Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.6 Обеспечение безопасности объектов критической информационной инфраструктуры»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2023

Рабочая программа дисциплины «*Б1.Д.В.6 Обеспечение безопасности объектов критической информационной инфраструктуры*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "09" марта 2023г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* И.В. Влацкая *расшифровка подписи*

Исполнители:
Доцент *должность* *подпись* Ю.Д. Фот *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись Н.Н. Бигалиева *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации 154900

© Фот Ю.Д., 2023
© ОГУ, 2023

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: обучить студентов (слушателей) основным принципам построения и технологиям, используемых в настоящее время при создании подсистем обеспечения безопасности значимых объектов критической информационной инфраструктуры, рекомендованных международными организациями по стандартизации в области ИБ и российскими нормативными актами, и стандартами.

Курс позволяет дать понятие студентам основные представления об основах категорирования значимых объектов критической информационной инфраструктуры.

Задачами дисциплины являются: дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области ОБЗОКИИ; организации и порядка проведения категорирования ЗО КИИ и отработки документов по результатам категорирования.

В результате обучения студенты должны ознакомиться с:

системой организационно-распорядительных, нормативных и информационных документов ФСТЭК России и Ростехрегулирования, определяющих организацию, правила и порядок осуществления категорирования ЗО КИИ;

организацией лицензирования деятельности в области защиты информации,

организацией контроля выполнения требований федерального законодательства и приказов ФСТЭК России;

должны знать:

организационно-технические основы категорирования ЗО КИИ;

должны уметь:

проводить специальные категорирование ЗО КИИ;

должны владеть навыками:

выявления критических процессов на ЗО КИИ;

разработки технических документов по результатам категорирования ЗО КИИ.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.30 Организационное и правовое обеспечение информационной безопасности*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-1 Проектирование объектов в	ПК*-1-В-1 Умеет проектировать средства и системы информатизации в защищенном исполнении	**Знать:** нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ и АСУ ТП и П;

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
защищенном исполнении	ПК*-1-В-2 Владеет навыками проектирования систем защиты информации на объектах информатизации	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 Федерации и 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; 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; 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; цели, задачи, основные принципы организации государственного контроля в области обеспечения безопасности значимых объектов КИИ; порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ; **Уметь:** формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциаль-

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		ных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации; обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ; определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ; 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; 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 работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов КИИ; навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами; навыками разработки организационно-распорядительных документов по безопасности значимых объектов КИИ; эксплуатации системы безопасности значимого объекта КИИ; навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ; навыками проведения работ по контролю состояния безопасности объектов КИИ.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**60,25**	**60,25**
Лекции (Л)	30	30
Практические занятия (ПЗ)	30	30
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата;* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю.*	**47,75**	**47,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 10 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основы обеспечения безопасности КИИ Российской Федерации.	12	4	4		4
2	Категорирование объектов КИИ	22	6	6		10
3	Обеспечение безопасности значимых объектов КИИ	20	6	6		8
4	Контроль за обеспечением безопасности значимого объекта КИИ	8	2	2		4
5	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)	8	2	2		4
6	Обеспечение защиты информации в АСУ ТП КИИ	10	2	2		6
7	Аудит безопасности критической инфраструктуры.	20	6	6		8
8	Сравнительный анализ подходов к регулированию критической информационной инфраструктуры других стран	8	2	2		4
	Итого:	108	30	30		48
	Всего:	108	30	30		48

4.2 Содержание разделов дисциплины

Раздел №1. Основы обеспечения безопасности КИИ Российской Федерации.

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.

Раздел № 2. Категорирование объектов КИИ

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 информационной инфраструктуры, подлежащих категорированию.

Категорирование объектов критической информационной инфраструктуры. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозы безопасности информации 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 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

Требований 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 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

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 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. 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)

Перечень информации, представляемой в ГосСОПКА и Порядок представления информации в ГосСОПКА. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).

Раздел №6. Обеспечение защиты информации в АСУ ТП КИИ

Обследование АСУ ТП. Разработка требований по обеспечению безопасности информации в АСУ ТП. Разработка концепции ОБИ в АСУ ТП. Разработка Технического задания на создание си-

стемы защиты АСУ ТП. Проектирование системы защиты АСУ ТП. Внедрение системы защиты АСУ ТП. Разработка комплекта организационно-распорядительной документации, регламентирующей процессы защиты АСУ ТП.

Раздел №7. Аудит безопасности критической инфраструктуры.

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 классификация информационно-технических воздействий. Оборонительные информационно-технические воздействия. Обеспечивающие информационно-технические воздействия. Атакующие информационно-технические воздействия. Классификация основных средств информационно-технических воздействий.

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

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.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Введение в безопасность объектов критической информационной инфраструктуры.	2
2	1	Правовые основы обеспечения безопасности КИИ Российской Федерации.	2
3	2	Правила категорирования объектов КИИ. Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ.	2
4	2	Построение модели угроз и нарушителей объектов КИИ.	2
5	2	Категорирование объектов критической информационной инфраструктуры. Оформление и передача в ФСТЭК России результатов категорирования.	2
6	3	Требований по обеспечению безопасности значимых объектов КИИ РФ.	2
7	3	Система безопасности значимого объекта КИИ.	2
8	3	Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ	2
9	4	Контроль за обеспечением безопасности значимого объекта КИИ	2
10	5	Перечень информации, представляемой в ГосСОПКА и Порядок представления информации в ГосСОПКА.	2
11	6	Обследование АСУ ТП. Определение класса защищенности АСУ ТП. Проектирование системы защиты АСУ ТП.	2
12	7	Этапы проведения аудита. Практические особенности проведения аудита КИИ.	2
13,14	7	Тестирование как один из основных типов аудита критической информационной инфраструктуры. Тестирование	4

№ занятия	№ раздела	Тема	Кол-во часов
		критической инфраструктуры специальными информационно-техническими воздействиями. Тестирование критической инфраструктуры специальными информационно-психологическими воздействиями	
15	8	Сравнительный анализ подходов к регулированию критической информационной инфраструктуры других стран	4
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Организационно-правовое обеспечение информационной безопасности: учебное пособие. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. / Под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

2. Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157086 (дата обращения: 09.03.2023). — Режим доступа: для авториз. пользователей.

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. — URL: https://e.lanbook.com/book/167606 (дата обращения: 09.03.2023). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1. Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180100 (дата обращения: 09.03.2023). — Режим доступа: для авториз. пользователей.

2. Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие / О. В. Литвиненко ; RU. — Новосибирск : СибГУТИ, 2021. — 63 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/257321 (дата обращения: 09.03.2023). — Режим доступа: для авториз. пользователей.

3. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 09.03.2023). — Режим доступа: для авториз. пользователей.

4. Риск-модели информационной безопасности : учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2021. — 79 с. — ISBN 978-5-7641-1578-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/191006 (дата обращения: 09.03.2023). — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

Журналы:

- «Информационная безопасность»;
- «Вестник информационной безопасности»;

- «Проблемы информационной безопасности. Компьютерные системы».

5.4 Интернет-ресурсы

1. http://www.fsb.ru – сайт ФСБ РФ
2. http://www.fstec.ru – сервер ФСТЭК РФ
3. http://www.gov.ru – сервер органов государственной власти РФ
4. http://www.minsvyaz.ru – сайт министерства информационных технологий и связи РФ
5. http://www.scrf.gov.ru – сайт Совета Безопасности РФ
6. www.consultant.ru – Консультант плюс
7. https://gost.ru – Росстандарт
8. http://docs.cntd.ru – Электронный фонд правовой и нормативно-технической документации
9. http://www.securrity.ru – Сайт Информационная безопасность
10. https://www.securitylab.ru – Информационный портал по информационной безопасности
11. https://securelist.ru/ - Сетевая штаб-квартира экспертов «Лаборатории Касперского»
12. https://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle
13. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК: Защита информации.
14. https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii - «Coursera». Курсы, МООК: Методы и средства защиты информации
15. https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti - «Coursera». Курсы, МООК: Менеджмент информационной безопасности
16. https://www.intuit.ru/studies/courses/3648/890/info – «Интуит. Национальный открытый университет» Курсы, МООК: Аттестация объектов информатизации по требованиям безопасности информации.
17. https://www.intuit.ru/studies/courses/3601/843/info - «Интуит. Национальный открытый университет» Курсы, МООК: Информационное право: Информация.
18. https://openedu.ru/course/ITMOUniversity/INTPRO/- «Открытое образование» Курсы, МООК: Правовые основы защиты интеллектуальной собственности.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

а) программно- аппаратное обеспечение:

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021.
2. Пакет офисных приложений LibreOffice[1]
3. Программная система для организации видео-конференц-связи Webinar.ru

б) базы данных, информационно-справочные и поисковые системы:

1. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2023]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe
2. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2023]. – Режим доступа к системе в сети ОГУ для установки системы: \\fileserver1\!CONSULT\cons.exe
3. http://edu.garant.ru/garant/study/ - Интернет-версия ГАРАНТ-Образование, Система ГАРАНТ для студентов, аспирантов и преподавателей

1 Включает в себя текстовый процессор для всех видов документов Writer, табличный процессор Calc, программу для создания презентаций Impress, векторный графический редактор для создания блок-схем и диаграмм Draw, редактор формул Math, компонент, предназначенный для создания баз данных Base.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.