

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ашмарина Светлана Игоревна

Должность: Ректор ФГБОУ ВО «Самарский государственный экономический университет»

Дата подписания: 01.02.2021 15:42:03

Уникальный программный ключ:

59650034d6e3a6baac49b7bd0f8e79fea1433ff3e82f1fc7e9279a031181baba

**Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«Самарский государственный экономический университет»

Институт экономики предприятий

Кафедра Цифровых технологий и решений

УТВЕРЖДЕНО

Ученым советом Университета
(протокол № 10 от 29 апреля 2020 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.О.19 Информационная безопасность

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа
Прикладная информатика в электронной экономике

Методический отдел УМУ

« 16 » апрель 20 20 г.
Сахарова / Сахарова С.К.

Научная библиотека СГЭУ

« 16 » апрель 20 20 г.
[подпись]

Рассмотрено к утверждению

на заседании кафедры Цифровых технологий и решений

(протокол № 8 от 05.03.2020)

Зав. кафедрой [подпись] /Е.В.Погорелова/

Квалификация (степень) выпускника бакалавр

Содержание (рабочая программа)

Стр.

- 1 Место дисциплины в структуре ОП
- 2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе
- 3 Объем и виды учебной работы
- 4 Содержание дисциплины
- 5 Материально-техническое и учебно-методическое обеспечение дисциплины
- 6 Фонд оценочных средств по дисциплине

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Информационная безопасность входит в обязательную часть блока Б1. Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Алгоритмизация и программирование, Вычислительные системы, сети и телекоммуникации, Безопасность жизнедеятельности, Информационные системы и технологии, Теория вероятностей и математическая статистика, Экономика фирмы (предприятия)

Последующие дисциплины по связям компетенций: Программная инженерия, Менеджмент, Информационные системы бизнес-планирования, Электронный документооборот

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Информационная безопасность в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Общепрофессиональные компетенции (ОПК):

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Планируемые результаты обучения по дисциплине			
Описание ИДК	Описание ИДК	Описание ИДК	Описание ИДК
ОПК-3 _ИДК1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК3з1 Основные требования к информационной безопасности.	ОПК3у1 Решать нестандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности.	ОПК3вз1 Навыками анализа профессионально-практической деятельности работы с использованием основных требований информационной безопасности с применением информационно-коммуникационных технологий.
ОПК-3 _ИДК2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК3з2 Информационную и библиографическую культуру с учетом требований безопасности.	ОПК3у2 Применять при решении стандартных задач современные подходы к обработке информации с учетом ее безопасности.	ОПК3в2 Приемами обработки библиографии и информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3 _ИДК3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов,	ОПК3з3 Правила составления обзоров, аннотаций, рефератов, научных докладов, публикаций, и	ОПК3у3 Эффективно составлять обзоры, аннотации, рефераты, научные доклады, публикации, и библиографию по	ОПК3в3 Навыками создания обзоров, аннотаций, рефератов, научных докладов, публикаций, и

публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	библиографии по научно-исследовательской работе.	научно-исследовательской работе.	библиографии по научно-исследовательской работе.
--	--	----------------------------------	--

ОПК-4 - Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

Планируемые результаты обучения по дисциплине			
Описание ИДК	Описание ИДК	Описание ИДК	Описание ИДК
ОПК-4_ИДК1 Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	ОПК4з1 Основные национальные и международные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	ОПК4у1 Применять основные национальные и международные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	ОПК4в1 Навыками составления технической документации на различных этапах жизненного цикла информационной системы при использовании любой модели жизненного цикла.
ОПК-4_ИДК2 Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	ОПК4з2 Стандарты оформления технической документации.	ОПК4у2 На различных стадиях жизненного цикла информационной системы применять стандарты оформления технической документации.	ОПК4в2 Навыками использования стандартов оформления технической документации.
ОПК-4_ИДК3 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	ОПК4з3 Техническую документацию на различных этапах жизненного цикла информационной системы.	ОПК4у3 Формировать техническую документацию на различных этапах жизненного цикла информационной системы.	ОПК4в3 Приемами создания технической документации на различных этапах жизненного цикла информационной системы.

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 4
Контактная работа, в том числе:	55.15/1.53
Занятия лекционного типа	18/0.5
Занятия семинарского типа	36/1
Индивидуальная контактная работа (ИКР)	0.15/0
Групповая контактная работа (ГКР)	1/0.03
Самостоятельная работа, в том числе:	33.85/0.94
Промежуточная аттестация	19/0.53
Вид промежуточной аттестации:	
Зачет с оценкой	ЗачО
Общая трудоемкость (объем части образовательной программы): Часы	108

Зачетные единицы	3
------------------	---

заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 5
Контактная работа, в том числе:	13.15/0.37
Занятия лекционного типа	4/0.11
Занятия семинарского типа	8/0.22
Индивидуальная контактная работа (ИКР)	0.15/0
Групповая контактная работа (ГКР)	1/0.03
Самостоятельная работа, в том числе:	91.85/2.55
Промежуточная аттестация	3/0.08
Вид промежуточной аттестации:	
Зачет с оценкой	ЗачО
Общая трудоемкость (объем части образовательной программы): Часы	108
Зачетные единицы	3

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Информационная безопасность представлен в таблице.

