МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ / О.В. Юсупова
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.01.03 «Защита информационных ресурсов промышленных объектов»

Код и направление подготовки (специальность)	15.04.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Интеллектуальные системы мониторинга состояния сложных инфраструктурных объектов
Квалификация	Магистр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Автоматизация и управление технологическими процессами"
Кафедра-разработчик	кафедра "Автоматизация и управление технологическими процессами"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Самара 2022

Б1.В.01.03 «Защита информационных ресурсов промышленных объектов»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **15.04.04 Автоматизация технологических процессов и производств**, утвержденного приказом Министерства образования и науки РФ от № 1452 от 25.11.2020 и соответствующего учебного плана.

Разработчик РПД:

Профессор, доктор технических наук, профессор (должность, степень, ученое звание)	В.Н Якимов (ФИО)
Заведующий кафедрой	С.В. Сусарев, кандидат технических наук, доцент (ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	Я.Г Стельмах, кандидат педагогических наук (ФИО, степень, ученое звание)
Руководитель образовательной программы	С.В. Сусарев, кандидат технических наук, доцент (ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Место дисциплины (модуля) в структуре образовательной программы 4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 6
4.1 Содержание лекционных занятий 6
4.2 Содержание лабораторных занятий 7
4.3 Содержание практических занятий 7
4.4. Содержание самостоятельной работы 8
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю) 10
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения 11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 11
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) 12
9. Методические материалы 12
10. Фонд оценочных средств по дисциплине (модулю) 14

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
	ОПК-6 Способен осуществлять научно-исследовательскую деятельность, используя современные информационно-коммуникационные технологии, глобальные информационные ресурсы;	ОПК-6.2 Уметь использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности	Уметь использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности
Профессиональные компетенции			
Не предусмотрено	ПК-4 Способен разрабатывать теоретические модели, позволяющие модернизировать средства и системы автоматизации	ПК-4.2 Уметь составлять теоретическое описание моделей средств и систем автоматизации для последующей их модернизации в целях повышения эффективности процессов, производить анализ и обосновывать эффективность применения конкретных моделей	Уметь составлять теоретическое описание моделей средств и систем автоматизации с целью обеспечения защиты информационных ресурсов.
Универсальные компетенции			
Системное и критическое мышление	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Знать методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях	Знать методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях.
		УК-1.2 Уметь применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций	Уметь применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций.
		УК-1.3 Владеть методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач	Владеть методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ОПК-6			Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы; Инженерное предпринимательство; Научно-исследовательская работа
ПК-4		Компьютерные технологии в области автоматизации и управления; Мастерская инноваций (проектная мастерская); Техническое и информационное обеспечение систем управления сложными инфраструктурными объектами	Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы; Компьютерные технологии в управления объектами в области машиностроения; Мастерская инноваций (проектная мастерская); Методы и алгоритмы обработки сигналов при мониторинге сложных инфраструктурных объектов; Патентоведение; Прикладное программное обеспечение; Применение программируемых логических контроллеров в интеллектуальных системах мониторинга; Программные средства моделирования сложных инфраструктурных объектов; Программные средства проектного расчета надежности сложных инфраструктурных объектов; Проектирование единого информационного пространства предприятий; Производственная практика: преддипломная практика; Современные проблемы управления объектами в области машиностроения; Специальные системы управления в нефтегазопереработке и машиностроении; Учебная практика: ознакомительная практика
УК-1			Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы; Обеспечение безопасности сложных инфраструктурных объектов; Учебная практика: ознакомительная практика

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	1 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	16	16
Лекции	8	8
Практические занятия	8	8
Внеаудиторная контактная работа, КСР	2	2
Самостоятельная работа (всего), в том числе:	99	99
подготовка к практическим занятиям	64	64
подготовка к экзамену	35	35
Контроль	27	27
Итого: час	144	144
Итого: з.е.	4	4

4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Правовое обеспечение защиты информационных ресурсов	2	0	0	9	11
2	Методы и средства защиты информационных ресурсов	6	0	8	90	104
	КСР	0	0	0	0	2
	Контроль	0	0	0	0	27
	Итого	8	0	8	99	144

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	**Содержание лекции** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
1 семестр				

