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 № 9 от 31 мая 2022 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.12 Информационная безопасность

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа Цифровые технологии в экономике

Квалификация (степень) выпускника Бакалавр

Самара 2022

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: Облачные технологии и услуги, Интеллектуальные информационные системы, Вычислительные системы, сети и телекоммуникации, Основы проектной деятельности, Инженерия знаний, Хранение, обработка и анализ данных, Системы искусственного интеллекта, Методы оптимизации и теория игр, Разработка интерфейсов и адаптивный Веб-дизайн, Технологии работы в социальных сетях, Информационно-коммуникационные технологии в профессиональной деятельности, Основы алгоритмизации и программирования, Современные технологии и языки программирования, Встроенные языки программирования, Организация вычислительных процессов

Последующие дисциплины по связям компетенций: Проектирование информационных систем, Управление ИТ-проектами, Разработка мобильных приложений, Интернет-предпринимательство, Управление качеством разработки приложений, Проектный практикум, Цифровые технологии управления предприятием, Современные цифровые платформы, Разработка профессиональных приложений

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):

ПК-2 - Способность к инженерно-технологической поддержке в ходе согласования коммерческого предложения с заказчиком

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-2	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности инженерно-технологической поддержки в ходе согласования коммерческого предложения с заказчиком	осуществлять инженерно-технологическую поддержку в ходе согласования коммерческого предложения с заказчиком	навыками инженерно-технологической поддержки в ходе согласования коммерческого предложения с заказчиком

ПК-4 - Способность к верификации структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС

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):
	особенности верификации структуры программного кода ИС относительно	верифицировать структуру программного кода ИС относительно архитектуры ИС и	навыками верификации структуры программного кода ИС относительно

	архитектуры ИС и требований заказчика к ИС	требований заказчика к ИС	архитектуры ИС и требований заказчика к ИС

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 6
Контактная работа, в том числе:	74.3/2.06
Занятия лекционного типа	36/1
Лабораторные работы (лабораторный практикум)	36/1
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	35.7/0.99
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	Экз
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 7
Контактная работа, в том числе:	6.3/0.18
Занятия лекционного типа	2/0.06
Лабораторные работы (лабораторный практикум)	2/0.06
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	103.7/2.88
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	Экз
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		
			Лаборат. работы				

1.	Организационные средства защиты информации.	18	18	0,15	1	20	ПК-2.1, ПК-2.2, ПК -2.3, ПК-4.1, ПК-4.2, ПК-4.3
2.	Технические и программные средства защиты информации.	18	18	0,15	1	15,7	ПК-2.1, ПК-2.2, ПК -2.3, ПК-4.1, ПК-4.2, ПК-4.3
	Контроль	34					
	Итого	**36**	**36**	**0.3**	**2**	**35.7**	

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 / Лаборат. работы	ИКР	ГКР		
1.	Организационные средства защиты информации.	1	1	0,15	1	60	ПК-2.1, ПК-2.2, ПК -2.3, ПК-4.1, ПК-4.2, ПК-4.3
2.	Технические и программные средства защиты информации.	1	1	0,15	1	43,7	ПК-2.1, ПК-2.2, ПК -2.3, ПК-4.1, ПК-4.2, ПК-4.3
	Контроль	34					
	Итого	**2**	**2**	0.3	2	**103.7**	

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.	Организационные средства защиты информации.	лекция	Стандартизация в управлении ИБ.
		лекция	Политика ИБ предприятия.
		лекция	Жизненный цикл политики ИБ.
		лекция	Выполнение политики ИБ.
		лекция	Процессный подход к управлению ИБ.
		лекция	Риски ИБ и их анализ.
		лекция	Система управления ИБ.
		лекция	Внедрение СУИБ.
		лекция	Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками.
2.	Технические и программные средства защиты информации.	лекция	Базовые принципы ИБ.
		лекция	Угрозы ИБ в компьютерных сетях.
		лекция	Программно-технический уровень ИБ. Архитектурная безопасность.
		лекция	Защита информации от утечек по техническим каналам.
		лекция	Защита программных средств от несанкционированного копирования и исследования.

		лекция	Защита от НСД в операционных системах Windows и Unix
		лекция	Идентификация и аутентификация пользователей, управление доступом. Протоколирование и аудит.
		лекция	Криптографические методы ЗИ, хеширование, стеганография.
		лекция	Средства антивирусной защиты.

