ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1. Б.2. 05 Обеспечение информационной безопасности на критически важных объектах

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Квалификация выпускника специалист

Форма обучения очная

1. Цели освоения дисциплины:

- сформировать знания о критически важных объектах (КВО) и информационных системах (КВИС) как об объектах защиты, об их специфике и особенностях, по сравнению с традиционными объектами и информационными системами;
- проанализировать основные отечественные и зарубежные нормативные правовые документы, а также методические рекомендации в области безопасности КВО и КВИС;
- изучить факторы, затрудняющие обеспечение должного уровня защищенности КВО и КВИС;
- изучить возможные источники угроз, угрозы и объекты атаки КВИС, а также наиболее уязвимые с точки зрения информационной безопасности компоненты критически важных объектов, научиться грамотно составлять модель нарушителя и модель угроз в соответствии с особенностями критически важных объектов (КВО), бизнес-процессы которых поддерживает КВИС;
- изучить особенности построения системы защиты информации КВИС, мероприятия, направленные на повышение уровня защищенности КВО, а также специализированные средства защиты информации автоматизированной системы управления технологическими и производственными процессами критически важных объектов (АСУ ТП КВО);
- изучить способы обеспечения целостности и доступности в критически важных информационных системах, а также современные отечественные и зарубежные средства резервирования ресурсов и данных;
- изучить элементы типовой структуры, защищенной критически важной информационной системы и способы их реализации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Обеспечение информационной безопасности на критически важных объектах» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Обеспечение информационной безопасности на критически важных объектах» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОК-4	Правоведение
ПСК-3.1	Основы радиотехники

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОК-4	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПСК-3.1	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

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

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-4 способность использовать основы правовых знаний в различных сферах деятельности	1 этап - сущность и содержание основных отраслей российского права; - нормативные правовые акты; - правовую терминологию; - практические свойства правовых знаний;	1 этап - ориентироваться в системе российского законодательства и нормативных правовых документов, регламентирующих профессиональную деятельность;	1 этап - ориентироваться в системе российского законодательства и нормативных правовых документов, регламентирующих профессиональную деятельность;
ОК-4 способность использовать основы правовых знаний в различных сферах деятельности	2 этап- основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации.	2 этап- применять правовые нормы в профессиональной и общественной деятельности; - логически верно, аргументировано и ясно строить устную и письменную речь; - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности.	2 этап - применять правовые нормы в профессиональной и общественной деятельности; - логически верно, аргументировано и ясно строить устную и письменную речь; - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности.
ПСК-3.1 способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных	Этап 1: основные информационные технологии	Этап 1: разрабатывать и использовать особенности информационных технологий	Этап 1: использования информационных технологий при организации системы защиты

системах критически важных объектов			
ПСК-3.1 способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	Этап 2: автоматизированные системы, применяемые при организации защиты информации	Этап 2: использовать особенности автоматизированных систем при организации системы защиты	Этап 2: навыки использования особенностей автоматизированных систем при организации системы защиты

4. Объем дисциплины

Объем дисциплины «Обеспечение информационной безопасности на критически важных объектах» составляет 2 зачетные единицы (72 академических часа), распределение объема 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

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 8	
				КР	СР
1	**2**	**3**	**4**	**5**	**6**
1	Лекции (Л)	18		18	
2	Лабораторные работы (ЛР)	34		34	
3	Практические занятия (ПЗ)				
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)				
10	Подготовка к занятиям (ПкЗ)		18		18
11	Промежуточная аттестация	2		2	
12	Наименование вида промежуточной аттестации	x	x	зачет	
13	Всего 72	54	18	54	18

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	**Тема 1** Основные сведения о КВО и КВИС как об объектах защиты	8	2					x			2	x	ОК-4 ПСК-3.1
2.	**Тема 2** Нормативная правовая база РФ в области обеспечения безопасности КВО	8	2	6				x			2	x	ПСК-3.1
3.	**Тема 3** Архитектура сети критически важного объекта и ее уязвимости	8	2					x			2	x	ОК-4 ПСК-3.1
4.	**Тема 4** Модель угроз критически важного объекта	8	2	12				x			2	x	ПСК-3.1
5.	**Тема 5** Специальные средства защиты ИТ-инфраструктур КВО	8	2	2				x			2	x	ОК-4 ПСК-3.1
6.	**Тема 6** Комплексная защита критически важных объектов	8	2	2				x			2	x	ПСК-3.1