Разделы, темы дисциплины и виды занятий

Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				
1.	Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	8	16			13	ОПК-3_ИДК1, ОПК-3_ИДК2, ОПК-3_ИДК3, ОПК-4_ИДК1, ОПК-4_ИДК2, ОПК-4_ИДК3
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	10	20			20.85	ОПК-3_ИДК1, ОПК-3_ИДК2, ОПК-3_ИДК3, ОПК-4_ИДК1, ОПК-4_ИДК2, ОПК-4_ИДК3
	Контроль	19					
	Итого	18	36	0.15	1	33.85	

заочная форма

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе	
		Лекции	Занятия семинарского типа		ИКР			ГКР
			Практич. занятия					
1.	Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	2	4			40	ОПК-3_ИДК1, ОПК-3_ИДК2, ОПК-3_ИДК3, ОПК-4_ИДК1, ОПК-4_ИДК2, ОПК-4_ИДК3	
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	2	4			51,85	ОПК-3_ИДК1, ОПК-3_ИДК2, ОПК-3_ИДК3, ОПК-4_ИДК1, ОПК-4_ИДК2, ОПК-4_ИДК3	
	Контроль	3						
	Итого	4	8	0.15	1	91.85		

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	лекция	Понятие информационной безопасности, информационной системы, видов информации. Понятия собственника информации, защиты информации, средств защиты информации. взаимодействие субъектов в информационном обмене.
		лекция	Классификация и свойства информации. Информация как объект юридической защиты.
		лекция	Понятие угрозы. Виды угроз. Источники угроз. Характер происхождения угроз: умышленные факторы, естественные факторы.

		лекция	Предпосылки появления угроз: объективные, субъективные, наиболее выраженные угрозы, опасность несанкционированного (случайного и преднамеренного) получения информации.
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	лекция	Структура правовых органов защиты информации. Правовые основы обеспечения защиты информации.
		лекция	Государственная политика информационной безопасности. Законодательство информационной безопасности.
		лекция	Архитектура систем защиты информации.
		лекция	Организационно-правовое обеспечение информационной безопасности ИС
		лекция	Государственная система правового обеспечения защиты информации в Российской Федерации. Информация и информационные услуги как продукт. Источники конфиденциальной информации в информационных системах.

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	практическое занятие	Основные понятия и определения информационной безопасности.
		практическое занятие	Классификация угроз информационной безопасности.
		практическое занятие	Характер происхождения угроз: умышленные факторы, естественные факторы.
		практическое занятие	Опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.
		практическое занятие	Направления обеспечения информационной безопасности.
		практическое занятие	Методы и средства нарушения конфиденциальности информации.
		практическое занятие	Методы и средства нарушения целостности информации.

		практическое занятие	Методы нарушения доступности.
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	практическое занятие	Направления обеспечения информационной безопасности.
		практическое занятие	Правовые основы обеспечения защиты информации.
		практическое занятие	Стандарты, используемые при создании систем информационной безопасности.
		практическое занятие	Методы нарушения конфиденциальности, целостности и доступности информации.
		практическое занятие	Защита информации от утечки по акустическим каналам.
		практическое занятие	Защита информации от утечки по электромагнитным каналам.
		практическое занятие	Системы защиты информации.
		практическое занятие	Функции и задачи защиты информации.
		практическое занятие	Информационная безопасность АИС.
		практическое занятие	Организационно-правовое обеспечение информационной безопасности АИС.

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/434171>

Дополнительная литература

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/432966>

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business
2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access, PowerPoint)
3. Project-Expert 7

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. 1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - <http://www.gov.ru/>)
2. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - <https://www.minfin.ru/ru/>)
3. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - <http://www.gks.ru/>)

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. справочно-правовая система «Консультант Плюс»
2. справочно-правовая система «ГАРАНТ-Максимум».

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и

	ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

Для проведения занятий лекционного типа используются демонстрационное оборудование и учебно-наглядные пособия в виде презентационных материалов, обеспечивающих тематические иллюстрации.

5.6 Лаборатории и лабораторное оборудование

Лаборатория информационных технологий в профессиональной деятельности	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ Лабораторное оборудование
---	--

6. Фонд оценочных средств по дисциплине Информационная безопасность:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком «+»
Текущий контроль	Оценка докладов	+
	Устный/письменный опрос	-
	Тестирование	+
	Практические задачи	-
	Оценка контрольных работ (для заочной формы обучения)	-
Промежуточный контроль	Зачет с оценкой	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования, утвержденными Ученым советом ФГБОУ ВО СГЭУ №10 от 29.04.2020г.