1	Правовое обеспечение защиты информационных ресурсов	Основы политики безопасности хранения и защиты информационных ресурсов.	Цели и задачи защиты информационных ресурсов. Субъекты и объекты правоотношений в области информационной безопасности. Политика безопасности.	2
2	Методы и средства защиты информационных ресурсов	Безопасность компьютерных технологий.	Угрозы информационной безопасности и их классификация. Источники и пути реализации угроз информационной безопасности. Иерархия угроз информационной безопасности. Структура и основные элементы модели нарушителя. Категории информационной безопасности.	2
3	Методы и средства защиты информационных ресурсов	Особенности информационной безопасности систем баз данных.	Понятие безопасности баз данных. Основные требования по безопасности, предъявляемые к базам данных. Угрозы безопасности баз данных. Простейшая модель безопасности баз данных. Предотвращение несанкционированного доступа к базам данных. Модель многоуровневой безопасности баз данных.	2
4	Методы и средства защиты информационных ресурсов	Основы безопасности информационных сетей.	Типовая корпоративная информационная сеть. Уровни инфраструктуры информационной сети. Источники уязвимости информационной сети. Классификация атак и типовой сценарий действий потенциальных нарушителей. Средства выявления уязвимостей узлов сетей и обнаружения атак на них.	2
			Итого за семестр:	**8**
			Итого:	**8**

4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

4.3 Содержание практических занятий

№ занятия	**Наименование раздела**	**Тема практического занятия**	**Содержание практического занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов / часов в электронной форме**
1 семестр				
1	Методы и средства защиты информационных ресурсов	Разработка и планирование мероприятий по обеспечению защиты объектов компьютерных систем от вероятных угроз.	Формулирование требований для анализа предметной области и ее анализ. Выделение активных объектов, которые производят и потребляют данные. Определение и моделирование процессов, которые преобразуют данные. Построение диаграммы потоков данных предметной области.	2

2	Методы и средства защиты информационных ресурсов	Основные механизмы защиты операционной системы MS WINDOWS.	Учетные записи и авторизация пользователей. Управление учетными записями. Разграничение доступа к объектам файловой системы. Разграничение доступа к системному реестру. Аудит использования привилегий, отслеживания процессов и системных событий. Контрольная точка 1. Устный опрос.	2
3	Методы и средства защиты информационных ресурсов	Программно-технические средства защиты компьютерных систем.	Защита памяти. Защита выполнения программ. Защита дисков. Анализ методов защиты дисков. Дисковые контроллеры. Средства защиты программного обеспечения с электронными ключами. Обзор элементной базы используемой для построения современных моделей электронных ключей.	2
4	Методы и средства защиты информационных ресурсов	Криптографическая защита компьютерной информации.	Разработка и исследование учебного варианта криптографической системы шифрования. Симметричные алгоритмы шифрования: принципы построения симметричных криптосистем; алгоритм шифрования DES; Шифрование и генерация ключей алгоритма DES. Асимметричные алгоритмы шифрования: стандарт асимметричного шифрования RSA; практическая реализация алгоритма RSA. Контрольная точка 2. Устный опрос.	2
			Итого за семестр:	**8**
			Итого:	**8**

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
1 семестр			
Правовое обеспечение защиты информационных ресурсов	Подготовка к экзамену	Основы политики безопасности хранения и защиты компьютерной информации. Субъекты и объекты правоотношений в области информационной безопасности. Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Стандарты по оценке защищенных систем.	9

Методы и средства защиты информационных ресурсов	Подготовка к практическим занятиям. Изучение теоретического материала.	Разработка и планирование мероприятий по обеспечению защиты объектов компьютерных систем от вероятных угроз. Формулирование требований для анализа предметной области и ее анализ. Выделение активных объектов, которые производят и потребляют данные. Определение и моделирование процессов, которые преобразуют данные. Построение диаграммы потоков данных предметной области.	15
Методы и средства защиты информационных ресурсов	Подготовка к практическим занятиям. Изучение теоретического материала.	Основные механизмы защиты операционной системы MS WINDOWS. Учетные записи и авторизация пользователей. Управление учетными записями. Разграничение доступа к объектам файловой системы. Разграничение доступа к системному реестру. Аудит использования привилегий, отслеживания процессов и системных событий.	15
Методы и средства защиты информационных ресурсов	Подготовка к практическим занятиям. Изучение теоретического материала.	Программно-технические средства защиты компьютерных систем. Защита памяти. Защита выполнения программ. Защита дисков. Анализ методов защиты дисков. Дисковые контроллеры. Средства защиты программного обеспечения с электронными ключами. Обзор элементной базы используемой для построения современных моделей электронных ключей.	15
Методы и средства защиты информационных ресурсов	Подготовка к практическим занятиям. Изучение теоретического материала.	Криптографическая защита компьютерной информации. Разработка и исследование учебного варианта криптографической системы шифрования. Симметричные алгоритмы шифрования: принципы построения симметричных криптосистем; алгоритм шифрования DES; Шифрование и генерация ключей алгоритма DES. Асимметричные алгоритмы шифрования: стандарт асимметричного шифрования RSA; практическая реализация алгоритма RSA.	15

Методы и средства защиты информационных ресурсов	Подготовка к экзамену	Основы политики безопасности хранения и защиты компьютерной информации. Разработка и планирование мероприятий по обеспечению защиты объектов компьютерных систем от вероятных угроз. Программно-технические средства защиты компьютерных систем. Криптографическая защита компьютерной информации. Стеганография: сокрытия сообщения внутри другого файла, сообщения, изображения или видео.	30
		Итого за семестр:	**99**
		Итого:	**99**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	**Библиографическое описание**	**Ресурс НТБ СамГТУ** (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Девянин, П.Н. Модели безопасности компьютерных систем : Учеб.пособие / П. Н. Девянин.- М., Academia, 2005.- 143 с.	Электронный ресурс
2	Запечников , С.В. Криптографические методы защиты информации : учеб. пособие для академ.бакалавриата / С. В. Запечников,О. В. Казарин, А. А. Тарасов.- М., Юрайт, 2015.- 309 с.	Электронный ресурс
3	Зубов, А.Ю. Криптографические методы защиты информации : Соверш.шифры:Учеб.пособие / А. Ю. Зубов.- М., Гелиос АРВ, 2005.- 191 с.	Электронный ресурс
4	Куприянов, А.И. Основы защиты информации : Учеб.пособие / А.И.Куприянов,А.В.Сахаров,В.А.Шевцов.- М., Academia, 2006.- 254 с.	Электронный ресурс
5	Мельников, В.П. Информационная безопасность : учеб. / В.П.Мельников,А.И.Куприянов,Т.Ю.Васильева;ред.В.П.Мельников.- М., RuScience, 2017.- 354 с.	Электронный ресурс
6	Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : Учеб.пособие / П. Б. Хорев .- 4-е изд.,стер..- М., Academia, 2008.- 255 с.	Электронный ресурс
7	Шаньгин, В.Ф. Защита компьютерной информации : Эффектив.методы и средства:Учеб.пособие / В. Ф. Шаньгин.- М., ДМК Пресс, 2008.- 542 с.	Электронный ресурс
Дополнительная литература		
8	Запечников , С.В. Криптографические методы защиты информации : учеб. пособие для академ.бакалавриата / С. В. Запечников,О. В. Казарин, А. А. Тарасов.- М., Юрайт, 2015.- 309 с.	Электронный ресурс
9	Зубов, А.Ю. Криптографические методы защиты информации : Соверш.шифры:Учеб.пособие / А. Ю. Зубов.- М., Гелиос АРВ, 2005.- 191 с.	Электронный ресурс

10	Казанцев, С.Я. Правовое обеспечение информационной безопасности : Учеб.пособие / Под ред.С.Я.Казанцева .- 3-е изд.,стер..- М., Academia, 2008.- 239 с.	Электронный ресурс
11	Организационное и правовое обеспечение информационной безопасности : учеб. и практикум для бакалавриата и магистратуры / под ред.Т. А. Поляковой, А. А. Стрельцова.- М., Юрайт, 2017.- 325 с.	Электронный ресурс
12	Семкин, С.Н. Основы правового обеспечения защиты информации : Учеб.пособие / С.Н.Семкин,А.Н.Семкин.- М., Горячая линия-Телеком, 2007.- 238 с.	Электронный ресурс
13	Снытников, А.А. Обеспечение и защита права на информацию / А.А.Снытников,Л.В.Туманова.- М., Городец-издат, 2001.- 339 с.	Электронный ресурс
14	Соколов, А.В. Защита информации в распеределенных корпоративных сетях и системах / А.В.Соколов,В.Ф.Шаньгин.- М., ДМК Пресс, 2002.- 655 с.	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Операционная система Windows 10	Microsoft Corporation (Зарубежный)	Лицензионное
2	Microsoft Office 2010, 2016	Microsoft Corporation (Зарубежный)	Лицензионное
3	Internet Explorer	Microsoft Corporation (Зарубежный)	Лицензионное
4	Visual Studio Code	Microsoft Corporation (Зарубежный)	Свободно распространяемое
5	Microsoft SQL Server	Microsoft Corporation (Зарубежный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Библиотека компьютерной литературы	http://it.eup.ru/	Ресурсы открытого доступа

2	Защита компьютера от вирусов, конфиденциальность личных данных и безопасность в сети [электронный ресурс] // Microsoft. Центр безопасности	http://www.microsoft.com/ru-ru/security/worldwide.aspx	Ресурсы открытого доступа
3	Информационная безопасность	http://bugtraq.ru/	Ресурсы открытого доступа
4	Официальный сайт информационно-правовой системы «Гарант»	http://www.garant.ru	Ресурсы открытого доступа
5	Консультант плюс	http://www.consultant.ru	Ресурсы открытого доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Пакеты ПО общего назначения (MS Office Word, MS Office Excel MS, PowerPoint).

Практические занятия

Аудитории для практических занятий укомплектованы специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук). На компьютерах/ноутбуках установлены специализированные программные комплексы и программное обеспечение для работы на практических занятиях. Рабочие места студентов подключены к локальной компьютерной сети СамГТУ, имеющей высокоскоростной доступ к глобальной сети Интернет.

Самостоятельная работа

Аудитории для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СамГТУ.

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и

выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических

задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины

Б1.В.01.03 «Защита информационных ресурсов промышленных объектов»

Фонд оценочных средств
по дисциплине
Б1.В.01.03 «Защита информационных ресурсов промышленных объектов»

Код и направление подготовки (специальность)	15.04.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Интеллектуальные системы мониторинга состояния сложных инфраструктурных объектов
Квалификация	Магистр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Автоматизация и управление технологическими процессами"
Кафедра-разработчик	кафедра "Автоматизация и управление технологическими процессами"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
	ОПК-6 Способен осуществлять научно-исследовательскую деятельность, используя современные информационно-коммуникационные технологии, глобальные информационные ресурсы;	ОПК-6.2 Уметь использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности	Уметь использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности
Профессиональные компетенции			
Не предусмотрено	ПК-4 Способен разрабатывать теоретические модели, позволяющие модернизировать средства и системы автоматизации	ПК-4.2 Уметь составлять теоретическое описание моделей средств и систем автоматизации для последующей их модернизации в целях повышения эффективности процессов, производить анализ и обосновывать эффективность применения конкретных моделей	Уметь составлять теоретическое описание моделей средств и систем автоматизации с целью обеспечения защиты информационных ресурсов.
Универсальные компетенции			
Системное и критическое мышление	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Знать методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях	Знать методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях.
		УК-1.2 Уметь применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций	Уметь применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций.
		УК-1.3 Владеть методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач	Владеть методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Правовое обеспечение защиты информационных ресурсов				
ОПК-6.2 Уметь использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности	**Уметь** использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности	Отчет по практическому занятию	Да	Нет
ПК-4.2 Уметь составлять теоретическое описание моделей средств и систем автоматизации для последующей их модернизации в целях повышения эффективности процессов, производить анализ и обосновывать эффективность применения конкретных моделей	**Уметь** составлять теоретическое описание моделей средств и систем автоматизации с целью обеспечения защиты информационных ресурсов.	Отчет по практическому занятию	Да	Да
УК-1.1 Знать методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях	**Знать** методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях.	Устный опрос	Да	Да
УК-1.2 Уметь применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций	**Уметь** применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций.	Отчет по практическому занятию	Да	Да
УК-1.3 Владеть методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач	**Владеть** методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач	Отчет по практическому занятию	Да	Да
Методы и средства защиты информационных ресурсов				
ОПК-6.2 Уметь использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности	**Уметь** использовать современные информационные технологии и глобальные информационные ресурсы в научно-исследовательской деятельности	Отчет по практическому занятию	Да	Нет