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
7.	**Тема 7** Средства защиты информации, использующиеся на критически важных объектах и в автоматизированных системах критически важных объектов	8	2	4				x			2	x	ОК-4 ПСК-3.1
8.	**Тема 8** Разработка и реализация планов реагирования и восстановления после инцидентов безопасности критически важного объекта	8	2	2				x			2	x	ПСК-3.1
9.	**Тема 9** Построение системы защиты информации на критически важном объекте.	8	2	6				x			2	x	ОК-4 ПСК-3.1
10.	**Контактная работа**		**18**	**34**				**x**				**2**	**x**
11.	**Самостоятельная работа**										**18**		**x**
12.	**Объем дисциплины в семестре**		**18**	**34**							**18**	**2**	**x**
13.	**Всего по дисциплине**	**x**	**18**	**34**							**18**	**2**	**x**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Основные сведения о КВО и КВИС как об объектах защиты	2
Л-2	Нормативная правовая база РФ в области обеспечения безопасности КВО	2
Л-3	Архитектура сети критически важного объекта и ее уязвимости	2
Л-4	Модель угроз критически важного объекта	2
Л-5	Специальные средства защиты ИТ-инфраструктур КВО	2
Л-6	Комплексная защита критически важных объектов	2
Л-7	Средства защиты информации, использующиеся на критически важных объектах и в автоматизированных системах критически важных объектов	2
Л-8	Разработка и реализация планов реагирования и восстановления после инцидентов безопасности критически важного объекта	2
Л-9	Построение системы защиты информации на критически важном объекте	2
Итого по дисциплине		18

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лабораторной работы	Объем, академические часы
ЛР-1	Изучение «Доктрины информационной безопасности».	2
ЛР-2-3	Изучение руководящих документов ФСТЭКРФ.	4
ЛР-4-5	Изучение «Базовой модели угроз безопасности информации в ключевых системах информационной инфраструктуры»	4
ЛР-6-7	Изучение «Методики определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»	4
ЛР-8-9	Изучение «Общих требований по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»	4
ЛР-10	Категорирование критически важных объектов	2
ЛР-11	Оценка уязвимости объектов информационной и телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий.	2
ЛР-12	Разработка требований к оформлению концепции обеспечения информационной безопасности объекта.	2

ЛР-13	Разработка требований безопасности при взаимодействии с открытыми (публичными) информационными системами и сетями.	2
ЛР-14	Определение конкретных способов реагирования на инциденты различной длительности и тяжести.	2
ЛР-15	Определение информационных и технических ресурсов, подлежащих защите	2
ЛР-16-17	Разработка рекомендаций по выбору средств защиты информации	4
Итого по дисциплине		34

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.

2.Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Хорев, П. Б. Программно-аппаратная защита информации Текст учеб. пособие для вузовпонаправлению10.03.01"Информ. безопасность" П. Б. Хорев. -2-е изд., испр. и доп. -М.: Форум :ИНФРА-М, 2017. -351с. ил.

2. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях Текст В. Ф. Шаньгин. -М.: ДМК ПРЕСС, 2012. -592с. ил. …

6.3 Методические материалы для обучающихся по освоению дисциплины

Электронное учебное пособие, включающее:

- конспект лекций;
- методические материалы по выполнению лабораторных работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие, включающее:

-методические рекомендации по подготовке к занятиям.

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

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

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.analitika.info Средства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации.
2. http://www.fstec.ru Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
3. http://www.fsb.ru Федеральная Служба безопасности Российской Федерации.

4. http://clsz.fsb.ru Центр по лицензированию, сертификации и защите государственной тайны ФСБ России.

5. http://www.consultant.ru Общероссийская Сеть распространения правовой информации КонсультантПлюс

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение лабораторных работ

Номер ЛР	Тема лабораторной работы	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ЛР-1	Изучение «Доктрины информационной безопасности».	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-2	Изучение руководящих документов ФСТЭКРФ.	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-3	Изучение «Базовой модели угроз безопасности информации в ключевых системах информационной инфраструктуры»	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-4	Изучение «Методики определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-5	Изучение «Общих требований по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-6	Категорирование критически важных объектов	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства

ЛР-7	Оценка уязвимости объектов информационной и телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий.	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-8	Разработка требований к оформлению концепции обеспечения информационной безопасности объекта.	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-9	Разработка требований безопасности при взаимодействии с открытыми (публичными) информационными системами и сетями.	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-10	Определение конкретных способов реагирования на инциденты различной длительности и тяжести.	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-11	Определение информационных и технических ресурсов, подлежащих защите	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-12	Разработка рекомендаций по выбору средств защиты информации	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства

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, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

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

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ № 1509 от 01.12.2016

Разработал(и): _____ Е. В. Каменева