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Общепрофессиональные компетенции (ОПК):

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Планируемые результаты обучения по дисциплине				
Описание ИДК	Уровень сформированности	Знать	Уметь	Владеть (иметь навыки)

ОПК-3 _ИДК1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Пороговый	ОПК3з1 Основные требования к информационной безопасности.	ОПК3у1 Решать нестандартные задачи профессиональной деятельности с учетом основных требований информационно й безопасности.	ОПК3вз1 Навыками анализа профессионально-практической деятельности работы с использованием основных требований информационной безопасности с применением информационно-коммуникационных технологий.
ОПК-3 _ИДК2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Базовый	ОПК3з2 Информационную и библиографическую культуру с учетом требований безопасности.	ОПК3у2 Применять при решении стандартных профессиональных задач современные подходы к обработке информации с учетом ее безопасности.	ОПК3в2 Приемы обработки библиографии и информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3 _ИДК3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Повышенный	ОПК3з3 Правила составления обзоров, аннотаций, рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе.	ОПК3у3 Эффективно составлять обзоры, аннотации, рефераты, научные доклады, публикации, и библиографию по научно-исследовательской работе.	ОПК3в3 Навыками создания обзоров, аннотаций, рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе.

ОПК-4 - Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

Описание ИДК	Планируемые результаты обучения по дисциплине			
	Уровень сформированности	Знать	Уметь	Владеть (иметь навыки)
ОПК-4_ИДК1 Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Пороговый	ОПК4з1 Основные национальные и международные стандарты оформления технической документации	ОПК4у1 Применять основные национальные и международные стандарты оформления технической документации	ОПК4в1 Навыками составления технической документации на различных этапах жизненного цикла

		на различных стадиях жизненного цикла информационной системы.	на различных стадиях жизненного цикла информационной системы.	информационной системы при использовании любой модели жизненного цикла.
ОПК-4_ИДК2 Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	Базовый	ОПК4з2Стандарты оформления технической документации.	ОПК4у2На различных стадиях жизненного цикла информационной системы применять стандарты оформления технической документации.	ОПК4в2Навыками использования стандартов оформления технической документации.
ОПК-4_ИДК3 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Повышенный	ОПК4з3Техническую документацию на различных этапах жизненного цикла информационной системы.	ОПК4у3Формировать техническую документацию на различных этапах жизненного цикла информационной системы.	ОПК4в3Приемами создания технической документации на различных этапах жизненного цикла информационной системы.

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	ОПК-3_ИДК1, ОПК-3_ИДК2, ОПК-3_ИДК3, ОПК-4_ИДК1, ОПК-4_ИДК2, ОПК-4_ИДК3	Оценка докладов Тестирование	Зачет
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	ОПК-3_ИДК1, ОПК-3_ИДК2, ОПК-3_ИДК3, ОПК-4_ИДК1, ОПК-4_ИДК2, ОПК-4_ИДК3	Оценка докладов Тестирование	Зачет

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	1. Классификация и свойства информации. 2. Основные задачи организационно-управленческой деятельности в сфере информационной безопасности. 3. Информация как объект юридической защиты. 4. Структура и функции службы обеспечения защиты ИС на предприятии. 5. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности. 6. Управление информационной безопасностью на предприятии. 7. Деятельность международных организаций в сфере информационной безопасности.
Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	8. Методология организационного обеспечения информационной безопасности на уровне крупных поставщиков информационных систем. 9. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности. 10. Формирование политики информационной безопасности на предприятии. 11. Использование программных средств для поддержки аудита качества и надежности защиты ИС. 12. Организационная структура и персонал службы информационной безопасности на предприятии. 13. Аудит состояния информационной безопасности на предприятии. 14. Политика ИБ предприятия.

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)

<https://lms2.sseu.ru/course/index.php?categoryid=514>

Под информационной безопасностью понимается...

защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера
программный продукт и базы данных должны быть защищены от воздействия
нет правильного ответа

Защита информации – это..

комплекс мероприятий, направленных на обеспечение информационной безопасности ИС

процесс разработки структуры базы данных в соответствии с требованиями безопасности

небольшая программа для выполнения определенной задачи

От чего зависит информационная безопасность?

от компьютеров

от поддерживающей инфраструктуры

от информации

Основные составляющие информационной безопасности:

целостность

достоверность

конфиденциальность

Доступность – это...

возможность за приемлемое время получить требуемую информационную услугу

логическая независимость

нет правильного ответа

Целостность – это..