*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.	Организационные средства защиты информации.	лабораторные работы	Изучение основных нормативноправовых документов в сфере защиты данных
		лабораторные работы	Изучение информационных сервисов для получения данных об организациях или гражданах
		лабораторные работы	Политика ИБ
		лабораторные работы	Модель угроз и модель нарушителя
		лабораторные работы	Изучение комплексных требований к системе ЗИ
		лабораторные работы	Формирование перечня конфиденциальных документов в организации
		лабораторные работы	Инвентаризация активов, анализ защищенности и управление инцидентами
		лабораторные работы	Изучение международного законодательства в сфере ЗИ
		лабораторные работы	Анализ объекта защиты
2.	Технические и программные средства защиты информации.	лабораторные работы	Изучение антивирусов и межсетевых экранов
		лабораторные работы	Изучение DLP -систем
		лабораторные работы	Знакомство с инструментами «Сканер-ВС», ITSM- инфра-менеджер, R-Vision
		лабораторные работы	Знакомство с программным анализатором трафика на на примере Wireshark
		лабораторные работы	Контроль целостности программной среды
		лабораторные работы	Проверка разрешительной системы доступа
		лабораторные работы	Изучение методов защиты от НСД в операционной системе Windows
		лабораторные работы	Изучение методов защиты от НСД в операционной системе Unix
		лабораторные работы	Изучение программ поиска и гарантированного уничтожения информации на дисках

** 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.	Организационные средства защиты информации.	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Технические и программные средства 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

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968

Дополнительная литература

1. Чекулаева, Е. Н. Управление информационной безопасностью: учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола: ПГТУ, 2020. — 154 с. Режим доступа по подписке — URL: https://e.lanbook.com/book/157473

Литература для самостоятельного изучения

1. Абденов, А. Ж. Современные системы управления информационной безопасностью: учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск: НГТУ, 2017. — 48 с. — URL: https://e.lanbook.com/book/118224

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 или GNU/Linux Ubuntu 22.04
2. Microsoft Office 365/2019/2016 (Word, Excel) или LibreOffice 7.3.3
3. WinDjView
4. Device Lock Демо-версия, система DLP
5. 10Сканер –ВС (сканер сети, демо-версия)
6. Terrier (Программа поиска и гарантированного уничтожения информации на дисках, демо-версия)
7. «Ревизор 1 XP», «Ревизор 2 XP»
8. ФИКС (контроль целостности программной среды демо-версия)
9. 10Страйк (Инвентаризация ресурсов в сети, демо-версия)
10. Инфра Менеджер-Service Desk (Управление заявками, демо-версия)

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

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	Экзамен	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования, утвержденными Ученым советом ФГАОУ ВО СГЭУ, протокол № 9 от 31.05.2022; 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

Профессиональные компетенции (ПК):

ПК-2 - Способность к инженерно-технологической поддержке в ходе согласования коммерческого предложения с заказчиком

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности инженерно-технологической поддержки в ходе согласования коммерческого предложения с заказчиком	осуществлять инженерно-технологическую поддержку в ходе согласования коммерческого предложения с заказчиком	навыками инженерно-технологической поддержки в ходе согласования коммерческого предложения с заказчиком
Пороговый	Усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен
Стандартный (в дополнение к пороговому)	Определения понятий даются неполные, допускается незначительные нарушения в последовательности	Выполняются все операции, последовательность их выполнения соответствует	В целом владение необходимыми навыками и/или имеет опыт

	изложения, небольшие неточности при использовании научных категорий, формулировки	требованиям, но действие выполняется недостаточно осознанно	
Повышенный (в дополнение к пороговому, стандартному)	Чётко и правильно даются определения, полно раскрывается содержание понятий, верно используется терминология, при этом ответ самостоятельный, использованы ранее приобретенные знания	Выполняются все операции, последовательность их выполнения достаточно хорошо продумана, действие выполняется в целом осознано	Владение всеми необходимыми навыками и/или имеет опыт

ПК-4 - Способность к верификации структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	особенности верификации структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС	верифицировать структуру программного кода ИС относительно архитектуры ИС и требований заказчика к ИС	навыками верификации структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС
Пороговый	Усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен
Стандартный (в дополнение к пороговому)	Определения понятий даются неполные, допускается незначительные нарушения в последовательности изложения, небольшие неточности при использовании научных категорий, формулировки	Выполняются все операции, последовательность их выполнения соответствует требованиям, но действие выполняется недостаточно осознанно	В целом владение необходимыми навыками и/или имеет опыт

Повышенный (в дополнение к пороговому, стандартному)	Чётко и правильно даются определения, полно раскрывается содержание понятий, верно используется терминология, при этом ответ самостоятельный, использованы ранее приобретенные знания	Выполняются все операции, последовательность их выполнения достаточно хорошо продумана, действие выполняется в целом осознано	Владение всеми необходимыми навыками и/или имеет опыт

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.	Организационные средства защиты информации.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка практических работ Тестирование	Экзамен
2.	Технические и программные средства защиты информации.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка практических работ Тестирование	Экзамен

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Организационные средства защиты информации.	Организация защиты персональных данных в образовательном учреждении.
	Построение типовой модели угроз безопасности информации медицинского учреждения.
Технические и программные средства защиты информации.	Система обеспечения защиты информации в переговорной комнате.
	Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удалённую систему.

