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 3 мая 2024 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 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: 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 - Способен 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 - Способен 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	верифицировать структуру программного кода ИС относительно архитектуры ИС и	навыками верификации структуры программного кода ИС относительно

	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

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**	

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.		лекция	Стандартизация в управлении ИБ.

	Организационные средства защиты информации.	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.		лабораторные работы	Изучение антивирусов и межсетевых экранов

	Технические и программные средства защиты информации.	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. 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

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. 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. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)
4. 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; 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 - Способен 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	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен

	недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной		
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

ПК-4 - Способен 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	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен

	доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной		
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 докладов; Устный/письменный опрос; Тестирование; Практические задачи; Оценка контрольных работ (для заочной формы обучения)	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 докладов; Устный/письменный опрос; Тестирование; Практические задачи; Оценка контрольных работ (для заочной формы обучения)	Экзамен

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Организационные средства защиты информации.	1. Организация защиты персональных данных в образовательном учреждении. 2. Построение типовой модели угроз безопасности информации медицинского учреждения.
Технические и программные средства защиты информации.	3. Система обеспечения защиты информации в переговорной комнате. 4. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удалённую систему.

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы
Организационные средства защиты информации.	1. Классификация вирусов как угрозы ИБ. 2. Меры защиты информации от утечек по техническим каналам.
Технические и программные средства защиты информации.	3. Классификация криптографических средств защиты информации. 4. 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. Что такое аутентификация?
a) Процесс проверки целостности данных
b) Процесс проверки подлинности пользователя (правильный ответ)
c) Процесс шифрования информации
d) Процесс резервного копирования данных

2. Что такое фаервол?
a) Устройство для физической защиты серверов
b) Программное обеспечение для обработки электронной почты
c) Устройство или программное обеспечение для фильтрации сетевого трафика (правильный ответ)
d) Устройство для аутентификации пользователей

3. Что означает аббревиатура DDoS?
a) Двойное шифрование данных
b) Дешифрование зашифрованных данных
c) Распределенная атака отказом в обслуживании (правильный ответ)
d) Угроза внутреннего характера для информационной безопасности

4. Какой тип атаки предполагает перехват и прослушивание сетевого трафика?
a) Вирусная атака
b) Атака "человек посередине" (Man-in-the-middle) (правильный ответ)
c) Атака отказом в обслуживании (DoS)
d) Фишинг-атака

5. Что такое шифрование данных?
a) Процесс удаления данных с носителя
b) Процесс разделения данных на несколько частей
c) Процесс преобразования данных в непонятный для посторонних вид (правильный ответ)
d) Процесс передачи данных по сети

6. Что означает аббревиатура VPN?
a) Виртуальная приватная сеть (правильный ответ)
b) Взлом персонального компьютера
c) Вирусный программный код
d) Возможность удаленного доступа к базам данных

7. Какой вид атаки связан с отправкой электронного письма, притворяющегося от имени легитимной организации с целью получения личной информации?
a) Спам-атака
b) Вирусная атака
c) Фишинг-атака (правильный ответ)
d) Атака отказом в обслуживании (DoS)

8. Что такое многофакторная аутентификация?
a) Аутентификация с использованием нескольких различных алгоритмов шифрования
b) Аутентификация с использованием нескольких физических барьеров для доступа к системе
c) Аутентификация, требующая предоставления нескольких независимых подтверждений личности пользователя (правильный ответ)
d) Аутентификация с использованием нескольких паролей

9. Какой вид атаки направлен на получение паролей путем перебора всех возможных комбинаций?
a) Фишинг-атака
b) Атака "человек посередине" (Man-in-the-middle)
c) Атака методом словаря (правильный ответ)
d) Атака отказом в обслуживании (DoS)

10. Что такое физическая безопасность?
a) Защита информации с помощью аппаратных устройств
b) Защита информации от физического доступа неавторизованных лиц (правильный ответ)
c) Защита информации с помощью программного обеспечения
d) Защита информации от внешних атак через сеть

11. Что такое политика информационной безопасности?
a) Список правил и рекомендаций по защите информации в организации (правильный ответ)
b) Программа для шифрования данных
c) Программа для мониторинга сетевого трафика
d) Методика восстановления данных после атаки

12. Какой вид атаки связан с отправкой электронного письма с вредоносным программным кодом?
a) Спам-атака
b) Вирусная атака (правильный ответ)
c) Фишинг-атака
d) Атака отказом в обслуживании (DoS)

13. Что такое бэкап данных?
a) Процесс шифрования данных
b) Процесс восстановления данных после их потери или повреждения (правильный ответ)
c) Процесс мониторинга сетевого трафика
d) Процесс удаления данных с носителя

14. Какой вид атаки связан с маскировкой вредоносного программного кода под легитимное приложление?
a) Спам-атака
b) Вирусная атака
c) Троян (правильный ответ)
d) Атака отказом в обслуживании (DoS)

15. Что такое периметр безопасности?
a) Физическое пространство вокруг серверов, защищенное физическими барьерами
b) Граница сети, на которой применяются меры защиты (правильный ответ)
c) Программа для мониторинга активности пользователей
d) Методика определения уязвимостей в сетевой инфраструктуре

16. Что такое угроза информационной безопасности "фишинг"?
a) Атака, направленная на перехват сетевого трафика
b) Атака, при которой злоумышленники отправляют электронные письма, притворяющиеся от имени легитимной организации, с целью получения личной информации (правильный ответ)
c) Атака на физическую безопасность серверов
d) Атака методом перебора паролей

17. Что такое угроза информационной безопасности "социальная инженерия"?
a) Атака, при которой злоумышленники перехватывают сетевой трафик
b) Атака, при которой злоумышленники используют манипуляции и манипулируют людьми, чтобы получить доступ к информации (правильный ответ)
c) Атака на физическую безопасность серверов
d) Атака, при которой злоумышленники перебирают пароли

18. Что такое IDS (система обнаружения вторжений)?
a) Программа для шифрования данных
b) Программа для мониторинга сетевого трафика
c) Система, предназначенная для обнаружения и предотвращения несанкционированного доступа к системе (правильный ответ)
d) Программа для резервного копирования данных

19. Что такое атака "фарминг"?
a) Атака на физическую безопасность серверовb) Атака, при которой злоумышленник создает поддельный веб-сайт, чтобы получить личную информацию пользователей (правильный ответ)
c) Атака на сетевую инфраструктуру, направленная на перехват трафика
d) Атака методом перебора паролей

20. Что такое уязвимость "нулевого дня"?
a) Уязвимость, обнаруженная в программном обеспечении в день его выпуска
b) Уязвимость, которая может быть использована злоумышленником до ее обнаружения и устранения разработчиками (правильный ответ)
c) Уязвимость, вызванная отсутствием актуальных антивирусных программ
d) Уязвимость, связанная с несанкционированным доступом к физическому оборудованию

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)
https://lms2.sseu.ru/course/index.php?categoryid=1819

Раздел дисциплины	Задачи
Организационные средства защиты информации.	1. Описание объекта информатизации. 2. Сбор и систематизация сведений об объекте информатизации. 3. Сбор и систематизация сведений об объекте информатизации для обеспечения ИБ. 4. Формирование требований защищенности объекта информатизации. 5. Категорирование информации и других ресурсов. 6. Анализ угроз и уязвимостей объекта информатизации. 7. Подбор и применение методики для формирования модели угроз. 8. Анализ системы ИБ.

	9. Комплексный анализ модели угроз и уязвимостей и существующих мер защиты информации. 10.Комплексный анализ модели угроз и уязвимостей и существующих мер защиты информации.
Технические и программные средства защиты информации.	11. Подбор необходимых мер и средств защиты на основе проведенного анализа. 12. Подбор антивирусного программного обеспечения. 13. Подбор системы DLP. 14. Подбор программного обеспечения инвентаризации ресурсов в сети. 15. Подбор системы инвентаризации лицензионного программного обеспечения. 16. Подбор системы контроля целостности программной среды. 17. Подбор программного обеспечения управления заявками (Service Desk). 18. Подбор программного обеспечения гарантированного уничтожения информации на дисках. 19. Подбор сканера уязвимостей. 20. Формирование комплексного проекта мер обеспечения защищенности объекта информатизации.

Тематика контрольных работ

Раздел дисциплины	Темы
Организационные средства защиты информации.	1. Подготовка аналитической записки по результатам анализа внутреннего аудита ИБ. 2. Подготовка отчёта по инциденту нарушения ИБ.
Технические и программные средства защиты информации.	3. Использование инструментов анализа трафика для выявления использования определенного программного обеспечения. 4. 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