целостность информации

непротиворечивость информации

защищенность от разрушения

Конфиденциальность – это защита от несанкционированного доступа:

к защищаемой информации

к программам и программным комплексам

технологиям разработки и отладки создаваемых программных продуктов

Для чего создаются информационные системы?

получения определенных информационных услуг

обработки информации

все ответы правильные

Целостность можно подразделить на:

статическую

динамическую

структурную

Где применяются средства контроля динамической целостности?

При анализе потока финансовых сообщений

при обработке данных

при выявлении кражи, дублирования отдельных сообщений

Какие трудности возникают в информационных системах при обеспечении конфиденциальности?

сведения о технических каналах утечки информации являются закрытыми

на пути пользовательской криптографии стоят многочисленные технические проблемы

Атака – это...

попытка реализации угрозы

потенциальная возможность определенным образом нарушить информационную безопасность

программы, предназначенные для поиска необходимых программ.

Угрозы ИС можно классифицировать по нескольким критериям:
по спектру ИБ
по способу осуществления угроз
по компонентам ИС

По каким компонентам классифицируются угрозы доступности:
отказ пользователей
отказ поддерживающей инфраструктуры
ошибка в программе

Основными источниками внутренних отказов являются:
ошибки при конфигурировании системы
отказы программного или аппаратного обеспечения
выход системы из штатного режима эксплуатации

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
обрабатывать большой объем программной информации
нет правильного ответа

Вирус – это...
Код обладающий способностью к распространению путем внедрения в другие программы
Способность объекта реагировать на запрос сообразно своему типу объектов
небольшая программа для выполнения определенной задачи

Конфиденциальную информацию можно разделить:
предметную
служебную
глобальную

Виды угроз в КСЗИ:
случайные
преднамеренные
природные

Предпосылки появления угроз:
объективные
субъективные
преднамеренные

К какому виду угроз относится присвоение чужого права на СЗИ?
нарушение права собственности
нарушение содержания
внешняя среда

Отказ работы системы -это...

нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

некоторая последовательность действий, необходимых для выполнения конкретного задания

структура, определяющая последовательность выполнения и взаимосвязи процессов

Ошибка – это...

неправильное выполнение элементом одной или нескольких функций

нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

негативное воздействие на программу

Сбой – это...

такое нарушение работоспособности какого-либо элемента системы

неправильное выполнение элементом одной или нескольких функций

происходящее в следствие специфического состояния объект-метод

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета с оценкой

Раздел дисциплины	Вопросы
Основные понятия и определения информационной безопасности. Классификация угроз информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.	1. Понятие информационной безопасности, информационной системы, видов информации. 2. Понятие угрозы. Виды угроз. Источники угроз. 3. Характер происхождения угроз: умышленные факторы, естественные факторы. 4. Защита информации на уровне предприятия (организации). 5. Организационно-правовое обеспечение 6. Информационной безопасности ИС. 7. Основные угрозы конфиденциальности информации 8. Виды технических средств защиты информационных систем. 9. Основные составляющие информационной безопасности. 10. Какими принципами следует руководствоваться для обеспечения информационной безопасности сетевых конфигураций? 11. Методы обеспечения информационной безопасности
Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации. Стандарты, используемые при создании систем информационной безопасности. Архитектура систем защиты информации. Функции защиты информации.	12. Основные организационно-правовые документы по организационному обеспечению комплексной информационной безопасности предприятия. 13. Принципы организации и функционирования системы информационной безопасности предприятия (фирмы). 14. Направления деятельности службы информационной безопасности. 15. Основные функции и задачи по обеспечению информационной безопасности предприятия (фирмы); 16. Основные задачи организационно-управленческой деятельности в сфере информационной безопасности. 17. Структура и функции службы обеспечения защиты ИС на предприятии. 18. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной

	<p>безопасности.</p> <p>19. Что входит в число основных понятий ролевого управления доступом?</p> <p>20. От чего зависит информационная безопасность?</p> <p>21. Методология организационного обеспечения информационной безопасности на уровне крупных поставщиков информационных систем.</p> <p>22. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности.</p> <p>23. Аудит состояния информационной безопасности на предприятии.</p> <p>24. Формирование политики информационной безопасности на предприятии.</p> <p>25. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности.</p> <p>26. Управление информационной безопасностью на предприятии.</p> <p>27. основополагающие документы для обеспечения безопасности внутри организации</p> <p>28. Защита информации от утечки по акустическим каналам.</p> <p>29. Защита информации от утечки по электромагнитным каналам.</p> <p>30. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?</p>
--	--

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	Критерии оценивания для мероприятий контроля с применением 4-х балльной системы
«отлично»	ОПК-3_ИДК3, ОПК-4_ИДК3
«хорошо»	ОПК-3_ИДК2, ОПК-4_ИДК2
«удовлетворительно»	ОПК-3_ИДК1, ОПК-4_ИДК1
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне