ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (КИИ)

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

- изучить нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ;
- основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- общие требования по обеспечению безопасности значимых объектов КИИ;
- общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования;
- научиться определять категории значимости объектов КИИ;
- определять структуру системы безопасности значимого объекта КИИ.

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.10 Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) относится к части, формируемой участниками образовательных отношений учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ)» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-1	Технология построения защищенных автоматизированных систем Безопасность систем баз данных Производственная (преддипломная) практика Основы защиты АИС
ПК-3	Безопасность вычислительных сетей Безопасность систем баз данных Производственная (преддипломная) практика Безопасность операционных систем
ПК-6	Системы реального времени Производственная (преддипломная) практика Аудит информационной безопасности Моделирование систем

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-1	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика КОИБАС
ПК-3	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика КОИБАС

ПК-6	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика КОИБАС

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	*Знать:* Нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ и АСУТПиП; основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; принципы организации систем безопасности значимых объектов КИИ Российской Федерациии обеспечения их функционирования; процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

		Уметь: Определять структуру системы безопасности значимого объекта КИИ; осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ *Владеть:* Навыками разработки организационно-распорядительных документов по безопасности значимых объектов КИИ

ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	*Знать:* Общие требования по обеспечению безопасности значимых объектов КИИ; общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования; требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ *Уметь:* Определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации; определять требования к обеспечению безопасности значимого объекта КИИ *Владеть:* Навыками проведения работ по контролю состояния безопасности объектов КИИ

ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* Процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ *Уметь:* Выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации *Владеть:* Навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ

ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* Общие требования по обеспечению безопасности значимых объектов КИИ; общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования; требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ; *Уметь:* Обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ *Владеть:* Навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ

ПК-6 Способен проводить анализ рисков информационной безопасности автоматизированной системы	ПК-6.1 Проводит оценку рисков информационной безопасности на основе существующих методик	*Знать:* Основные принципы выявления наличия критических процессов у субъекта КИИ; основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и(или) осуществляют управление, контроль или мониторинг критических процессов; процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ *Уметь:* Выявлять возможные уязвимости, приводящих к возникновению рисков безопасности информации *Владеть:* Навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами

4. Объем дисциплины

Объем дисциплины Б1.В.10 Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) составляет 4 зачетных(ые) единиц(ы) (ЗЕ), (144 академических часов), распределение объёма дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

Вид учебной работы	Итого КР	Итого СР	Семестр №8	
			КР	СР
Лекции (Л)	36		36	

Лабораторные работы (ЛР)				
Практические занятия (ПЗ)	36		36	
Семинары(С)				
Курсовое проектирование (КП)				
Самостоятельная работа		68		68
Промежуточная аттестация	4		4	
Наименование вида промежуточной аттестации	x	x	Экзамен	
Всего	76	68	76	68

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименование тем	Семестр	Объем работы по видам учебных занятий, академические часы									Коды формируемых компетенций, код индикатора достижения компетенции
		Лекции	Лабораторная работа	Практические занятия	Семинары	Курсовое проектирование	Индивидуальные домашние задания (контрольные работы)	Самостоятельноеизучение вопросов	Подготовка к занятиям	Промежуточная аттестация	
Раздел 1. Основы обеспечения безопасности КИИ Российской Федерации	8	4		4							

Тема 1. Введение в безопасность объектов критической информационной инфраструктуры. Основные термины и определения. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. Правовые основы обеспечения безопасности КИИ Российской Федерации. Федеральные законы. Указы Президента РФ. Постановления Правительства РФ. Приказы ФСТЭК России и ФСБ России.	8	4		4					2		ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1
Раздел 2. Категорирование объектов КИИ	8	6		10							

Тема 2. Объекты и субъекты КИИ. Правила категорирования объектов КИИ. Общий порядок работ. Критерии значимости объектов КИИ. Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ. Создание комиссии по категорированию. Формирование перечня критических процессов. Формирование перечня объектов критической ин- формационной инфраструктуры, подлежащих категорированию. Категорирование объектов критической информационной инфраструктуры. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозы безопасности ин- формации объекта КИИ. Построение модели угроз и нарушителей объектов КИИ. Процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ. Оценка масштаба последствий и соотнесение со значениями показателей категорий. Определение	8	6		10					10		ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1

категории значимости объекта КИИ. Оформление и передача в ФСТЭК России результатов категорирования. Внесение изменений в результаты категорирования. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.											
Раздел 3. Обеспечение безопасности значимых объектов КИИ	8	6		6							

Тема 3. Требования по обеспечению безопасности значимых объектов КИИ РФ. Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию, мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации Система безопасности значимого объекта КИИ. Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Стадии (этапы) работ по созданию систем безопасности объекта КИИ. Требования к созданию систем безопасности	8	6		6					10		ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1

значимых объектов КИИ РФ и обеспечению их функционирования. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ											
Раздел 4. Контроль за обеспечением безопасности значимого объекта КИИ	8	4	2								

Тема 4. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК. Порядок ведения реестра значимых объектов КИИ РФ. Итоги проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственным и организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их	8	4		2					10		ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1

предупреждения и обнаружения. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.											
Тема 5. Перечень информации, представляемой в ГосСОПКА и Порядок представления информации в ГосСОПКА. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).	8	2		2					10		ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1
Тема 6. Обследование АСУ ТП. Разработка требований по обеспечению безопасности информации в АСУ ТП. Разработка концепции ОБИ в АСУ ТП. Разработка Технического задания на создание системы защиты АСУ ТП. Проектирование системы защиты АСУ ТП. Внедрение системы защиты АСУ ТП. Разработка комплекта организационно-распорядительной документации, регламентирующей процессы защиты АСУ ТП.	8	4		4			10				ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1

Раздел 7. Аудит безопасности критической инфраструктуры.	8	6		8							
Тема 7. Аудит критической информационной инфраструктуры. Особенности проведения аудита критической информационной инфраструктуры. Определение аудита информационной безопасности. Цели и задачи аудита. Этапы проведения аудита. Схема проведения аудита. Общие подходы к проведению аудита. Классификация аудита. Тестирование как один из основных типов аудита критической информационной инфраструктуры. Тестирование: определение, требования, классификация. Тестирование на основе моделей. Тестирование специальными средствами и способами информационных воздействий. Особенности тестирования критической инфраструктуры информационными воздействиями в технической и в психологических сферах. Тестирование критической инфраструктуры специальными информационно-техническими воздействиями. Общая	8	6		8			16				ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1

классификация информационно-технических воздействий. Оборонительные информационно-технические воздействия. Обеспечивающие информационно-технические воздействия. Атакующие информационно-технические воздействия. Классификация основных средств информационно-технических воздействий.											
Тема 8. Модели правового регулирования в сфере обеспечения безопасности КИИ. Невластные субъекты обеспечения безопасности КИИ, их правовой статус. Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами. Сравнительно-правовой анализ предлагаемых экономических моделей распределения издержек по обеспечению безопасности КИИ.	8	4									ПК-1.1, ПК-1.2, ПК-3.1, ПК-3.2, ПК-6.1
Контактная работа	8	36		36						4	x
Самостоятельная работа	8						26		42		x
Объем дисциплины в семестре	8	36		36			26		42	4	x
Всего по дисциплине		36		36			26		42	4	

5.2. Темы курсовых работ (проектов)

Данный вид работы не предусмотрен учебным планом

5.3. Темы индивидуальных домашних заданий (контрольных работ)

Вопросы для опроса:

Раздел №1. Основы обеспечения безопасности КИИ Российской Федерации.

1. Введение в безопасность объектов критической информационной инфраструктуры. Основные термины и определения.
2. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.
3. Правовые основы обеспечения безопасности КИИ Российской Федерации. Федеральные законы. Указы Президента РФ. Постановления Правительства РФ. Приказы ФСТЭК России и ФСБ России.

Раздел № 2. Категорирование объектов КИИ

1. Объекты и субъекты КИИ.
2. Правила категорирования объектов КИИ. Общий порядок работ. Критерии значимости объектов КИИ.
3. Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ.
4. Создание комиссии по категорированию. Формирование перечня критических процессов.
5. Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию.
6. Категорирования объектов критической информационной инфраструктуры.
7. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозы безопасности информации объекта КИИ.
8. Построение модели угроз и нарушителей объектов КИИ. Процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ.
9. Оценка масштаба последствий и соотнесение со значениями показателей категорий.
10. Определение категории значимости объекта КИИ.
11. Оформление и передача в ФСТЭК России результатов категорирования.
12. Внесение изменений в результаты категорирования. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.

Раздел №3. Обеспечение безопасности значимых объектов КИИ

1. Требований по обеспечению безопасности значимых объектов КИИ РФ.
2. Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
3. Требования к параметрам настройки программных и программно- аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации
4. Система безопасности значимого объекта КИИ.
5. Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
6. Стадии (этапы) работ по созданию систем безопасности объекта КИИ.
7. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования.
8. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ

Раздел № 4. Контроль за обеспечением безопасности значимого объекта КИИ

1. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.

2. Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК.

3. Порядок ведения реестра значимых объектов КИИ РФ.

4. Итоги проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.

5. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

6. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.

Раздел №5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)

1. Перечень информации, представляемой в ГосСОПКА и Порядок представления информации в ГосСОПКА.

2. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).

Раздел №6. Обеспечение защиты информации в АСУ ТП КИИ

1. Обследование АСУ ТП.

2. Разработка требований по обеспечению безопасности информации в АСУ ТП. Разработка концепции ОБИ в АСУ ТП.

3. Разработка Технического задания на создание системы защиты АСУ ТП.

4. Проектирование системы защиты АСУ ТП.

5. Внедрение системы защиты АСУ ТП.

6. Разработка комплекта организационно-распорядительной документации, регламентирующей процессы защиты АСУ ТП.

Раздел №7. Аудит безопасности критической инфраструктуры.

1. Аудит критической информационной инфраструктуры. Особенности проведения аудита критической информационной инфраструктуры.

2. Определение аудита информационной безопасности. Цели и задачи аудита.

3. Этапы проведения аудита. Схема проведения аудита.

4. Общие подходы к проведению аудита. Классификация аудита.

5. Тестирование как один из основных типов аудита критической информационной инфраструктуры. Тестирование: определение, требования, классификация.

6. Тестирование на основе моделей. Тестирование специальными средствами и способами информационных воздействий.

7. Особенности тестирования критической инфраструктуры информационными воздействиями в технической и в психологических сферах.

8. Тестирование критической инфраструктуры специальными информационно-техническими воздействиями.

9. Общая классификация информационно-технических воздействий.

10. Оборонительные информационно-технические воздействия.

11. Обеспечивающие информационно-технические воздействия.

12. Атакующие информационно-технические воздействия.

13. Классификация основных средств информационно-технических воздействий.

Раздел №8. Сравнительный анализ подходов к регулированию критической информационной инфраструктуры других стран

1. Модели правового регулирования в сфере обеспечения безопасности КИИ.

2. Невластные субъекты обеспечения безопасности КИИ, их правовой статус.

3. Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами.

4. Сравнительно-правовой анализ предлагаемых экономических моделей распределения издержек по обеспечению безопасности КИИ.

Вопросы к зачету.

1. Введение в безопасность объектов критической информационной инфраструктуры. Основные термины и определения.

2. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.

3. Правовые основы обеспечения безопасности КИИ Российской Федерации. Федеральные законы. Указы Президента РФ. Постановления Правительства РФ. Приказы ФСТЭК России и ФСБ России.

4. Объекты и субъекты КИИ.

5. Правила категорирования объектов КИИ. Общий порядок работ. Критерии значимости объектов КИИ.

6. Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ.

7. Создание комиссии по категорированию. Формирование перечня критических процессов.

8. Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию.

9. Категорирования объектов критической информационной инфраструктуры.

10. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозы безопасности информации объекта КИИ.

11. Построение модели угроз и нарушителей объектов КИИ. Процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ.

12. Оценка масштаба последствий и соотнесение со значениями показателей категорий.

13. Определение категории значимости объекта КИИ.

14. Оформление и передача в ФСТЭК России результатов категорирования.

15. Внесение изменений в результаты категорирования. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.

16. Требований по обеспечению безопасности значимых объектов КИИ РФ.

17. Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

18. Требования к параметрам настройки программных и программно- аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации

19. Система безопасности значимого объекта КИИ.

20. Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

21. Стадии (этапы) работ по созданию систем безопасности объекта КИИ.

22. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования.

23. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ

24. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.

25. Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК.

26. Порядок ведения реестра значимых объектов КИИ РФ.

27. Итоги проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.

28. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

29. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.

30. Перечень информации, представляемой в ГосСОПКА и Порядок представления информации в ГосСОПКА.

31. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).

32. Обследование АСУ ТП.

33. Разработка требований по обеспечению безопасности информации в АСУ ТП. Разработка концепции ОБИ в АСУ ТП.

34. Разработка Технического задания на создание системы защиты АСУ ТП.

35. Проектирование системы защиты АСУ ТП.

36. Внедрение системы защиты АСУ ТП.

37. Разработка комплекта организационно-распорядительной документации, регламентирующей процессы защиты АСУ ТП.

38. Аудит критической информационной инфраструктуры. Особенности проведения аудита критической информационной инфраструктуры.

39. Определение аудита информационной безопасности. Цели и задачи аудита.

40. Этапы проведения аудита. Схема проведения аудита.

41. Общие подходы к проведению аудита. Классификация аудита.

42. Тестирование как один из основных типов аудита критической информационной инфраструктуры. Тестирование: определение, требования, классификация.

43. Тестирование на основе моделей. Тестирование специальными средствами и способами информационных воздействий.

44. Особенности тестирования критической инфраструктуры информационными воздействиями в технической и в психологических сферах.

45. Тестирование критической инфраструктуры специальными информационно-техническими воздействиями.

46. Общая классификация информационно-технических воздействий.
47. Оборонительные информационно-технические воздействия.
48. Обеспечивающие информационно-технические воздействия.
49. Атакующие информационно-технические воздействия.
50. Классификация основных средств информационно-технических воздействий.
51. Модели правового регулирования в сфере обеспечения безопасности КИИ.
52. Невластные субъекты обеспечения безопасности КИИ, их правовой статус.
53. Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами.
54. Сравнительно-правовой анализ предлагаемых экономических моделей распределения издержек по обеспечению безопасности КИИ.

5.4 Вопросы для самостоятельного изучения по очной форме обучения

Данный вид работы не предусмотрен учебным планом

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Фот, Ю. Д. Методы защиты информации : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст : электронный // Лань : электронно-библиотечная система.
2. Информационные технологии в процессе подготовки современного специалиста : сборник научных трудов. — Липецк : Липецкий ГПУ, 2019. — 235 с. — ISBN 978-5-907168-56-5. — Текст : электронный // Лань : электронно-библиотечная система.
3. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Информационные технологии в процессе подготовки современного специалиста : сборник научных трудов. — Липецк : Липецкий ГПУ, 2019. — 235 с. — ISBN 978-5-907168-56-5. — Текст : электронный // Лань : электронно-библиотечная система.
2. Волкова, В. Н. Системный анализ информационных комплексов : учебное пособие / В. Н. Волкова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 336 с. — ISBN 978-5-8114-5601-7. — Текст : электронный // Лань : электронно-библиотечная система.

6.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

7. Требования к материально-техническому и учебно-методическому содержанию дисциплины

7.1 Учебные аудитории для проведения учебных занятий по дисциплине

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованных специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

7.2 Перечень оборудования и технических средств обучения по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа-проектором, компьютером и учебной доской.

7.3 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

7.4 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант +

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Доцент, к.т.н. _____ Фот Юлия Дмитриевна

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 7 от 22.02.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна

Дополнения и изменения

в рабочей программе дисциплины Б1.В.10 Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) на 2021 - 2022 учебный год.

В программу вносятся следующие изменения: без изменений

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович