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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.06.02 Системы обнаружения вторжений

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:

- изучение основных принципов, методов и средств защиты информации в процессе ее обработке, хранении и передачи с использованием компьютерных средств в информационных системах;

- теоретическое и практическое обучение студентов методам и средствам выявления и блокирования каналов утечки информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Системы обнаружения вторжений» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Системы обнаружения вторжений» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-3	Теория автоматов Разработка и эксплуатация защищенных автоматизированных систем Безопасность систем баз данных Безопасность операционных систем
ПК-8	Информатика. Курс полного общего школьного образования
ПК-11	Основы информационной безопасности
ПК-12	Информатика. Курс полного общего школьного образования
ПК-13	Разработка и эксплуатация защищенных автоматизированных систем
ПК-14	Метрология и электро-радиоизмерения Криптографические методы защиты информации
ПК-17	Информатика. Курс полного общего школьного образования
ПК-19	Информатика. Курс полного общего школьного образования
ПК-21	Информатика. Курс полного общего школьного образования
ПК-22	Основы информационной безопасности
ПК-23	Информатика. Курс полного общего школьного образования
ПК-27	Разработка и эксплуатация защищенных автоматизированных систем

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-3	Производственная научно-исследовательская работа Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-8	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-11	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-12	Управление информационной безопасностью Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста) Производственная (преддипломная) практика
ПК-13	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-14	Учебная практика по получению профессиональных умений , в том числе первичных умений и навыков научно-исследовательской деятельности Производственная практика по получению профессиональных умений и опыта профессиональной деятельности Производственная (преддипломная) практика Системы предотвращения утечек Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

ПК-17	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-19	Управление информационной безопасностью Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-21	Организационное и правовое обеспечение информационной безопасности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-22	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-23	Организационное и правовое обеспечение информационной безопасности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-27	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности 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
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 1 Принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных	Этап 1 Уметь реализовывать политику безопасности баз данных	Этап 1 Навыки выявления организационных, программно- аппаратных и технических угроз безопасности база данных
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 2 Средства обеспечения безопасности данных	Этап 2 Применять средства обеспечения безопасности данных	Этап 2 Навыки проведения анализа защищенности автоматизированных систем
ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 2: основные методы технико-экономического обоснования проектных решений	Этап 2: проводить технико-экономическое обоснование проектных решений	Этап 2: навыки технико- экономического обоснования проектных решений
ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы	Этап 1основные составляющие политики безопасности	Этап 1: разрабатывать политик у безопасности	Этап 1: навыки разработки политики безопасности
ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы	Этап 2: принципы разработки политики безопасности	Этап 2: применять комплексный подход к обеспечению информационной безопасности	Этап 2применения комплексного подхода к обеспечению информационной безопасности
ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-12 – способностью участвовать в проектировании и системы управле-	Этап 2: основные методы технико-экономического	Этап 2: проводить технико-экономическое	Этап 2: навыки технико- экономического обоснова-

ния информационно безопасностью автоматизированной системы	обоснования проектных решений	обоснование проектных решений	ния проектных решений
ПК-13 -способностью участвовать в проектировании средств защиты информации автоматизированной системы	Этап 1: знать принцип ы построения криптографических алгоритмов	Этап 1: уметь выполнять настройки по обслуживанию криптосистем	Этап 1: выполнения настроек по обслуживанию криптосистем;
ПК-13 -способностью участвовать в проектировании средств защиты информации автоматизированной системы	Этап 2: знать криптографические стандарты и их использование в информационных системах	Этап 2: уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием криптосистем	Этап 2: осуществления мер противодействия нарушениям сетевой безопасности с использованием криптосистем
ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации	Этап 1: разрабатывать методик у контрольных проверок технических средств защиты информации	Этап 1: навыки применения контрольных проверок
ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Этап 2: основные принципы работы технических средств защиты информации	Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 2: навыки оценки эффективности применении аппаратно-программных комплексов
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации	Этап 1: методику анализа информационной безопасности	Этап 1: разрабатывать методик у анализа информационной безопасности	Этап 1: разработки анализа информационной безопасности
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации	Этап 2: современные стандарты в области информационной безопасности	Этап 2: использовать стандарт ы в области информационной безопасности	Этап 2: использования стандартов в области информационной безопасности
ПК-19 – Способностью	Этап 1 Общие мето-	Этап 1 Умения	Этап 1 Навыки

разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	дологические принципы построения комплексных систем обеспечения информационной безопасности;	ми работы с нормативно-правовыми актами	участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
ПК-19– Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Этап 2 комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем;	Этап 2 Первичными навыкам и работы с основными средства ми обеспечения информационной безопасности	Этап 2 Навыки управления процессом реализации комплекса мер по обеспечению информационной безопасности
ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной без опасности автоматизированных систем	Этап 1: основные этапы оформления рабочей документации	Этап 1: разрабатывать основные рабочие документы	Этап 1: навыки разработки рабочих документов
ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной без опасности автоматизированных систем	Этап 2: основные нормативные и методические документы	Этап 2: применять нормативные документы в рабочей документации	Этап 2: навыки применения нормативных документов
ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	Этап 1основные составляющие политики безопасности	Этап 1: разрабатывать политику безопасности	Этап 1: навыки разработки политики безопасности
ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	Этап 2: принцип ы разработки политики безопасности	Этап 2: применять комплексный подход к обеспечению информационной безопасности	Этап 2:применения комплексного подхода к обеспечению информационной безопасности
ПК-23 – способностью формировать комплекс мер (правила, процедуры,	Этап 1: основные принципы администрирования	Этап 1: основные принципы администрирования	Этап 1: навыки администрирования подсистемы безопасности

