Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол №10 от 30 мая 2024 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.17 Информационная безопасность

Основная профессиональная образовательная программа 38.05.01 Экономическая безопасность
Экономическая безопасность

Квалификация (степень) выпускника Экономист, Юрист

Самара 2024

Содержание (рабочая программа)

Стр.

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 часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Математика, Судебная экономическая экспертиза, Финансовая безопасность, Основы теории национальной безопасности, Философия, История государства и права России, История государства и права зарубежных стран, Экономическая теория, Основы менеджмента, История России, Организация и методика проведения налоговых проверок, Арбитражный процесс, Арбитражно-процессуальное право

Последующие дисциплины по связям компетенций: Актуальные проблемы обеспечения экономической безопасности, Нефинансовая отчетность экономических субъектов, Государственный аудит

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:

Профессиональные компетенции (ПК):

Универсальные компетенции (УК):

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
УК-1	УК-1.1: Знать:	УК-1.2: Уметь:	УК-1.3: Владеть (иметь навыки):
	понятие и содержание критического анализа, системного подхода, методы выработки стратегии действий	осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	методами осуществления критического анализа проблемных ситуаций на основе системного подхода и методами выработки стратегии действий

Профессиональные компетенции (ПК):

ПК-4 - Способен выявлять, документировать, пресекать и раскрывать преступления и иные правонарушения в сфере экономики; способность реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**

ПК-4	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	Систему юридической документации и правила их оформления, принципы правовой квалификации фактов и обстоятельств; методологию подготовки юридического заключения, методику проведения юридической консультации; принципы оценки действия правовой нормы; систему юридической терминологии, необходимой для дачи юридического заключения и юридических консультаций	юридически правильно применять методы и способы квалификации фактов и обстоятельств в практической деятельности; готовить правовые заключения анализировать юридические факты и возникающие в связи с ними правовые отношения; давать устные и письменные консультации, проводить экспертизу документов и правовых актов	приемами правовой квалификации фактов и обстоятельств, навыками подготовки правовых заключений, навыками юридического консультирования, приемами осуществления правовой экспертизы документов и правовых актов

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 9
Контактная работа, в том числе:	54.15/1.5
Занятия лекционного типа	18/0.5
Занятия семинарского типа	36/1
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	71.85/1
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	 Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

очно-заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 9
Контактная работа, в том числе:	4.15/0.12
Занятия лекционного типа	2/0.06

Занятия семинарского типа	2/0.06
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	121.85/2.38
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

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 теории информационной безопасности. Задачи защиты информации.	8	18	0,075		31,85	УК-1.1, УК-1.2, УК -1.3, ПК-4.1, ПК- 4.2, ПК-4.3
2.	Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	10	18	0,075		40,00	УК-1.1, УК-1.2, УК -1.3, ПК-4.1, ПК- 4.2, ПК-4.3
	Контроль	18					
	Итого	**18**	**36**	**0.15**		**71.85**	

очно-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 теории информационной безопасности. Задачи защиты информации.	1	1	0,075		60	УК-1.1, УК-1.2, УК -1.3, ПК-4.1, ПК- 4.2, ПК-4.3
2.	Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	1	1	0,075		61,85	УК-1.1, УК-1.2, УК -1.3, ПК-4.1, ПК- 4.2, ПК-4.3
	Контроль	18					
	Итого	**2**	**2**	0.15		**121.85**	

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 теории информационной безопасности. Задачи защиты информации.	лекция	Основные понятия теории информационной безопасности. Защита информации в России
		лекция	Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий
		лекция	Понятия предметной области «защита информации». Понятия, связанные с организацией защиты информации
		лекция	Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации.
2.	Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного	лекция	Информация как объект защиты. Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации.
		лекция	Информационные ресурсы. Структура и шкала ценности информации. Классификация

	обеспечения информационной безопасности.		информационных ресурсов. Правовой режим информационных ресурсов
		лекция	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.
		лекция	Структура государственной системы защиты информации. Угрозы информационной безопасности
		лекция	Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы

*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 теории информационной безопасности. Задачи защиты информации.	практическое занятие	Работа в одноранговой сети Windows
		практическое занятие	Основные нормативные руководящие документы информационной безопасности. Справочно-правовая система «Консультант Плюс»
		практическое занятие	Основные нормативные руководящие документы информационной безопасности. Справочно-правовая система «ГАРАНТ-Максимум
		практическое занятие	Стандарты информационного обмена
		практическое занятие	Работа с антивирусными программами
		практическое занятие	Программная реализация криптографических алгоритмов (Симметричные криптосистемы-шифр перестановки)
		практическое занятие	Программная реализация криптографических алгоритмов (алгоритмы двойных перестановок).

