год начала подготовки 2019

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 и сферы обслуживания

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 « 22» января 2019, протокол № 5/1.

Заведующий кафедрой Прикладной экономики и сферы обслуживания
(название кафедры)
к.п.н., доцент Гнездилова Н.А. _____
(ученая степень, ученое звание, фамилия и инициалы, подпись заведующего кафедрой)

Елец
2019 год

1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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).

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП БАКАЛАВРИАТА

Учебная дисциплина «Системы информационной безопасности» относится к части учебного плана, формируемой участниками образовательных отношений, изучается по заочной форме обучения в ходе 2 сессии 4 курса и 1 сессии 5 курса.

Изучению данной учебной дисциплины по очной и заочной формам обучения предшествует освоение следующих учебных дисциплин: Информационные системы и технологии, Управление информационными системами, Программная инженерия. Параллельно с учебной дисциплиной «Системы информационной безопасности» изучаются дисциплины: Проектирование информационных систем, Корпоративные информационные системы, Предметно-ориентированные экономические ИС.

Результаты освоения дисциплины «Системы информационной безопасности» являются базой для прохождения обучающимися производственной практики: преддипломной, а также для изучения учебных дисциплин: Реинжиниринг процессов, Внедрение информационных систем, Системная архитектура.

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

В результате освоения дисциплины обучающийся должен овладеть дополнительной профессиональной компетенцией: Способен разрабатывать шаблоны документов

год начала подготовки 2019

требований (ДПК -15)

Показатели оценивания компетенции

Формируемая компетенция	**Планируемые результаты обучения**	**Соотнесение показателей обучения дисциплины с индикаторами достижения компетенций**	
		Код показателя результатов обучения	**Код показателя результатов обучения**
Способен разрабатывать шаблоны документов требований (ДПК -15)	**Знать:**		
	Определения в области защиты интеллектуальной собственности	ДПК-15-З1	И-ДПК-15.1 И-ДПК-15.2
	Основные требования информационной безопасности	ДПК-15-З2	И-ДПК-15.1 И-ДПК-15.2
	Принципы работы систем информационной безопасности	ДПК-15-З3	И-ДПК-15.1 И-ДПК-15.2
	Методы и способы составления технической документации проектов автоматизации и информатизации прикладных процессов	ДПК-15-З4	И-ДПК-15.1 И-ДПК-15.2
	Уметь:		
	Классифицировать угрозы информационной безопасности	ДПК-15-У1	И-ДПК-15.3
	Применять криптографические методы защиты информации	ДПК-15-У2	И-ДПК-15.3
	Использовать действующее законодательство и другие правовые документы для защиты интеллектуальной собственности	ДПК-15-У3	И-ДПК-15.3
	Оценивать эффективность систем информационной безопасности	ДПК-15-У4	И-ДПК-15.3
	Владеть:		
	Навыками администрирования подсистем информационной безопасности	ДПК-15-В1	И-ДПК-15.4 И-ДПК-15.5
	Навыками применения методики реализации защиты интеллектуальной собственности	ДПК-15-В2	И-ДПК-15.4 И-ДПК-15.5
	Навыками оценки систем информационной безопасности	ДПК-15-В3	И-ДПК-15.4 И-ДПК-15.5
	Основными правилами проведения аудита информационной информации	ДПК-15-В4	И-ДПК-15.4 И-ДПК-15.5

4. 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.

4.1. Общий объем учебной дисциплины (модуля)

№	Форма обучения	Семестр/ сессия, курс	Общая трудоемкость		в том числе контактная работа с преподавателем					СР	Контроль
			в з.е.	в часах	Всего	Л	Сем	КоР	зачет		
1.	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

Дисциплина предполагает изучение 8 тем. Общая трудоемкость дисциплины составляет 2 зачетных единиц (72 часа).

4.2. Распределение учебного времени по темам и видам учебных занятий заочная форма обучения

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем					Сам. работа	Контроль	Формируемые результаты обучения
			Всего	Лекции	Сем	Кор	Зач			
	Модуль 1. Введение в безопасность информации современного предприятия									
1	1. Основные понятия, термины и определения в области защиты информации	5	1	1				4		ДПК-15-З1 ДПК-15-З2
2	2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.	5	1	1				4		ДПК-15-З4 ДПК-15-В3
3	3. Законодательная и нормативная база правового регулирования вопросов защиты информации.	5	1	1				4		ДПК-15-В2
4	4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	5	1	1				4		ДПК-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		ДПК-15-З3 ДПК-15-У1
7	6. Меры и средства защиты информации	9	1		1			8		ДПК-15-В4 ДПК-15-У4
8	7. Применения криптографических методов защиты информации при работе в сетях.	9	1		1			8		ДПК-15-У2
9	8. Аудит информационной безопасности	9,3	1		1			8,3		ДПК-15-У3
10	***Промежуточная аттестация (Зачет)***		2			1,7	0,3	14		
11	**Всего по дисциплине**	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 и заземления.

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 информационной безопасности.

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

Литература:

а) основная:1-3.

б) дополнительная: 4-6.

ПЛАНЫ СЕМИНАРСКИХ ЗАНЯТИЙ

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

1. Конфиденциальность, целостность, доступность.
2. Объекты, цели и задачи защиты информации

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

Вопросы:

1. Классификация угроз и рисков ИБ.
2. Модель нарушителя ИБ.

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

Вопросы:

1. Закон № 152.
2. Законы о государственной, служебной, корпоративной тайнах.
3. Законодательство в области информационной безопасности.

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

Вопросы:

1. Закон о персональных данных.
2. Системы защиты и обработки персональных данных.

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

Вопросы:

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

Тема 6. Меры и средства защиты информации.

Вопросы:

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

Тема 7. Применения криптографических методов защиты информации при работе в сетях. Вопросы:

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

Тема 8. Аудит информационной безопасности. Вопросы:

1. Этапы аудита.
2. Результативные документы.

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

6.1. Задания для приобретения новых знаний, углубления и закрепления ранее приобретенных знаний (ДПК-15- 31, ДПК-15- 32, ДПК-15- 33, ДПК-15- 34).

Основными видами внеаудиторной самостоятельной работы при изучении данного предмета являются: чтение основной и дополнительной литературы (в соответствии с перечнем основной и дополнительной литературы, необходимой для освоения дисциплины) по указанию преподавателя, а также с использованием Интернета; изучение конспектов лекций; выполнение заданий на семинарах, учебно-исследовательская работа под руководством преподавателя с использованием компьютерной техники; повторная работа над учебным материалом, подготовка докладов для выступления на семинарах, выполнение домашних заданий.

6.1. Задания для приобретения, закрепления и углубления знаний.

ДПК -15-з1

1. Назовите основные термины в области защиты информации

2. Проанализируйте системное обеспечение для защиты информации.

ДПК -15-з2

3. Проанализируйте прикладное обеспечение для защиты информации.

4. Расскажите о процедуре аттестации средств защиты.

ДПК -15-з3

5. Перечислите основные правовые акты в области защиты информации.

6. Классифицируйте системы информационной безопасности

ДПК -15-з4

7. Что такое информационная угроза? 8.Каковы причины утечки информации.

6.2. Задания, направленные на формирование профессиональных умений.

ДПК -15-у1

9.Проведите сравнительный анализ видов информационных угроз.

10.Проанализируйте законодательство в сфере разработки систем информационной безопасности.

ДПК -15-у2

11. Создайте таблицу с результатами оценивания информационных угроз для конкретного предприятия.

12. Какова мера оценки несанкционированного доступа.

ДПК -15-у3

13. Выработать критерии для анализа предлагаемых на рынке инструментальных средств для информационной защиты организации.

14. Что представляет собой аудит системы информационной безопасности.

ДПК-15-у4

15. Приведите примеры объектов интеллектуальная деятельности.

16. Какие виды охраняемых результатов интеллектуальной деятельности и средств индивидуализации вам известны.

6.3. Задания, направленные на формирование профессиональных навыков, владений.

ДПК -15-в1

17. Подготовить требования к системе информационной безопасности.

18. Нарисуйте схему структуры системы информационной безопасности.

ДПК -15-в2

19. Нарисуйте иерархическую схему роли персонала в защите информации на предприятии.

20. Охарактеризовать организационные меры защиты информации.

ДПК-15-в3

21. Оформите требования к оформлению технической документации по системам информационной безопасности.

22. Выработать критерии для анализа предлагаемых на рынке инструментальных средств информационной безопасности.

ДПК-15-в4

23. Создайте модель нарушителя информационной безопасности.

24. 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

№	Формируемая компетенция	Показатели результата обучения	ФОС текущего контроля
1	*Способен разрабатывать шаблоны документов требований (ДПК-15)*	ДПК-15-З1	Письменный опрос на занятиях по темам основных терминов учебной дисциплины. Задание 1,2 для приобретения, закрепления и углубления знаний из п. 6.1
2		ДПК-15-З2	Задание 3,4 для приобретения, закрепления и углубления знаний из п. 6.1.
3		ДПК-15-З3	Задание 5,6 для приобретения, закрепления и углубления знаний из п. 6.1
4		ДПК-15-З4	Задание 7,8 для приобретения, закрепления и углубления знаний из п. 6.1
5		ДПК-15-У1	Задание 9,10 направленные на формирование профессиональных умений из п. 6.2
6		ДПК-15-У2	Задание 11,12 направленные на формирование профессиональных умений из п. 6.2
7		ДПК-15-У3	Задание 13,14 направленные на формирование профессиональных умений из п. 6.2
8		ДПК-15-У4	Задание 15,16 направленные на формирование профессиональных умений из п. 6.2
9		ДПК-15-В1	Задание 17,18 направленные на формирование профессиональных навыков, владений из п. 6.3.
10		ДПК-15-В2	Задание 19,20 направленные на формирование профессиональных навыков, владений из п. 6.3.
11		ДПК-15-В3	Задание 21,22 направленные на формирование профессиональных навыков, владений из п. 6.3.
12		ДПК-15-В4	Задание 23,24 направленные на формирование профессиональных навыков, владений из п. 6.3.

7.3 ФОС для промежуточной аттестации.

7.3.1. Задания для оценки знаний.

№	Формируемая компетенция	Показатели результата обучения	ФОС для оценки знаний
1	*Способен разрабатывать шаблоны документов требований (ДПК -15)*	ДПК-15-З1	Вопросы для контроля 1-9
2		ДПК-15-З2	Вопросы для контроля 10-19
3		ДПК-15-З3	Вопросы для контроля 20-30
4		ДПК-15-З4	Вопросы для контроля 31-40

Вопросы для подготовки к зачету

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.
10. Основные виды угроз безопасности субъектов информационных отношений.
11. Основные непреднамеренные и преднамеренные искусственные угрозы.
12. Основные преднамеренные искусственные угрозы.
13. Закон РФ от 21.09.93 «О государственной тайне».
14. Закон РФ от 09.07.2004г. «О коммерческой тайне».
15. Закон РФ от 08.07.2006г. «О персональных данных».
16. «Концепция защиты СВТ и АС от НСД», предназначение, основные понятия и направления.
17. Основные принципы защиты от НСД, изложенные в нормативных документах концепции защиты СВТ и АС.
18. Свойства защищенных автоматизированных систем обработки информации.
19. Специфика возникновения угроз и рисков в открытых сетях.
20. Что понимается под уязвимостью защищенных компьютерных систем?
21. Основные направления обеспечения информационной безопасности в компьютерных системах.
22. Основные понятия безопасности компьютерных систем.
23. Что понимается под лицензированием деятельности в области защиты информации?
24. Перечислить основные мероприятия, позволяющие решить задачу построения системы защиты рабочей станции.
25. Для чего используются системы многоуровневой защиты?
26. Какие вы знаете аспекты защиты информации в системе с разграничением полномочий?
27. Перечислите и дайте характеристику основным методам построения систем защиты с многоуровневым доступом.
28. Какое место занимает механизм подотчетности в политике безопасности и, на какие категории делятся средства подотчетности?
29. Какие проблемы возникают при использовании защиты информации путем ограничения доступа?
30. Какие принципы положены в концепцию построения защищенных систем?
31. Перечислить и дать характеристику основным компонентам технологии построения защищенной компьютерной системы.
32. Каким способом происходит интеграция средств защиты и распространенных приложений в защищенной компьютерной системе?
33. Что понимается под несанкционированным доступом к информации.
34. Перечислить и дать характеристику обобщенным методам защиты от НСД.
35. Что понимается под стойкостью системы идентификации?
36. Что является интегральной характеристикой защищенной системы?
37. Понятие политики безопасности и её основные базовые представления.
38. В каких случаях используют модели безопасности производители защищенных компьютерных систем?
39. Из каких частей состоит ГОСТ Р 15408?
40. На каких базовых представлениях основаны модели безопасности?

7.3.2. Задания для оценки умений.

В качестве фондов оценочных средств для оценки умений обучающегося используются задания 9-16, рекомендованные для выполнения в часы самостоятельной работы (раздел 6)

7.3.3. Задания для оценки навыков, владений, опыта деятельности

В качестве фондов оценочных средств для оценки навыков, владений, опыта деятельности обучающегося используются задания 17-24, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.2.), а также практическая работа: чтение лекций, проведение различных видов семинарских и практических занятий с использованием активных методов обучения.

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 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

8.1. ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

3.Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

4.Семененко В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)

5.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 с. — 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:

- пакеты офисного программного обеспечения Microsoft Office (Word, Excel, Power Point), Open Office;
- веб-браузер (Google Chrome, Mozilla Firefox, Internet Explorer др.); электронную библиотечную систему IPRBooks;
- систему размещения в сети «Интернет» и проверки на наличие заимствований курсовых, научных и выпускных квалификационных работ «ВКР-ВУЗ.РФ».

Справочно-правовые системы Консультант Плюс, Гарант.

Для доступа к учебному плану и результатам освоения дисциплины, формирования Портфолио обучающегося используется Личный кабинет студента (он-лайн доступ через сеть Интернет http://lk.rosnou.ru). Для обеспечения доступа обучающихся во внеучебное время к электронным образовательным ресурсам учебной дисциплины, а также для студентов, обучающихся с применением дистанционных образовательных технологий, используется портал электронного обучения на базе СДО Moodle (он-лайн доступ через сеть Интернет https://e-edu.rosnou.ru).

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. ПЕРЕЧЕНЬ УЧЕБНЫХ АУДИТОРИЙ И ОБОРУДОВАНИЯ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПРОВЕДЕНИЯ УЧЕБНЫХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

№	Виды занятий	Учебные аудитории	Оборудование
1.	Лекции	№ 200(компьютерный класс №2), № 305 (компьютерный класс №3), № 403 (компьютерный класс №4).	Экран, проектор, компьютеры со специализированным программным обеспечением.
2.	Семинары	№ 200(компьютерный класс №2), № 305 (компьютерный класс №3), № 403	Компьютер, проектор, компьютеры со специализированным программным

		(компьютерный класс №4).	обеспечением.
3.	Практические занятия	№ 200(компьютерный класс №2), № 305 (компьютерный класс №3), № 403 (компьютерный класс №4).	Компьютеры со специализированным программным обеспечением, проектор.

Для самостоятельной работы обучающихся используется «Зал для самостоятельной работы», оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечен доступ в электронную информационно-образовательную среду Организации.

Занятия с инвалидами по зрению, слуху, с нарушениями опорно-двигательного аппарата проводятся в специально оборудованных аудиториях по их просьбе, выраженной в письменной форме.

Автор (составитель): доцент Н.А. Гнездилова _____
(подпись)

Аннотация рабочей программы учебной дисциплины

СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

Учебная дисциплина «Системы информационной безопасности» относится к части учебного плана, формируемой участниками образовательных отношений, изучается по заочной форме обучения в ходе 2 сессии 4 курса и 1 сессии 5 курса.

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).

В результате освоения дисциплины обучающийся должен овладеть дополнительной профессиональной компетенцией ДПК-15 - Способен разрабатывать шаблоны документов требований