методы)для защиты информации ограниченного доступа			
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	Этап2:современные инструментальные средства администрирования	Этап 2: современные инструментальные средства администрирования инструментальные средства администрирования подсистемы безопасности	Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Этап 1: основные меры по выполнения обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 2: разработки мер поддержки обеспечения информационной безопасности

4. Объем дисциплины

Объем дисциплины «Системы обнаружения вторжений» составляет 5 зачетных единиц (180 академических часов), 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 № 7		Семестр №8	
				КР	СР	КР	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Лекции (Л)	52		34		18	
2	Лабораторные работы (ЛР)						
3	Практические занятия (ПЗ)	50		32		18	
4	Семинары(С)						
5	Курсовое проектирование (КП)						
6	Рефераты (Р)						
7	Эссе (Э)						
8	Индивидуальные домашние задания (ИДЗ)						
9	Самостоятельное изучение вопросов (СИВ)		72		40		32
10	Подготовка к занятиям (ПкЗ)						
11	Промежуточная аттестация	6		2		4	
12	Наименование вида промежуточной аттестации	х	х	зачёт		экзамен	
13	Всего	108	72	68	40	40	32

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.	**Раздел 1 Введение в предмет**	**7**	**16**		**16**			**x**		**20**		**x**	**ПК-3 ПК-8 ПК-11**
1.1.	**Тема 1** Основные элементы технологий открытых информационных систем	7	8		8			x		10		x	ПК-3 ПК-8 ПК-11
1.2.	**Тема 2** Совместимость, переносимость и способность взаимодействовать открытых систем. Основные модели открытых систем	7	8		8			x		10		x	ПК-3 ПК-8 ПК-11
2.	**Раздел 2 Интранет как открытая система**	**7**	**18**		**18**			**x**		**20**		**x**	**ПК-12 ПК-13 ПК-14**
2.1.	**Тема 3** Уязвимость открытых систем на примере интранета. Базовые по-	7	8		8			x		8		x	ПК-12 ПК-13 ПК-14

№ 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
	нятия. Основные угрозы. Уязвимость архитектуры клиент-сервер												
2.2.	**Тема 4** Уязвимость открытых систем на примере интранета. Уязвимости системных утилит, команд, сервисов	7	6		6			х		6		х	ПК-12 ПК-13 ПК-14
2.3	**Тема 5** Уязвимости современных технологий программирования. Ошибки в ПО	7	4		4					6			ПК-12 ПК-13 ПК-14
3.	**Контактная работа**	**7**	**34**		**32**			**х**				**2**	**х**
4.	**Самостоятельная работа**	**7**								**40**			**х**
5.	**Объем дисциплины в семестре**	**7**	**34**		**32**					**40**		**2**	**х**
6	**Раздел 3 Обеспечение информационной безопасности в открытых системах**	**8**	**18**		**18**			**х**		**32**		**х**	**ПК-17 ПК-19 ПК-21 ПК-23**
6.1	**Тема 6** Принципы создания защищенных средств связи объектов в	8	8		8					12			ПК-17 ПК-19 ПК-21

№ 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
	открытых системах												ПК-23
6.2	**Тема 7** Политика безопасности открытых систем	8	6		6			х		10		х	ПК-17 ПК-19 ПК-21 ПК-23
6.3	**Тема 8** Управление безопасностью открытых систем	8	4		4			х		10		х	ПК-17 ПК-19 ПК-21 ПК-23
7.	**Контактная работа**	**8**	**18**		**18**			**х**				**4**	**х**
8.	**Самостоятельная работа**	**8**								**32**			**х**
9.	**Объем дисциплины в семестре**	**8**	**18**		**18**					**32**		**4**	**х**
10.	**Всего по дисциплине**	**х**	**52**		**50**					**72**		**6**	**х**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1-4	Введение в предмет. Базовые понятия	8
Л-5-9	Основные элементы технологий открытых информационных систем. Совместимость, переносимость и способность взаимодействовать открытых систем.	10
Л-10-13	Основные модели открытых систем. Интранет как открытая система.	8
Л-14-17	Уязвимость открытых систем на примере интранета. Основные угрозы.	8
Л-18-20	Уязвимость архитектуры клиент-сервер. Уязвимость открытых систем на примере интранета.	6
Л-21-22	Уязвимости системных утилит, команд, сервисов. Уязвимости современных технологий программирования. Ошибки в ПО	4
Л-23-24	Обеспечение информационной безопасности в открытых системах. Принципы создания защищенных средств связи объектов в открытых системах	4
Л-25-26	Политика безопасности открытых систем. Управление безопасностью открытых систем	4
Итого по дисциплине		52

5.2.2 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
ПЗ-1-4	Введение в предмет. Базовые понятия	8
ПЗ-5-8	Основные элементы технологий открытых информационных систем. Совместимость, переносимость и способность взаимодействовать открытых систем.	8
ПЗ-9-12	Основные модели открытых систем. Интранет как открытая система.	8
ПЗ-13-16	Уязвимость открытых систем на примере интранета. Основные угрозы.	8
ПЗ-17-19	Уязвимость архитектуры клиент-сервер. Уязвимость открытых систем на примере интранета.	6
ПЗ-20-21	Уязвимости системных утилит, команд, сервисов. Уязвимости современных технологий программирования. Ошибки в ПО	4
ПЗ-22-23	Обеспечение информационной безопасности в открытых системах. Принципы создания защищенных средств связи объектов в открытых системах	4
ПЗ-24-25	Политика безопасности открытых систем. Управление безопасностью открытых систем	4
Итого по дисциплине		50

5.2.3 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1	**Тема 1** Основные элементы технологий открытых информационных систем	Основные понятия и определения. Статистика вторжений на Web-ресурсы.	10
2	**Тема 2** Совместимость, переносимость и способность взаимодействовать открытых систем. Основные модели открытых систем	Проблемы обеспечения безопасности при удалённом доступе. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.	10
3	**Тема 3** Уязвимость открытых систем на примере интранета. Базовые понятия. Основные угрозы. Уязвимость архитектуры клиент-сервер	Обнаружение факта проведения и причин возникновения сетевой атаки подручными средствами Дидактическая единица: Общие сведения об IDS snort.	8
4	**Тема 4** Уязвимость открытых систем на примере интранета. Уязвимости системных утилит, команд, сервисов	Значение IDS для решения задач поиска злоумышленников в собственной ЛВС. Классификация, средства и методы защиты от атак.	6
5	**Тема 5** Уязвимости современных технологий программирования. Ошибки в ПО	Идентификация и аутентификация. Ознакомление с криптографическими системами. Экранирование, анализ защищенности.	6
6	**Тема 6** Принципы создания защищенных средств связи объектов в открытых системах	Виртуальные частные сети. Туннелирование. Сетевые уязвимости.	12
7	**Тема 7** Политика безопасности открытых систем	Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры. Особенности сетевого сканера Nessus.	10
8	**Тема 8** Управление безопасностью открытых систем	Защита программ от изучения. Защита от разрушающих программных воздействий.	10
Итого по дисциплине			72

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Защита информации в компьютерных системах и сетях. /В.Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592с.
2. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft/ С.А. Нестеров – М.: Национальный Открытый Университет «ИНТУИТ», 2009 – 375с.
3. Мельников В.В. Безопасность информации в автоматизированных системах – М.: Финансы и статистика, 2003. (Электронная библиотека)

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Иванова Н.Ю., Маняхина В.Г. Системное и прикладное программное обеспечение: Учебное пособие. – М.: МПГУ, 2011 – 202с.
2. Защита Windows от сбоев [Текст]/ А.С.Перетолчин. – Новосибирск: Сиб.унив.изд-во, 2008. – 108с
3. Операционная система UNIX: курс лекций. Учебное пособие / Г.В. Курячий. – М.: ИНТУИТ.РУ, Интернет-Университет Информационных Технологий, 2004. – 288с.
4. Введение в OracleSQL/В.В. Пржиялковский – М.: Национальный Открытый Университет «ИНТУИТ», 2011- 356с
5. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учеб. пособие/ О.Р.Лапонина; под ред. В.А.Сухомлина. – М.: Интернет-Ун-т Информ. Технологий, 2005. – 608с. [Книгафонд]
6. Межсетевое экранирование: Учебное пособие / О.Р. Лапонина. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лабораториязнаний, 2007. – 343.
7.

6.3 Методические материалы для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие включающее:

- конспект лекций;
- методические материалы по выполнению практических (семинарских) работ.

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

Электронное учебное пособие, включающее:

- методические рекомендации по самостоятельному изучению вопросов;
- 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. HP WebInspect.
2. SANS

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

1. http://e.lanbook.com/ - ЭБС
2. http://rucont.ru/ - ЭБС
3. http://elibrary.ru/defaultx.asp - ЭБС
4. http://www.rsl.ru Российская государственная библиотека (РГБ)
5. http://www.edu.ru/ - федеральный портал российского образования

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 практических работ

Номер ПЗ	Тема лабораторной работы	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ПЗ 1-16	Практические занятия в соответствии с рабочей программой	943 – Лаборатория технологии, методов программирования и программного обеспечения, 957 – Лаборатория аппаратных средств вычислительной системы.	ПЭВМ	Графический пакет 3ds Max OpenOffice

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, 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 от 1 декабря 2016 г. №1509.

Разработал(и):_____ Урбан В.А.

Оценочные материалы для проведения текущего контроля и промежуточной атте-

стации 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 от 1 декабря 2016 г. №1509.

Разработал(и):_____ Урбан В.А.