год начала подготовки 2021

АНО ВО «Российский новый университет»

Елецкий филиал Автономной некоммерческой организации высшего образования «Российский новый университет»
(Елецкий филиал АНО ВО «Российский новый университет»)

кафедра прикладной экономики

Рабочая программа учебной дисциплины (модуля)

Системы информационной безопасности
(наименование учебной дисциплины (модуля))

09.03.03 Прикладная информатика
(код и направление подготовки/специальности)

Прикладная информатика в экономике
(код и направление подготовки/специальности, в случаях, если программа разработана для разных направлений подготовки/специальностей)

Рабочая программа учебной дисциплины (модуля) рассмотрена и утверждена на заседании кафедры «12» января 2021, протокол № 5.

Заведующий кафедрой Прикладной экономики
(название кафедры)
к.э.н., доцент Преснякова Д.В. _____
(ученая степень, ученое звание, фамилия и инициалы, подпись заведующего кафедрой)

Елец
2021 год

1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учебная дисциплина «Системы информационной безопасности» изучается обучающимися, осваивающими образовательную программу «Прикладная информатика» по профилю Прикладная информатика в экономике в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденным приказом Министерства образования и науки РФ от 19.09.2017 N 922 (ФГОС ВО 3++).

Целью изучения дисциплины является обучение студентов основным понятиям, положениям и методам курса Системы информационной безопасности подготовка специалистов, владеющих знаниями и умениями в области организационных и технических основ обеспечения информационной безопасности (ИБ) на предприятиях различного профиля и организационной структуры, необходимыми для выполнения обязанностей должностными лицами системы органов управления, служб и центров защиты информации, центров и узлов связи по организации и обеспечению защиты конфиденциальной информации и персональных данных.

Изучение учебной дисциплины направлено на подготовку обучающихся к осуществлению деятельности по концептуальному, функциональному и логическому проектированию систем среднего и крупного масштаба и сложности, планированию разработки или восстановления требований к системе, анализу проблемной ситуации заинтересованных лиц, разработке бизнес-требований заинтересованных лиц, постановки целей создания системы, разработки концепции системы и технического задания на систему, организации оценки соответствия требованиям существующих систем и их аналогов, представлению концепции, технического задания на систему и изменений в них заинтересованным лицам, организации согласования требований к системе, разработке шаблонов документов требований, постановке задачи на разработку требований к подсистемам и контроль их качества, сопровождению приемочных испытаний и ввода в эксплуатацию системы, обработке запросов на изменение требований к системе, определенных профессиональным стандартом «Системный аналитик», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 28.10.2014 N 809н (Регистрационный номер №34882)..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина Системы информационной безопасности относится к части учебного плана формируемой участниками образовательных отношений и изучается на 4, 5 курсе очной и заочной форме обучения.

2.1. Требования к предварительной подготовке обучающегося:

Изучению данной учебной дисциплины предшествует освоение следующих учебных дисциплин: Информатика и программирование, Операционные системы, Информационные системы и технологии, Вычислительные системы, сети и телекоммуникации, Математическое и имитационное моделирование, Проектирование информационных систем, Программная инженерия, Информационная безопасность.

Параллельно с учебной дисциплиной «Системы информационной безопасности» изучаются дисциплины:

Внедрение информационных систем, Корпоративные информационные системы, Электронный документооборот,

Управление информационными системами, Разработка программных приложений.

2.2. Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Результаты освоения дисциплины «Системы информационной безопасности» являются базой для прохождения обучающимися производственной практики:

преддипломной.

Развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств обеспечивается чтением лекций, проведением семинарских занятий, нацеленных на профессиональную деятельности выпускников и потребности работодателей.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины обучающийся по программе бакалавриата должен овладеть:

- Способен разрабатывать шаблоны документов требований (ПК-15)

Планируемые результаты обучения по дисциплине

Формируемая компетенция	Планируемые результаты обучения	Код показателя результатов обучения
Способен разрабатывать шаблоны документов требований (ПК-15)	**Знать:**	
	нормативно правовые документы, регулирующие документационные процессы на предприятии	ПК-15-З1
	государственные и международные стандарты по подготовке технической документации	ПК-15-З2
	различные подходы и методики подготовки научно-технической документации	ПК-15-З3
	основные функции, свойства и характеристики документов, а также информационных систем по их обработке	ПК-15-З4
	Уметь:	
	проводить обследование документооборота на предприятии его	ПК-15-У1
	описывать текущее состояние документооборота на предприятии	ПК-15-У2
	формулировать предложения по совершенствованию процессов обработки документов на предприятии	ПК-15-У3
	разрабатывать шаблоны документов требований	ПК-15-У4
	Владеть:	
	навыками применять на практике способы и методы проведения исследования документооборота предприятия	ПК-15-В1
	навыкали подготовки технической документации по проектам внедрения электронного документооборота на предприятии	ПК-15-В2
	навыками применения программных и технических средств для оформления результатов исследования документооборота предприятия	ПК-15-В3
	навыками анализа и моделирования процессов обработки документов на предприятия	ПК-15-В4

4. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 2 зачетных единиц (72 часа).

год начала подготовки 2021

Общий объём учебной дисциплины

№	Форма обучения	Семестр/ сессия, курс	Общая трудоемкость		в том числе контактная работа с преподавателем							СР	Контроль
			в з.е.	в часах	Всего	Л	ПР	КоР	зачет	Конс	экзамен		
1.	Очная	7 семестр, 4 курс	2	72	38	12	24	1,7	0,3			34	
		Итого:	**2**	**72**	**38**	**12**	**24**	**1,7**	**0,3**			**34**	
2	Заочная	2 сессия, 4 курс	1	36	4	4						32	
		1 сессия, 5 курс	1	36	6		4	1,7	0,3			26,3	3,7
		Итого	**2**	**72**	**10**	**4**	**4**	**1,7**	**0,3**			**58,3**	**3,7**

Распределение учебного времени по темам и видам учебных занятий

очная форма обучения

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем					СР	Контроль	Формируемые результаты обучения
			Всего	Лекции	Сем	КоР	Зачет			
	Модуль 1. Введение в безопасность информации современного предприятия									
1	1. Основные понятия, термины и определения в области защиты информации	7	3	1	2			4		ПК-15-31 ПК-15-32
2	2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.	7	3	1	2			4		ПК-15-34 ПК-15-В3
3	3. Законодательная и нормативная база правового регулирования вопросов защиты информации.	7	3	1	2			4		ПК-15-В2
4	4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	7	3	1	2			4		ПК-15-В1
5	**Модуль 2. Технологии обеспечения информационной безопасности предприятия**									

год начала подготовки 2021

6	5..Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	10	6	2	4			4		ПК-15-З3 ПК-15-У1
7	6. Меры и средства защиты информации	10	6	2	4			4		ПК-15-В4 ПК-15-У4
8	7. Применения криптографических методов защиты информации при работе в сетях.	10	6	2	4			4		ПК-15-У2
9	8. Аудит информационной безопасности	12	6	2	4			6		ПК-15-У3
10	*Промежуточная аттестация (зачет)*	2	2			1,7	0,3			
11	**Итого**	**72**	**38**	**12**	**24**	**1,7**	**0,3**	**34**		

заочная форма обучения

№	**Наименование разделов, тем учебных занятий**	**Всего часов**	**Контактная работа с преподавателем**					**СР**	**Контроль**	**Формируемые результаты обучения**
			Всего	**Лекции**	**Сем**	**КоР**	**Зачет**			
	Модуль 1. Введение в безопасность информации современного предприятия									
1	1. Основные понятия, термины и определения в области защиты информации	5	1	1				4		ПК-15-З1 ПК-15-З2
2	2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.	5	1	1				4		ПК-15-З4 ПК-15-В3
3	3. Законодательная и нормативная база правового регулирования вопросов защиты информации.	5	1	1				4		ПК-15-В2
4	4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	5	1	1				4		ПК-15-В1