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы
Организационные средства защиты информации.	Классификация вирусов как угрозы ИБ.
	Меры защиты информации от утечек по техническим каналам.
Технические и программные средства защиты информации.	Классификация криптографических средств защиты информации.
	Обзор стандартов и спецификаций в области ИБ.

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=1819

1. Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
Б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия
В) нет правильного ответа

2. Защита информации – это..
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

4. Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

5. Доступность – это…
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

6. Целостность – это..
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность – это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

10. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

12. Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

15. Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:

А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

20. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации

В) нет правильного ответа

22. Какие существуют грани вредоносного П.О.?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) все ответы правильные

24. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

27. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

28. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

29. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

30 .Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

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

Раздел дисциплины	**Задачи**
Организационные средства защиты информации.	Описание объекта информатизации.
	Сбор и систематизация сведений об объекте информатизации.
	Сбор и систематизация сведений об объекте информатизации для обеспечения ИБ.

	Формирование требований защищенности объекта информатизации
	Категорирование информации и других ресурсов.
	Анализ угроз и уязвимостей объекта информатизации
	Подбор и применение методики для формирования модели угроз.
	Анализ системы ИБ
	Комплексный анализ модели угроз и уязвимостей и существующих мер защиты информации.
	Комплексный анализ модели угроз и уязвимостей и существующих мер защиты информации
Технические и программные средства защиты информации.	Подбор необходимых мер и средств защиты на основе проведенного анализа.
	Подбор антивирусного программного обеспечения
	Подбор системы DLP
	Подбор программного обеспечения инвентаризации ресурсов в сети
	Подбор системы инвентаризации лицензионного программного обеспечения
	Подбор системы контроля целостности программной среды
	Подбор программного обеспечения управления заявками (Service Desk)
	Подбор программного обеспечения гарантированного уничтожения информации на дисках
	Подбор сканера уязвимостей
	Формирование комплексного проекта мер обеспечения защищенности объекта информатизации

Тематика контрольных работ

Раздел дисциплины	Темы
Организационные средства защиты информации.	Подготовка аналитической записки по результатам анализа внутреннего аудита ИБ
	Подготовка отчёта по инциденту нарушения ИБ
Технические и программные средства защиты информации.	Использование инструментов анализа трафика для выявления использования определенного программного обеспечения
	Применение методов асимметричного шифрования

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме экзамена

Раздел дисциплины	Вопросы
Организационные средства защиты информации.	1. Основные понятия науки об управлении. Понятие системы и системного подхода к защите информации. Методы моделирования систем и угроз ИБ. Понятие системы управления информационной безопасностью (СУИБ). 2. Структура ISMS. Функции управления. Законы управления. Требования к управленческому решению. Понятие процесса. Понятие процессного подхода. Процессный подход к разработке, эксплуатации, анализу, сопровождению и совершенствованию СУИБ. 3. Стандартизация в области построения систем управления. Методы формализации процессов. Стандартизация в области построения систем управления. Моделирование систем с помощью различных нотаций. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов. 4. Ролевая структура СУИБ. Политика СУИБ понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Квалификационные требования к

	руководителю службы ИБ. 5. Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.). 6. Основные понятия информационной безопасности. Политики ИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ. 7. Схема объекта информатизации. Классификация и идентификация информационных активов, Классификация ресурсов и их контроль. Категорирование активов компании. Классификация конфиденциальной информации. Основы защищенного документооборота
Технические и программные средства защиты информации.	8. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ. 9. Внедрение процессов управления ИБ: этапы и последовательность 10. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения. 11. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ. 12. Внедрение разработанных процессов. Документ «Положение о применимости» Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа. 13. Внедрение мер (контрольных процедур) по обеспечению ИБ Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик. 14. Эксплуатация и независимый аудит СУИБ. - «Внутренний аудит», «Корректирующие действия», «Предупреждающие действия». – Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). – Понятие «Зрелость процесса». – Процесс «Анализ со стороны высшего руководства». – Процесс «Обучение и обеспечение осведомленности». 15. Программные средства аудита ИБ. 16. Защита от вредоносного программного обеспечения. Планирование систем и их приёмка

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»	Повышенный ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3
«хорошо»	Стандартный ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3
«удовлетворительно»	Пороговый ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне