Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«31» августа 2021 г.

Наименование дисциплины (модуля) Б1.В.ДВ.02.02 Техническая защита объектов критической информационной инфраструктуры
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки Техническая защита информации
Квалификация выпускника бакалавр
Форма обучения очная

Согласовано с УМК физического факультета

Протокол №308 от «31»августа 2021 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 1 от «30» августа 2021 г.

И.О. зав. кафедрой _____ Колесник С.Н.

2021 г.

Содержание

стр.

I. Цели и задачи дисциплины (модуля):

Цели: Целями освоения дисциплины являются формирование у студентов системных знаний по обеспечению информационной безопасности критической информационной инфраструктуры, а также практических навыков по разработке и реализации планов реагирования на компьютерные инциденты.

Задачи:

1.Формирование системных знаний о значимых объектах критической информационной инфраструктуры, а также методах и средствах обеспечения их безопасности.

2. Изучение нормативно-правовых актов по безопасности критической информационной инфраструктуры.

3. Изучение методов оценки уровня защищенности (аудита) систем и сетей и содержащейся в них информации.

4. Освоение необходимых знаний по проведению категорирования объектов критической информационной инфраструктуры.

5. Формирование умений и знаний по проведению оценки угроз безопасности информации на объектах критической информационной инфраструктуры.

6. Изучения механизма проведения инвентаризации систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств.

7. Освоение методов организации и планирования мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина (модуль) Б1.В.ДВ.04.02 Техническая защита объектов критической информационной инфраструктуры.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б1.О.27 Защита операционных систем; Б1.О.36 Программно-аппаратные средства защиты информации.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенции ПК-1;

ПК-3 в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки (специальности) 10.03.01 Информационная безопасность:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-1 Способен проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации.	$ИДК_{ПК1.1}$ Проводит специальные исследования на побочные электромагнитные излучения и наводок технических средств обработки информации	Знать: методологию проведения специальных исследований на побочные электромагнитные излучения и наводок технических средств обработки информации Уметь: формировать требования к проведению специальных исследования на побочные электромагнитные излучения. Владеть: навыками проведения специальных исследования на побочные электромагнитные излучения и наводок средств обработки информации.
	$ИДК_{ПК1.2}$ Выбирает методики исследования на побочные	Знать: методологию и основные принципы исследования на побочные

	электромагнитные излучения и наводок технических средств обработки информации	электромагнитные излучения и наводки технических средств обработки информации. Уметь: Применять методики исследования на побочные электромагнитные излучения и наводок технических средств обработки информации Владеть: навыками выбора методик исследований на побочные электромагнитные излучения и наводки технических средств обработки информации
ПК-3. Способен проводить контроль защищенности акустической речевой информации от утечки по техническим каналам	ИДК$_{ПК3.1}$ Проводит контроль защищенности акустической речевой информации от утечки по техническим каналам	Знать: методологию проведения защищенности акустической речевой информации от утечки по техническим каналам Уметь: формировать требования к проведению контроля защищенности акустической речевой информации от утечки по техническим каналам Владеть: навыками проведения контроля защищенности акустической речевой информации от утечки по техническим каналам.
	ИДКПК3.2 Выбирает методики контроля защищенности акустической речевой информации от утечки по техническим каналам	Знать: способы выбора методик проведения защищенности акустической речевой информации от утечки по техническим каналам Уметь: формировать требования к проведению контроля защищенности акустической речевой информации от утечки по техническим каналам Владеть: навыками выбора методик проведения контроля защищенности акустической речевой информации от утечки по техническим каналам.

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единиц, 144 часов,

Форма промежуточной аттестации: зачет

4.1 Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости/ Форма промежуточной аттестации (по семестрам)
					Контактная работа преподавателя с обучающимися			Самостоятельная работа (в том числе, внеаудиторная СР, КСР)	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	**Раздел 1. Основы обеспечения безопасности значимых объектов КИИ**	8					0.2		
1.1	Правовые основы обеспечения безопасности КИИ Российской Федерации	8	15	3	3	8		4	
1.2	Угрозы безопасности информации, обрабатываемой на объектах КИИ	8	15	4	3	8		4	Защита ЛР

2.0.	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ**	8					0.4		
2.1.	Категорирование объектов КИИ	8	17	5	3	10		4	Защита ЛР
2.3.	Требования по обеспечению безопасности значимых объектов КИИ	8	17	5	3	10		4	
2.4.	Система безопасности значимого объекта КИИ	8	19	5	3	10		6	
2.5.	Стадии (этапы) работ по созданию системы безопасности	8	19	5	3	10		6	Защита ЛР
3.0	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ**	8					0.4		
3.1.	Контроль за обеспечением безопасности значимого объекта КИИ	8	21	5	4	10		7	Защита ЛР
2.5	**Зачет**	8							Тестирование
					22	66		35	

. работы (в том числе КСР) обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Проработка лекционного материала по теме «Правовые основы обеспечения безопасности КИИ Российской Федерации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	1 -2 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к практическому занятию по теме «Угрозы безопасности информации, обрабатываемой на объектах КИИ»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	3-4 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к практическому занятию по теме «Категорирование объектов КИИ»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	5-6 неделя	4	Устный опрос	Из списка литературы, конспект

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Подготовка к практическому занятию по теме «Требования по обеспечению безопасности значимых объектов КИИ»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	7-8 неделя	4	Устный опрос	Из списка лителатуры, конспект
8	Подготовка к практическому занятию по теме «Система безопасности значимого объекта КИИ»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	9 неделя	6	Устный опрос	Из списка лителатуры, конспект
8	Подготовка к практическому занятию по теме «Стадии (этапы) работ по созданию системы безопасности»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	10 неделя	6	Устный опрос	Из списка лителатуры, конспект
8	Подготовка к практическому занятию по теме «Контроль за обеспечением безопасности значимого объекта КИИ»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	11 неделя	7	Устный опрос	Из списка лителатуры, конспект

4.3. Содержание учебного материала

Т 1. Правовые основы обеспечения безопасности КИИ Российской Федерации
Т 2. Угрозы безопасности информации, обрабатываемой на объектах КИИ
Т3. Категорирование объектов КИИ
Т4. Требования по обеспечению безопасности значимых объектов КИИ
Т5. Система безопасности значимого объекта КИИ
Т6. Стадии (этапы) работ по созданию системы безопасности
Т7. Контроль за обеспечением безопасности значимого объекта КИИ

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы)*
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	Т1.	Правовые основы обеспечения безопасности КИИ Российской Федерации	4	3	Письменный текущий контроль. Защита ПР,ЛР	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$
2	Т2.	Угрозы безопасности информации, обрабатываемой на объектах КИИ	4	3	Письменный текущий контроль. Защита ПР,ЛР	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$
3	Т3.	Категорирование объектов КИИ	4	3	Письменный текущий контроль. Защита ПР,ЛР	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$
4	Т4.	Требования по обеспечению безопасности значимых объектов КИИ	4	3	Письменный текущий контроль. Защита ПР,ЛР	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$
5	Т5.	Система безопасности значимого объекта КИИ	6	4	Письменный текущий контроль. Защита ПР,ЛР	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$
6	Т6.	Стадии (этапы) работ по созданию системы безопасности	6	3	Письменный текущий контроль. Защита ПР,ЛР	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$
7	Т7.	Контроль за обеспечением безопасности	7	3	Письменный текущий контроль.	ИДК$_{ПК1.1}$ ИДК$_{ПК1.2}$ ИДК$_{ПК3.1}$

		значимого объекта КИИ			Защита ПР,Лр	

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	**2**	**3**	**4**	**5**
1	Т1. Правовые основы обеспечения безопасности КИИ Российской Федерации	Осмысление материала лекций. Подготовка к ПР.1.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$
2.	Т2.Угрозы безопасности информации, обрабатываемой на объектах КИИ	Осмысление материала лекций. Подготовка к ЛР.1.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$
3.	Т3.Категорирование объектов КИИ	Осмысление материала лекций. Подготовка к ПР2.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$
4.	Т4.Требования по обеспечению безопасности значимых объектов КИИ	Осмысление материала лекций. Подготовка к ЛР2.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$
5.	Т5.Система безопасности значимого объекта КИИ	Осмысление материала лекций. Подготовка к ЛР3.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$
6.	Т6.Стадии (этапы) работ по созданию системы безопасности	Осмысление материала лекций. Подготовка к ЛР4.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$
7.	Т7Контроль за обеспечением безопасности значимого объекта КИИ	Осмысление материала лекций. Подготовка к ЛР.5.	ПК-1. ПК-3	$ИДК_{ПК1.1}$ $ИДК_{ПК1.2}$ $ИДК_{ПК3.1}$

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа бакалавров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой бакалавр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи.

На самостоятельную работу выносятся следующие вопросы и задания по темам дисциплины:

Т1. Правовые основы обеспечения безопасности КИИ Российской Федерации

Т 2. Угрозы безопасности информации, обрабатываемой на объектах КИИ

Т3. Категорирование объектов КИИ

Т4. Требования по обеспечению безопасности значимых объектов КИИ

Т5. Система безопасности значимого объекта КИИ

Т6. Стадии (этапы) работ по созданию системы безопасности

Т7. Контроль за обеспечением безопасности значимого объекта КИИ.

Контроль самостоятельной работы проводится на практических занятиях и при защите лабораторных работ.

4.4. Примерная тематика курсовых работ (проектов) не предусмотрено

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Электронная информационно-образовательная среда университета обеспечивает доступ к электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочей программе дисциплины (модуля).

Библиотечный фонд укомплектован печатными зданиями из расчета не менее 0,25 экземпляра каждого из изданий на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль).

1. Технические средства и методы защиты информации. Технические средства и методы защиты информации. Учебно-практическое пособие. Москва: Евразийский открытый ин-т, 2011 100% онлайн. https://search.rsl.ru/ru/record/01006553324

б) периодические издания

в) список авторских методических разработок:

г) базы данных, информационно-справочные и поисковые системы

1. Научная библиотека ИГУ *http://library.isu.ru/ru/resources/edu_resources/index.html*

2. БД книг и продолжающихся изданий http://ellibnb.library.isu.ru/cgi-bin/irbis64r_15/cgiirbis_64.htm?LNG=&C21COM=F&I21DBN=IRCAT&P21DBN=IRCAT

3. Электронный читальный зал «БиблиоТех» https://isu.bibliotech.ru/.

4. Электронная библиотечная система «Издательство «Лань» http://e.lanbook.com.

5. Электронная библиотечная система «РУКОНТ» http://rucont.ru.

VI.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Учебно-лабораторное оборудование:

Класс ЭВМ, аудитория 323А, оснащенная вычислительной техникой, специальным ПО и свободным доступом в сеть Internet.

6.2. Программное обеспечение:

1. ABBY PDF Transformer 3.0 Пакет из 10 неименных лицензий Per Seat (10лиц.) EDU. Код позиции: AT30-1S1P10-102 Котировка № 03-165-11 от 23.11.2011. Бессрочно.
2. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmc. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.
3. WinPro10 Rus Upgrd OLP NL Acdmc. Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия № 68203568. Бессрочно.
4. Kaspersky Free (ежегодно обновляемое ПО). Условия использования по ссылке: http://www.kaspersky.ru/free-antivirus/ . Бессрочно.

6.3. Технические и электронные средства:

Мультимедийный проектор, экран (по необходимости), меловая или маркерная доска.

VII.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Практические занятия проводятся в интерактивной форме. Лабораторные работы проводятся с использованием ПЭВМ с последующей защитой.

VIII.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ6, при защите лабораторных работ ЛР1-ЛР3. Текущий контроль направлен на выявление сформированности компетенции ПК-1.

Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

За посещение одного вида занятия дается 0,6 балла (25 занятий (Л+Пз+ЛР)*0,6 балла = 15 баллов), максимальное количество баллов за письменный контроль на СКР – 5 баллов, за Пз – 54 баллов (6 летучек *5 балла= 30 баллов, решение задач у доски или самостоятельное досрочное решение всех задач, выносимых на ПЗ – 6 занятий*4 балла=24 баллов), лабораторные работы (ЛР) – 30 баллов (3*ЛР*10 баллов=30 баллов).

Параметры оценочного средства для письменного текущего контроля и решения задачи у доски или самостоятельного досрочного решения всех задач, выносимых на ПЗ1-ПЗ6. Параметры оценочного средства для КСР.

Критерии оценки	Оценка / баллы			
	Отлично 5 баллов.	Хорошо 3,5 балла	Удовлетв. 2 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки. .	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок. .

Параметры оценочного средства для защиты лабораторных работ ЛР1-ЛР3

Критерии оценки	Оценка / баллы			
	Отлично 7-10 баллов	Хорошо 4-6 балла	Удовлетв. 1-3 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно оформлен отчет, сделаны выводы. При защите показано всестороннее и глубокое	В целом отчет оформлен корректно, сделаны выводы, но имеются незначительные недостатки. При защите студент	Отчет оформлен полностью. Имеются замечания по оформлению, выводы сделаны не полностью. При защите - суждения поверхностны,	Отчет не оформлен. Отчет оформлен со значительными замечаниями, выводы не полные, при защите студент с трудом

	знание материала.	показывает понимает материала, приводит примеры, но испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы.	содержат ошибки, примеры не приводятся, ответы на дополнительные вопросы не уверенные.	формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы .

Вопросы для письменного текущего контроля приведены ниже:

1. Объекты и субъекты. Права и обязанности субъектов КИИ.
2.Полномочия органов государственной власти Российской Федерации в обеспечения безопасности КИИ.
3.Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ.
5.Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ
6.Права и обязанности субъектов КИИ.
7.Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.
9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.
10. Правила и порядок категорирования объектов КИИ.
11. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.
12.Формирование комиссии по категорированию объектов КИИ Российской Федерации.
13.Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ.
14.Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управления, контроль и мониторинг критических процессов.
15. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение.
16. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.
17. Формирования перечня объектов КИИ Российской Федерации, подлежащих категорированию.
18.Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации.

19.Формирование сведений о результатах категорирования объектов КИИ,
20.Устанеовление требований по обеспечению безопасности значимого объекта КИИ.
21. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.
22. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.
23. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.
24. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.
25. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности.
26. Требования к созданию систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.
27. Требования к силам обеспечения безопасности значимого объекта КИИ.
28.Требования к организационно-распорядительным документам по безопасности значимого объекта КИИ.
29. Перечень необходимых документов в рамках создания систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.
30. Этапы жизненного цикла системы безопасности значимого объекта КИИ.
31. Стадии (этапы) работ по созданию системы безопасности значимого объекта КИИ.
32.Внедрение системы безопасности значимого объекта КИИ.
33. Контроль за обеспечением уровня безопасности значимого объекта КИИ.
34.Мониторинг событий безопасности и контроль за действиями персонала значимого объекта КИИ.
35.Оценка соответствия значимых объектов КИИ требованиям безопасности.
36. Документирование процедур и результатов контроля за обеспечением безопасности значимого объекта КИИ.
37. Ответственность за нарушения законодательства о безопасности КИИ Российской Федерации.

Перечень примерных вопросов для защиты лабораторных работ:

ЛР1.Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

ЛР2. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.

ЛР3. Правила и порядок категорирования объектов КИИ. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.

ЛР4.Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ. Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управления, контроль и мониторинг критических процессов.

ЛР5. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение. Устанеовление требований по обеспечению безопасности значимого объекта КИИ.

Перечень примерных вопросов для защиты практических работ:

ПР1. Полномочия органов государственной власти Российской Федерации в обеспечения безопасности КИИ. Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ. Права и обязанности субъектов КИИ.

ПР2. Внедрение системы безопасности значимого объекта КИИ. Контроль за обеспечением уровня безопасности значимого объекта КИИ. Мониторинг событий безопасности и контроль за действиями персонала значимого объекта КИИ. Оценка соответствия значимых объектов КИИ требованиям безопасности. Документирование процедур и результатов контроля за обеспечением безопасности значимого объекта КИИ. Ответственность за нарушения законодательства о безопасности КИИ Российской Федерации.

Оценочные средства для промежуточной аттестации (в форме зачета).

Форма промежуточного контроля – зачет. Зачет выставляется по итогам изучения дисциплины в течение семестра при условии положительных результатов защиты всех лабораторных работ, предусмотренных программой.

Промежуточная аттестация направлена на проверку сформированности компетенций ОПК-1 и проводится в форме тестирования. Для реализации промежуточного контроля используется балльно-рейтинговая система оценки, принятая в университете.

Зачет выставляется по сумме балов, полученных при изучении дисциплины.

Усвоение бакалавром изучаемой дисциплины максимально оценивается 100 баллами. Из них 90 баллов обучающийся может набрать в течение семестра и от 0 до 10 баллов могут быть даны в качестве «премиальных» баллов за активные формы работы, высокое качество выполненных лабораторных и т.д.

Параметры оценочного средства для аттестации в форме зачета.

Итоговый семестровый рейтинг	Академическая оценка
0-59 баллов	«не зачтено»
60-100 баллов	«зачтено»

Материалы для проведения текущего и промежуточного контроля знаний студентов:

Пример теста для проведения промежуточной аттестации в форме зачета

Вариант 1

1. Безопасность критической информационной инфраструктуры:

а) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак:

б) обеспечение безопасного уровня защиты информации для обеспечения устойчивого функционирования критической информационной инфраструктуры

в) состояние защиты информации критической информационной инфраструктуры обеспечивающее её устойчивое функционирование.

2. Значимый объект критической информационной инфраструктуры:

а), объект критической информационной инфраструктуры который включен в реестр значимых объектов критической информационной инфраструктуры;

б). объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;
в). объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости

3. Объекты критической информационной инфраструктуры:

а). объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия с автоматизированными системами управления;
б). объекты информационной инфраструктуры, прошедшие процедуру категорирования;
в). информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

4. Принципами обеспечения безопасности критической информационной инфраструктуры являются:

а). законность, непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;
б). приоритет предотвращения компьютерных атак, законность;
в). законность, непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры, приоритет предотвращения компьютерных атак.

5. Категорирование объекта критической информационной инфраструктуры:

а). процедура установления объекту критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения;
б). установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений;
в). установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

6. **Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:**

а). предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
б). недопущение воздействия на технические средства обработки информации, обеспечение функционирования значимого объекта критической информационной инфраструктуры;
3) восстановление функционирования значимого объекта критической информационной инфраструктуры.

7. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение:

а). отсутствие доступа к государственной услуге в течении, которого государственная услуга может быть недоступна для получателей;
б). причинение ущерба жизни и здоровью людей;
в). прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны.

8. Максимальный срок категорирования не должен превышать;

а). одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений);
б). двух лет со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений);
в). 6 месяцев со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений).

9. Создание и функционирование систем безопасности должно быть направлено на;

а). обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак;
б). обеспечение защиты значимых объектов критической информационной инфраструктуры от компьютерных атак;
в). обеспечение функционирования значимых объектов критической информационной инфраструктуры при возникновении угроз информационной безопасности.

10. Системы безопасности должны обеспечивать:

а). восстановление функционирования системы безопасности значимых объектов критической информационной инфраструктуры;
б). недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов критической информационной инфраструктуры
в). устойчивое функционирование системы безопасности значимых объектов критической информационной инфраструктуры.

11. К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся:

а). подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры;
б). подразделения (работники), участвующие в подготовке плана безопасности значимого объекта критической информационной инфраструктуры.
в). подразделения (работники), эксплуатирующие значимые объекты критической информационной инфраструктуры.

12. Организационно-технические меры по обеспечению безопасности значимого объекта должны включать:

а). анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);
б) разработку технического задания на создание системы безопасности значимого объекта;
в) разработку рабочей (эксплуатационной) документации на систему защиты

13. Модель угроз безопасности информации должна содержать:

а). краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;
б). числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;
в). краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации.

14. Кем осуществляется государственный контроль за обеспечением уровня безопасности значимого объекта КИИ осуществляет;

а). ФСБ;
б). ФСТЭК;
в). Органами прокуратуры РФ.

15. Ответственность за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

а). дисциплинарная;
б). дисциплинарная и административная;
в). дисциплинарная, гражданско-правовая, административная и уголовная ответственность.

Разработчики:

Доцент кафедры РФиРЭ _____ Серёдкин С.П.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «30» августк 2021 г. протокол № 1

И.О. зав. кафедрой Колесник С.Н.