5	**Модуль 2. Технологии обеспечения информационной безопасности предприятия**									
6	5..Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	5	1		1			4		ПК-15-З3 ПК-15-У1
7	6. Меры и средства защиты информации	9	1		1			8		ПК-15-В4 ПК-15-У4
8	7. Применения криптографических методов защиты информации при работе в сетях.	9	1		1			8		ПК-15-У2
9	8. Аудит информационной безопасности	9,3	1		1			8,3		ПК-15-У3
10	*Промежуточная аттестация (Зачет)*		2			1,7	0,3	14		
11	**Итого**	72	10	4	4	1,7	0,3	58,3	3,7	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ)

Модуль 1. Введение в безопасность информации современного предприятия

Тема 1. Основные понятия, термины и определения в области защиты информации

Информация, информационные отношения, субъекты информационных отношений, их интересы и пути нанесения им ущерба. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации

Литература:

а) основная:1-2.

б) дополнительная: 3-5.

Тема 2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности

Формирование модели угроз: угрозы, реализуемые через технические каналы утечки информации, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах или вспомогательных технических средствах и системах; угрозы, реализуемые за счет несанкционированного доступа к персональным данным. Модель угроз и модель нарушителя информационной безопасности. Риски информационной безопасности.

Литература:

а) основная:1-2.

б) дополнительная: 3-5.

Тема 3. Законодательная и нормативная база правового регулирования вопросов защиты информации

Доктрина информационной безопасности Российской Федерации. Федеральные законы Российской Федерации. Постановления правительства Российской Федерации. Указы президента Российской Федерации. Система руководящих и специальных

нормативных документов Российской Федерации в области защиты информации. Порядок проведения инвентаризации персональных данных.

Литература:

а) основная:1-2.

б) дополнительная: 3-5.

Тема 4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.

Подготовка к аттестации на соответствие положениям ФЗ №152 Национальные (ГОСТ), международные и отраслевые стандарты в области защиты информации

,информационных технологий и непрерывности бизнеса. Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства РФ. Ответственность за правонарушения в области защиты информации

Литература:

а) основная:1-2.

б) дополнительная: 3-5.

Модуль 2. Технологии обеспечения информационной безопасности предприятия

Тема 5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Комплексная система обеспечения информационной безопасности организации. Организационная структура системы обеспечения информационной безопасности организации Типовая структура, задачи и функции подразделения (службы) информационной безопасности организации. Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности.

Литература:

а) основная:1-2.

б) дополнительная: 3-5.

Тема 6. Методы и средства защиты информации и персональных данных.

Разработка и построение системы защиты персональных данных. Система управления непрерывностью бизнеса организации в соответствии с требованиями стандарта BS25999. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам. *С*редства защиты информации от ее утечки по техническим каналам. Защита сети электропитания изаземления.

Экономические аспекты обеспечения безопасности. Риск-ориентированный подход в информационной безопасности.

Литература:

а) основная:1-2.

б) дополнительная: 3-5.

Тема 7. Применения криптографических методов защиты информации при работе в сетях. Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам.

Криптографические методы и средства защиты информации. Специфика инфраструктуры открытых ключей. Обеспечение безопасности типовых технологических процессов организации с использованием средств криптографической защиты, электронная подпись.

Литература:
а) основная:1-2.
б) дополнительная: 3-5.

Тема 8. Аудит информационной безопасности

Самооценка и аудит как показатели эффективности процессов обеспечения информационнойбезопасности.

Роли, цели и задачи аудита в процессе обеспечения информационной безопасности.

Литература:
а) основная:1-3.
б) дополнительная: 4-6.

Планы семинарских, практических, лабораторных занятий
очная форма обучения

Тема. **Практическое занятие:** Политика безопасности и формирование организационной структуры системы защиты информации на предприятии.

Продолжительность занятия - 2 часа

Основные вопросы:

1. Требования к защите персональных данных
2. Определение гостайны.

Тема 6. **Практическое занятие:** Меры и средства защиты информации.

Продолжительность занятия - 2 часа

Основные вопросы:

1. Технические методы защиты информации.
2. Организационные методы защиты информации.

Тема 7. **Практическое занятие:** Применения криптографических методов защиты информации при работе в сетях.

Продолжительность занятия - 2 часа

Основные вопросы:

1. Специфика возникновения угроз в открытых сетях.
2. Стеганография

Тема 8. **Практическое занятие:** Аудит информационной безопасности.

Продолжительность занятия - 2 часа

Основные вопросы:

1. Этапы аудита.
2. Результативные документы.

Планы семинарских, практических, лабораторных занятий
заочная форма обучения

Тема. **Практическое занятие:** Политика безопасности и формирование организационной структуры системы защиты информации на предприятии.

Продолжительность занятия - 1 час

Основные вопросы:

3. Требования к защите персональных данных
4. Определение гостайны.

Тема 6. **Практическое занятие:** Меры и средства защиты информации.

Продолжительность занятия - 1 час
Основные вопросы:
3. Технические методы защиты информации.
4. Организационные методы защиты информации.

Тема 7. **Практическое занятие:** Применения криптографических методов защиты информации при работе в сетях.
Продолжительность занятия - 1 час
Основные вопросы:
3. Специфика возникновения угроз в открытых сетях.
4. Стеганография

Тема 8. **Практическое занятие:** Аудит информационной безопасности.
Продолжительность занятия - 1 час
Основные вопросы:
3. Этапы аудита.
4. Результативные документы.

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

6.1. Задания для повторения и углубления приобретаемых знаний.

№	Код результата обучения	Задания
1.	ПК-15-З1	Назовите основные термины в области защиты информации
2.	ПК-15-З1	Проанализируйте системное обеспечение для защиты информации.
3.	ПК-15-З2	Проанализируйте прикладное обеспечение для защиты информации.
4.	ПК-15-З2	Расскажите о процедуре аттестации средств защиты.
5.	ПК-15-З3	Перечислите основные правовые акты в области защиты информации
6.	ПК-15-З3	Классифицируйте системы информационной безопасности
7.	ПК-15-З4	Что такое информационная угроза?
8.	ПК-15-З4	Каковы причины утечки информации.

6.2. Задания, направленные на формирование профессиональных умений

№	Код результата обучения	Задания
9.	ПК-15-У1	Проведите сравнительный анализ видов информационных угроз.
10.	ПК-15-У1	Проанализируйте законодательство в сфере разработки систем информационной безопасности.
11.	ПК-15-У2	Создайте таблицу с результатами оценивания информационных угроз для конкретного предприятия.
12.	ПК-15-У2	Какова мера оценки несанкционированного доступа.
13.	ПК-15-У3	Выработать критерии для анализа предлагаемых на рынке инструментальных средств для информационной защиты организации.

14.	ПК-15-У3	Что представляет собой аудит системы информационной безопасности.
15.	ПК-15-У4	Приведите примеры объектов интеллектуальной деятельности.
16.	ПК-15-У4	Какие виды охраняемых результатов интеллектуальной деятельности и средств индивидуализации вам известны.

6.3. Задания, направленные на формирование профессиональных навыков, владений

№	Код результата обучения	Задания
17.	ПК-15-В1	Подготовить требования к системе информационной безопасности.
18.	ПК-15-В1	Нарисуйте схему структуры системы информационной безопасности.
19.	ПК-15-В2	Нарисуйте иерархическую схему роли персонала в защите информации на предприятии.
20.	ПК-15-В2	Охарактеризовать организационные меры защиты информации.
21.	ПК-15-В3	Оформите требования к оформлению технической документации по системам информационной безопасности.
22.	ПК-15-В3	Выработать критерии для анализа предлагаемых на рынке инструментальных средств информационной безопасности.
23.	ПК-15-В4	Создайте модель нарушителя информационной безопасности.
24.	ПК-15-В4	Проведите процедуры аутентификации и идентификации.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Средства оценивания в ходе текущего контроля:

- письменные краткие опросы в ходе аудиторных занятий на знание категорий учебной дисциплины
- задания и упражнения, рекомендованные для самостоятельной работы;
- практическая работа,
- задания, упражнения и выполнение теста в ходе практических занятий.

7.2. ФОС для текущего контроля

№	Показатели результата обучения	ФОС текущего контроля
1	ПК-15-31	Письменный опрос на занятиях по темам основных терминов учебной дисциплины. Задание 1,2 для приобретения, закрепления и углубления знаний из п. 6.1
2	ПК-15-32	Задание 3,4 для приобретения, закрепления и углубления знаний из п. 6.1.
3	ПК-15-33	Задание 5,6 для приобретения, закрепления и углубления знаний из п. 6.1
4	ПК-15-34	Задание 7,8 для приобретения, закрепления и углубления знаний из п. 6.1

5	ПК-15-У1	Задание 9,10 направленные на формирование профессиональных умений из п. 6.2
6	ПК-15-У2	Задание 11,12 направленные на формирование профессиональных умений из п. 6.2
7	ПК-15-У3	Задание 13,14 направленные на формирование профессиональных умений из п. 6.2
8	ПК-15-У4	Задание 15,16 направленные на формирование профессиональных умений из п. 6.2
9	ПК-15-В1	Задание 17,18 направленные на формирование профессиональных навыков, владений из п. 6.3.
10	ПК-15-В2	Задание 19,20 направленные на формирование профессиональных навыков, владений из п. 6.3.
11	ПК-15-В3	Задание 21,22 направленные на формирование профессиональных навыков, владений из п. 6.3.
12	ПК-15-В4	Задание 23,24 направленные на формирование профессиональных навыков, владений из п. 6.3.

7.3. ФОС для промежуточной аттестации
Задания для оценки знаний

№	Показатели результата обучения	ФОС для оценки знаний
1	ПК-15-З1	Вопросы для зачета 1-9 1. Информация как объект правового регулирования. 2. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней. 3. Законодательство РФ в области информационной безопасности. 4. Информационная безопасность объекта при осуществлении международного сотрудничества. 5. Виды угроз информационной безопасности. 6. Угрозы конституционным правам и свободам гражданина в области информационной деятельности. 7. Угрозы информационному обеспечению государственной политики Российской Федерации. 8.Угрозы безопасности информационных и телекоммуникационных средств и систем. 9.Внешние и внутренние источники угроз информационной безопасности.
2	ПК-15-З2	Вопросы для зачета 10-19 9. Основные виды угроз безопасности субъектов информационных отношений. 10. Основные непреднамеренные и преднамеренные искусственные угрозы. 11. Основные преднамеренные искусственные угрозы. 12. Закон РФ от 21.09.93 «О государственной тайне». 13. Закон РФ от 09.07.2004г. «О коммерческой тайне». 14. Закон РФ от 08.07.2006г. «О персональных данных». 15. «Концепция защиты СВТ и АС от НСД», предназначение, основные понятия и направления. 16. Основные принципы защиты от НСД, изложенные в нормативных документах концепции защиты СВТ иАС. 17. Свойства защищенных автоматизированных систем обработки информации 18.Специфика возникновения угроз и рисков в открытых сетях. 19. Что понимается под уязвимостью защищенных компьютерных систем?
3	ПК-15-З3	Вопросы для зачета 20-30 20. Специфика возникновения угроз и рисков в открытых сетях. 21. Что понимается под уязвимостью защищенных компьютерных систем? 22.Основные направления обеспечения информационной безопасности в компьютерных системах. 23. Основные понятия безопасности компьютерных систем. 24. Что понимается под лицензированием деятельности в области защиты информации?

		25. Перечислить основные мероприятия, позволяющие решить задачу построения системы защиты рабочей станции. 26. Для чего используются системы многоуровневой защиты? 27. Какие вы знаете аспекты защиты информации в системе с разграничением полномочий? 28. Перечислите и дайте характеристику основным методам построения систем защиты с многоуровневым доступом. 29. Какое место занимает механизм подотчетности в политике безопасности и, на какие категории делятся средства подотчетности? 30. Какие проблемы возникают при использовании защиты информации путем ограничения доступа?
4	ПК-15-34	Вопросы для контроля 31-40 31. Какие проблемы возникают при использовании защиты информации путем ограничения доступа? 32. Какие принципы положены в концепцию построения защищенных систем? 33. Перечислить и дать характеристику основным компонентам технологии построения защищенной компьютерной системы. 34. Каким способом происходит интеграция средств защиты и распространенных приложений в защищенной компьютерной системе? 35. Что понимается под несанкционированным доступом к информации. 36. Перечислить и дать характеристику обобщенным методам защиты от НСД. 37. Что понимается под стойкостью системы идентификации? 38. Что является интегральной характеристикой защищенной системы? Понятие политики безопасности и её основные базовые представления. 39. В каких случаях используют модели безопасности производители защищенных компьютерных систем? 40. На каких базовых представлениях основаны модели безопасности?

Задания для оценки умений.

№	Код результата обучения	Задания
1.	ПК-15-У1-У.4	В качестве фонда оценочных средств для оценивания умений обучающегося используются задания 9-16, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.2.)

Задания для оценивания навыков, владений, опыта деятельности

№	Код результата обучения	Задания
1	ПК-15-В1-В.4	В качестве фондов оценочных средств для оценки навыков, владений, опыта деятельности обучающегося используются задания 17-24, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.3.), а также практические работы.

8. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

8.1. Основная литература

1. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6.— Режим доступа: http://www.iprbookshop.ru/63592.html

2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

8.2. Дополнительная литература

1. Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.
2. Семененко В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)
3. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html

9. ПЕРЕЧЕНЬ КОМПЛЕКТОВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

При изучении учебной дисциплины (в том числе в интерактивной форме) предполагается применение современных информационных технологий. Комплект программного обеспечения для их использования включает в себя: операционная система Microsoft Windows 7 Pro, офисный пакет программ Microsoft Office Professional Plus 2010, офисный пакет программ Microsoft Office Professional Plus 2007, антивирусная программа Dr. Web Desktop Security Suite, архиватор 7-zip, аудиопроигрыватель AIMP, просмотр изображений FastStone Image Viewer, ПО для чтения файлов формата PDF Adobe Acrobat Reader, ПО для сканирования документов NAPS2, ПО для записи видео и проведения видеотрансляций OBS Studio, ПО для удалённого администрирования Aspia, правовой справочник Гарант Аэро, онлайн-версия КонсультантПлюс: Студент, электронно-библиотечная система IPRBooks, электронно-библиотечная система Юрайт, математические вычисления Mathcad 14 University, версия 1С для использования типовых конфигураций в учебных целях: 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях, моделирование бизнес-процессов CA ERwin Process Modeler 7.3, версия 1С для обучения программированию: 1С: Предприятие 8.2 Версия для обучения программированию

10. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

10.1. Интернет-ресурсы

1. ЭБС IPRbooks (АйПиАрбукс) http://www.iprbookshop.ru
2. Образовательная платформа ЮРАЙТ https://urait.ru
3. http://citforum.ru/ Сервер информационных технологий. Содержит большое количество информации по всем областям ИТ-технологий, в том числе новости ИТ-мира.
4. http://www.intuit.ru/ Образовательный проект, главными целями которого являются свободное распространение знаний во Всемирной Сети и предоставление услуг дистанционного обучения.
5. http://www.microsoft.com/rus/ Русифицированный сайт компании Майкрософт. http://www.infoforum.ru/ Национальный форум информационной безопасности «Инфофорум»

6. hptt;//www.rupto.ru Сайт федеральной службы по интеллектуальной собственности

11. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ.

Изучение учебной дисциплины «Системы информационной безопасности» обучающимися инвалидами и лицами с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства образования и науки РФ от 9 ноября 2015 г. № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи» (с изменениями и дополнениями), Методическими рекомендациями по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденными Министерством образования и науки РФ 08.04.2014г. № АК-44/05вн, Положением об организации обучения студентов – инвалидов и лиц с ограниченными возможностями здоровья, утвержденным приказом ректора Университета от 6 ноября 2015 года №60/о, Положением о Центре инклюзивного образования и психологической помощи АНО ВО «Российский новый университет», утвержденного приказом ректора от 20 мая 2016 года № 187/о.

Лица с ограниченными возможностями здоровья и инвалиды обеспечиваются электронными образовательными ресурсами, адаптированными к состоянию их здоровья.

Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом индивидуальных психофизиологических особенностей обучающихся и специфики приема-передачи учебной информации на основании просьбы, выраженной в письменной форме.

С обучающимися по индивидуальному плану или индивидуальному графику проводятся индивидуальные занятия и консультации.

12. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации

Ауд.305 (компьютерный класс № 3)

Специализированная мебель:

- столы студенческие;
- стулья студенческие;
- стол для преподавателя;
- стул для преподавателя;
- столы компьютерные;
- кресла компьютерные;
- шкаф для хранения раздаточного материала;
- доска (меловая);
- маркерная доска (переносная).

Технические средства обучения:

- проектор (портативный);

- ПК для преподавателя с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза;
- ПК для обучающихся с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду;
- веб-камера;
- экран (переносной);
- колонки;
- микрофон.

Специализированное оборудование:

- наглядные пособия (плакаты), информационный стенд

Автор (составитель): ст.преподаватель Суздальская Е.А. 
(подпись)

Лист внесения изменений в рабочую программу учебной дисциплины «Системы информационной безопасности»

Рабочая программа рассмотрена и одобрена на 2021/2022 учебный год.
Протокол № 10 заседания кафедры ПЭ от «11» июня 2021 г.

Зав. кафедрой _____/Преснякова Д.В./

год начала подготовки 2021

Аннотация рабочей программы учебной дисциплины

СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код и направление подготовки 09.03.03 Прикладная информатика

Прикладная информатика в экономике

Учебная дисциплина «Системы информационной безопасности» изучается обучающимися, осваивающими образовательную программу «Прикладная информатика» по профилю Прикладная информатика в экономике в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению Прикладная информатика (уровень бакалавриата), утвержденным приказом Министерства образования и науки РФ от 19.09.2017 N 922 (ФГОС ВО 3++).

Целью изучения дисциплины является обучение студентов основным понятиям, положениям и методам курса «Системы информационной безопасности» подготовка специалистов, владеющих знаниями и умениями в области организационных и технических основ обеспечения информационной безопасности (ИБ) на предприятиях различного профиля и организационной структуры, необходимыми для выполнения обязанностей должностными лицами системы органов управления, служб и центров защиты информации, центров и узлов связи по организации и обеспечению защиты конфиденциальной информации и персональных данных.

Изучение учебной дисциплины направлено на подготовку обучающихся к осуществлению деятельности по концептуальному, функциональному и логическому проектированию систем среднего и крупного масштаба и сложности, планированию разработки или восстановления требований к системе, анализу проблемной ситуации заинтересованных лиц, разработке бизнес-требований заинтересованных лиц, постановки целей создания системы, разработки концепции системы и технического задания на систему, организации оценки соответствия требованиям существующих систем и их аналогов, представлению концепции, технического задания на систему и изменений в них заинтересованным лицам, организации согласования требований к системе, разработке шаблонов документов требований, постановке задачи на разработку требований к подсистемам и контроль их качества, сопровождению приемочных испытаний и ввода в эксплуатацию системы, обработке запросов на изменение требований к системе, определенных профессиональным стандартом «Системный аналитик», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 28.10.2014 N 809н (Регистрационный номер № 34882).

Учебная дисциплина Системы информационной безопасности относится к части учебного плана формируемой участниками образовательных отношений и изучается на 4, 5 курсе очной и заочной форме обучения.

В результате освоения дисциплины обучающийся должен овладеть

ПК-15 - способен разрабатывать шаблоны документов требований