ПК-4.2 Уметь составлять теоретическое описание моделей средств и систем автоматизации для последующей их модернизации в целях повышения эффективности процессов, производить анализ и обосновывать эффективность применения конкретных моделей	**Уметь** составлять теоретическое описание моделей средств и систем автоматизации с целью обеспечения защиты информационных ресурсов.	Отчет по практическому занятию	Да	Да
УК-1.1 Знать методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях	**Знать** методы системного подхода для поиска, сбора и критического анализа информации о проблемных ситуациях.	Устный опрос	Да	Да
УК-1.2 Уметь применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций	**Уметь** применять методы системного подхода для поиска, сбора и анализа информации, вырабатывать стратегию действий для решения проблемных ситуаций.	Отчет по практическому занятию	Да	Нет
УК-1.3 Владеть методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач	**Владеть** методиками системного подхода к критическому анализу, различными способами поиска и сбора информации, навыками выработки стратегии действий по решению проблемных ситуаций и поставленных задач	Отчет по практическому занятию	Да	Да

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Формы текущей/промежуточной аттестации

Текущая аттестация студентов производится на практических и лабораторных занятиях в форме устного опроса и проверка отчетов по лабораторным работам. Промежуточная аттестация студентов проводится в форме зачета с оценкой. Для подготовки к промежуточной аттестации студентам выдается список вопросов для проведения зачета.

Перечень вопросов для промежуточной аттестации (Экзамен)

1) Определение, свойства, виды и формы представления информации;
2) Аттестация объектов по требованиям безопасности;
3) Анализ информационных ресурсов на предприятии;
4) Организация и планирование безопасности компьютерных систем;
5) Факторы и критерии принятия решения о защите компьютерных систем;
6) Лицензирование и сертификация средств защиты информации;
7) Понятие информационной безопасности;
8) Объекты информационной безопасности Российской Федерации;
9) Государственные стандарты в области защиты информации;
10) Экономические аспекты обеспечения безопасности сложных систем;
11) Правовые и организационно-технические вопросы безопасности компьютерных систем;
12) Понятие и виды конфиденциальной информации;
13) Защита конфиденциальной информации;
14) Угрозы информационной безопасности и их классификация;
15) Структура и основные элементы модели нарушителя;
16) Объекты, цели и задачи защиты компьютерных систем;
17) Категорирование ресурсов компьютерных систем и определение требований к уровню обеспечения их безопасности;
18) Принципы защиты компьютерных систем;
19) Аудит информационной безопасности, алгоритмы и методы аудита информационной безопасности;
20) Комплексный анализ безопасности компьютерных систем на методологическом, организационно-управленческом, технологическом и техническом уровнях;
21) Стратегия управления информационными рисками на основе получения их качественных и количественных оценок;
22) Понятие и признаки компьютерных преступлений, классификация компьютерных преступлений;
23) Компьютерные вирусы и принципы их функционирования;
24) Программные антивирусные средства;
25) Проблемы обеспечения программно-технологической безопасности компьютерных систем;
26) Технологическая безопасность и жизненный цикл компьютерных систем;

27) Требования, предъявляемые к архитектуре баз данных для обеспечения безопасности функционирования компьютерных систем;
28) Средства собственной защиты информационных систем;
29) Средства активной защиты компьютерных систем;
30) Средства пассивной защиты компьютерных систем;
31) Защита памяти компьютерных систем;
32) Защита выполнения программ компьютерных систем;
33) Защиты дисков компьютерных систем;
34) Средства защиты программного обеспечения с электронными ключами;
35) Уровни инфраструктуры информационной сети, источники уязвимости информационной сети;
36) Классификация атак и типовой сценарий действий потенциальных нарушителей инфраструктуры информационной сети;
37) Защитные механизмы и средства обеспечения безопасности информационной сети;
38) Краткая характеристика протоколов сетевого взаимодействия;
39) Проблемы обеспечения безопасности сетевых ОС;
40) Критерии оценки защищенности ОС;
41) Мероприятия по настройке системы безопасности сетевых ОС;
42) Криптография и криптология;
43) Обобщенная схема криптосистемы;
44) Теоретическая, практическая и временная стойкость системы криптографической защиты;
45) Симметричные алгоритмы шифрования;
46) Алгоритм шифрования DES;
47) Методы генерации псевдослучайных чисел;
48) Асимметричные алгоритмы шифрования;
49) Стандарт шифрования RSA;
50) Электронная цифровая подпись;
51) Криптографические протоколы;
52) Информационная безопасность баз данных;
53) Защита информационных ресурсов в сетях, подключенных к Internet;
54) Технические каналы утечки информации.

Дополнительная литература

1) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
2) Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных».
3) ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.
4) Савельев А.И. Лицензирование программного обеспечения в России: Законодательство и практика. – Infotropic Media, 2012. – 432 с.
5) Борисов, А. Н. Комментарий к Федеральному закону от 4 мая 2011 г. №99-ФЗ "О лицензировании отдельных видов деятельности" (постатейный) / А.Н. Борисов. - М.: Юстицинформ, 2016. - 226 с.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Формы текущей/промежуточной аттестации

Текущая аттестация студентов производится на практических и лабораторных занятиях в форме устного опроса и проверка отчетов по лабораторным работам. Промежуточная аттестация студентов проводится в форме зачета с оценкой. Для подготовки к промежуточной аттестации студентам выдается список вопросов для проведения зачета.

Перечень вопросов для промежуточной аттестации (Экзамен)

1) Определение, свойства, виды и формы представления информации;
2) Аттестация объектов по требованиям безопасности;
3) Анализ информационных ресурсов на предприятии;
4) Организация и планирование безопасности компьютерных систем;
5) Факторы и критерии принятия решения о защите компьютерных систем;
6) Лицензирование и сертификация средств защиты информации;
7) Понятие информационной безопасности;
8) Объекты информационной безопасности Российской Федерации;
9) Государственные стандарты в области защиты информации;
10) Экономические аспекты обеспечения безопасности сложных систем;
11) Правовые и организационно-технические вопросы безопасности компьютерных систем;
12) Понятие и виды конфиденциальной информации;
13) Защита конфиденциальной информации;
14) Угрозы информационной безопасности и их классификация;
15) Структура и основные элементы модели нарушителя;
16) Объекты, цели и задачи защиты компьютерных систем;
17) Категорирование ресурсов компьютерных систем и определение требований к уровню обеспечения их безопасности;
18) Принципы защиты компьютерных систем;
19) Аудит информационной безопасности, алгоритмы и методы аудита информационной безопасности;
20) Комплексный анализ безопасности компьютерных систем на методологическом, организационно-управленческом, технологическом и техническом уровнях;
21) Стратегия управления информационными рисками на основе получения их качественных и количественных оценок;
22) Понятие и признаки компьютерных преступлений, классификация компьютерных преступлений;
23) Компьютерные вирусы и принципы их функционирования;
24) Программные антивирусные средства;
25) Проблемы обеспечения программно-технологической безопасности компьютерных систем;
26) Технологическая безопасность и жизненный цикл компьютерных систем;

27) Требования, предъявляемые к архитектуре баз данных для обеспечения безопасности функционирования компьютерных систем;
28) Средства собственной защиты информационных систем;
29) Средства активной защиты компьютерных систем;
30) Средства пассивной защиты компьютерных систем;
31) Защита памяти компьютерных систем;
32) Защита выполнения программ компьютерных систем;
33) Защиты дисков компьютерных систем;
34) Средства защиты программного обеспечения с электронными ключами;
35) Уровни инфраструктуры информационной сети, источники уязвимости информационной сети;
36) Классификация атак и типовой сценарий действий потенциальных нарушителей инфраструктуры информационной сети;
37) Защитные механизмы и средства обеспечения безопасности информационной сети;
38) Краткая характеристика протоколов сетевого взаимодействия;
39) Проблемы обеспечения безопасности сетевых ОС;
40) Критерии оценки защищенности ОС;
41) Мероприятия по настройке системы безопасности сетевых ОС;
42) Криптография и криптология;
43) Обобщенная схема криптосистемы;
44) Теоретическая, практическая и временная стойкость системы криптографической защиты;
45) Симметричные алгоритмы шифрования;
46) Алгоритм шифрования DES;
47) Методы генерации псевдослучайных чисел;
48) Асимметричные алгоритмы шифрования;
49) Стандарт шифрования RSA;
50) Электронная цифровая подпись;
51) Криптографические протоколы;
52) Информационная безопасность баз данных;
53) Защита информационных ресурсов в сетях, подключенных к Internet;
54) Технические каналы утечки информации.

Дополнительная литература

1) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
2) Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных».
3) ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.
4) Савельев А.И. Лицензирование программного обеспечения в России: Законодательство и практика. – Infotropic Media, 2012. – 432 с.
5) Борисов, А. Н. Комментарий к Федеральному закону от 4 мая 2011 г. №99-ФЗ "О лицензировании отдельных видов деятельности" (постатейный) / А.Н. Борисов. - М.: Юстицинформ, 2016. - 226 с.