		практическое занятие	Программная реализация криптографических алгоритмов(Шифры простой замены)
		практическое занятие	Программная реализация криптографических алгоритмов(Шифры сложной замены)
2.	Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	практическое занятие	Асимметричные криптосистемы.
		практическое занятие	Механизмы контроля целостности данных создать ЭЦП шифрованием профиля сообщения закрытым ключом
		практическое занятие	Механизмы контроля целостности данных создание профиля дешифрованием ЭЦП открытым ключом отправителя
		практическое занятие	Защита документов MS Office
		практическое занятие	Проект «Подготовка документов для разработки проекта политики и программы информационной безопасности предприятия»
		практическое занятие	Задание 1 «Классификация угроз».
		практическое занятие	Задание 2 «Нормативно-методическое обеспечение СУИБ».
		практическое занятие	Задание 3 «Требования к кандидату на должность начальника службы безопасности коммерческой фирмы»
		практическое занятие	Задание 4 «Управление инцидентами ИБ»

** 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 теории информационной безопасности. Задачи защиты информации.	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	- 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

1.Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029

Дополнительная литература

1.Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

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

5.6 Лаборатории и лабораторное оборудование

Лаборатория информационных технологий в профессиональной деятельности	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интренет» 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	+
	Тестирование	+
	Практические задачи	+
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

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

Универсальные компетенции (УК):

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	УК-1.1: Знать:	УК-1.2: Уметь:	УК-1.3: Владеть (иметь навыки):
	понятие и содержание критического анализа, системного подхода, методы выработки стратегии действий	осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	методами осуществления критического анализа проблемных ситуаций на основе системного подхода и методами выработки стратегии действий
Пороговый	понятие критического анализа, системного подхода для выработки стратегии действий	осуществлять критический анализ проблемных ситуаций	методами осуществления критического анализа проблемных ситуаций
Стандартный (в дополнение к пороговому)	понятие и содержание критического анализа, системного подхода для выработки стратегии действий	вырабатывать стратегию действий на основе системного подхода	методами осуществления критического анализа проблемных ситуаций на основе системного подхода
Повышенный (в дополнение к пороговому, стандартному)	методы выработки стратегии действий в проблемных ситуациях	вырабатывать стратегию действий на основе системного подхода в проблемных ситуациях	методами выработки стратегии действий в проблемных ситуациях

Профессиональные компетенции (ПК):

ПК-4 - Способен выявлять, документировать, пресекать и раскрывать преступления и иные правонарушения в сфере экономики; способность реализовывать мероприятия по получению

юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	Систему юридической документации и правила их оформления, принципы правовой квалификации фактов и обстоятельств; методологию подготовки юридического заключения, методику проведения юридической консультации; принципы оценки действия правовой нормы; систему юридической терминологии, необходимой для дачи юридического заключения и юридических консультаций	юридически правильно применять методы и способы квалификации фактов и обстоятельств в практической деятельности; готовить правовые заключения анализировать юридические факты и возникающие в связи с ними правовые отношения; давать устные и письменные консультации, проводить экспертизу документов и правовых актов	приемами правовой квалификации фактов и обстоятельств, навыками подготовки правовых заключений, навыками юридического консультирования, приемами осуществления правовой экспертизы документов и правовых актов
Пороговый	систему юридической документации и правила их оформления, принципы правовой квалификации фактов и обстоятельств	юридически правильно применять методы и способы квалификации фактов и обстоятельств в практической деятельности	приемами правовой квалификации фактов и обстоятельств
Стандартный (в дополнение к пороговому)	методологию подготовки юридического заключения, методику проведения юридической консультации; принципы оценки действия правовой нормы	готовить правовые заключения анализировать юридические факты и возникающие в связи с ними правовые отношения	навыками подготовки правовых заключений
Повышенный (в дополнение	систему юридической терминологии,	давать устные и письменные	авыками юридического консультирования, приемами

к пороговому, стандартному)	необходимой для дачи юридического заключения и юридических консультаций	консультации, проводить экспертизу документов и правовых актов	осуществления правовой экспертизы документов и правовых актов

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 теории информационной безопасности. Задачи защиты информации.	УК-1.1, УК-1.2, УК- 1.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка докладов Практические работы Тестирование	Зачет
2.	Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	УК-1.1, УК-1.2, УК- 1.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка докладов Практические работы Тестирование	Зачет

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Основные понятия теории информационной безопасности. Задачи защиты информации.	1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности. 2. Понятие безопасности и её составляющие. Безопасность информации. 3. Обеспечение информационной безопасности: содержание и структура понятия. 4. Национальные интересы в информационной сфере. 5. Источники и содержание угроз в информационной сфере. 6. Соотношение понятий «информационная безопасность» и «национальная безопасность» 7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. 8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. 9. Система обеспечения информационной безопасности. 10.Обеспечение информационной безопасности Российской Федерации. 11.Понятие информационной войны. Проблемы информационной войны. 12. Информационное оружие и его классификация. 13. Цели информационной войны, её составные части и средства её

	ведения. Объекты воздействия в информационной войне. 14. Уровни ведения информационной войны. Информационные операции. Психологические операции. 15. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	16.Основные положения государственной информационной политики Российской Федерации. 17.Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. 18.Виды защищаемой информации в сфере государственного и муниципального управления. 19.Обеспечение информационной безопасности организации. 20.Характеристика эффективных стандартов по безопасности. 21.Требования к полноте эффективных стандартов по безопасности. 22.Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере. 23. Информация - фактор существования и развития общества. 24.Обеспечение информационной безопасности: содержание и структура понятия. 25.Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации. 26.Обеспечение информационной безопасности Российской Федерации. 27.Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности 28.Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. 29. Административный уровень обеспечения информационной безопасности. 30.Организационные структуры системы обеспечения информационной безопасности предприятия (организации). 31.Корпоративная нормативная база по защите информации. 32.Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия). 33.Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия). 34.Нормативно-методические документы по обеспечению безопасности информации.

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

https://lms2.sseu.ru/mod/quiz/view.php?id=1912

Обеспечение информационной безопасности не зависит от:
руководства организаций;
системных и сетевых администраторов;
внутренних пользователей;
внешних пользователей.

При анализе стоимости защитных мер не следует учитывать:
расходы на закупку оборудования
расходы на закупку программ
расходы на обучение персонала

расходы на премии персонала

В число универсальных сервисов безопасности входят:
управление доступом
управление информационными системами и их компонентами
управление носителями

Не являются сервисами безопасности:
идентификация и аутентификация
шифрование
контроль целостности
регулирование конфликтов
экранирование
обеспечение безопасного восстановления

В число архитектурных принципов, направленных на обеспечение высокой доступности информационных сервисов, не входит:
управляемость процессов, контроль состояния частей
невозможность обхода защитных средств
автоматизация процессов

Цифровой сертификат содержит:
открытый ключ удостоверяющего центра
секретный ключ удостоверяющего центра
имя удостоверяющего центра "

В число направлений физической защиты не входят:
физическая защита пользователей
защита поддерживающей инфраструктуры
защита от перехвата данных

Криптография необходима для реализации следующих сервисов безопасности:
шифрование
туннелирование
разграничение доступа

В число целей политики безопасности верхнего уровня не входит:
решение сформировать или пересмотреть комплексную программу безопасности
обеспечение базы для соблюдения законов и правил
+обеспечение конфиденциальности почтовых сообщений

В число целей программы безопасности верхнего уровня входят:
управление рисками
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

В рамках программы безопасности нижнего уровня не осуществляется:
стратегическое планирование
повседневное администрирование
отслеживание слабых мест защиты

Политика безопасности строится на основе:
общих представлений об ИС организации

изучения политик родственных организаций
анализа рисков

В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

В число целей программы безопасности верхнего уровня входят:
составление карты информационной системы
координация деятельности в области информационной безопасности
пополнение и распределение ресурсов

Контроль целостности может использоваться для:
предупреждения нарушений ИБ
обнаружения нарушений
локализации последствий нарушений

Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией органов лицензирования и сертификации по данной тематике:
да, поскольку наличие лицензий и сертификатов при прочих равных условиях является важным достоинством
нет, поскольку реально используемые продукты все равно не могут быть сертифицированы
не имеет значения, поскольку если информация о лицензиях или сертификатах понадобится, ее легко найти

Программно-технические меры безопасности не включают:
превентивные, препятствующие нарушениям информационной безопасности
меры обнаружения нарушений
меры воспроизведения нарушений

В число направлений повседневной деятельности на процедурном уровне входят:
поддержка пользователей
поддержка программного обеспечения
поддержка унаследованного оборудования

Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
способна противостоять только информационным угрозам, как внешним так и внутренним
способна противостоять только внешним информационным угрозам

Методы повышения достоверности входных данных
Отказ от использования данных
Проведение комплекса регламентных работ
Введение избыточности в документ первоисточник
Многократный ввод данных и сличение введенных значений

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)

Раздел дисциплины	Задачи
Основные понятия теории информационной безопасности. Задачи защиты информации.	Работа в одноранговой сети Windows. Основные нормативные руководящие документы информационной безопасности. Стандарты информационного обмена безопасности.
Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	Работа с антивирусными программами. Программная реализация криптографических алгоритмов. Механизмы контроля целостности данных. Защита документов MS Office.

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Основные понятия теории информационной безопасности. Задачи защиты информации.	1. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны? 2. Покажите связь между уровнем развития общества и технологиями защиты информации. 3. В каких направлениях идет развитие теории информационной безопасности в настоящее время? 4. Каков вклад российских ученых в теорию информационной безопасности? 5. С чем связан возросший интерес к проблемам защиты информации? 6. Каковы отличия формального и неформального подходов к проблемам защиты информации? 7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время? 8. Что такое информационная система? Телекоммуникационная система? Автоматизированная система? 9. Каковы правовые понятия в области защиты информации? 10. Что такое защита информации? Информационная безопасность? 11. Охарактеризуйте понятия, связанные с организацией защиты информации.

	12. Каковы основные принципы построения систем защиты информации? 13. Что такое комплексный подход к обеспечению информационной безопасности? 14. Что такое информация и каковы уровни ее представления? 15. Перечислите основные носители информации, особенности их использования и защиты. 16. Какими свойствами определяется ценность информации?
Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	17. Какие критерии оценки ценности информации Вы можете предложить? 18. Приведите примеры различной зависимости ценности информации от времени. 19. Что понимается под информационными ресурсами? 20. Что не разрешается относить к информации ограниченного доступа? 21. Что понимается под конфиденциальной информацией? 22. Какие существуют виды тайны? 23. Какое назначение имеет перечень конфиденциальных сведений предприятия? 24. Каково место информационной безопасности в системе национальной безопасности Российской Федерации? 25. Сформулируйте основные положения Доктрины информационной безопасности РФ. 26. Каковы основные цели защиты информации? 27. Каковы основные задачи в области информационной безопасности? 28. Какова структура государственной системы защиты информации? 29. Кто несет ответственность за нарушение режима защиты информации? 30. Каковы функции руководителей предприятий при организации защиты информации? 31. Каковы основные функции ФСТЭК? 32. Покажите роль различных министерств и ведомств в вопросах защиты информации. 33. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности). 34. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации. 35. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации? 36. В каких системах на первом месте стоит обеспечение доступности информации? 37. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?

	38. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.

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 2-х балльной системы**
«зачтено»	УК-1, ПК-4
«не зачтено»	Результаты обучения не сформированы на пороговом уровне