификация информационных систем и категорирование объекта информатизации.
Практическое задание 7 Организация предпроектного обследования объекта информатизации.
Практическое задание 8 Анализ и использование результатов проведения контрольных мероприятий функционирования КСЗИ.

Критерии оценивания:

-(для каждого задания):
8 б. – задание выполнено верно;
7-5 б. – при выполнении задания были допущены неточности, не влияющие на результат;
5-3 б. – при выполнении задания были допущены ошибки;
2 - 1 б. – при выполнении задания были допущены существенные ошибки;
0 б. – задание не выполнено

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию промежуточной аттестации в письменном виде. Количество вопросов в экзаменационном билете – 3. Проверка ответов и объявление результатов производится в день экзамена.

Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются теоретические вопросы с учетом практико-ориентированности изучаемой дисциплины, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки сбора информации по основным темам курса.

При подготовке к практическим занятиям каждый обучающийся должен:

– изучить рекомендованную учебную литературу;

– изучить практические примеры, рассмотренные на лекциях;

– подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом опроса и посредством выполнения практических заданий. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.