МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Аудит информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Белёв А.В., старший преподаватель, Кафедра информационной безопасности

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от «____»_____20__г. , протокол № _____

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат	eg_1575874368
Номер транзакции	0000000000E9876D
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Аудит информационной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с аудитом информационной безопасности в своей профессиональной деятельности; формирование у обучаемых профессиональных компетенций в эксплуатационно-технической и научно-исследовательской областях профессиональной деятельности в соответствии с ОП специальности 10.05.03 - «Информационная безопасность автоматизированных систем».

Задачи дисциплины:

- изучение базовых понятий, методов, технологий аудита информационной безопасности организации;
- изучение отечественных и зарубежных стандартов, на основе которых осуществляется аудит информационной безопасности организации;
- освоение программных средств для проведения аудита информационной безопасности организации.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности	РД4	Знание	национальные и международные стандарты в области аудита и оценки информационной безопасности; типовые проектные решения по созданию систем обеспечения безопасности информации
			РД5	Умение	применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; контролировать эффективность принятых мер по реализации частных политик информационной безопасности

					автоматизированных систем
			РД6	Навык	способами оценки защищённости автоматизированной системы; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах	РД1	Знание	особенности проведения проверок работоспособности систем защиты информации и автоматизированных систем управления
			РД2	Умение	проводить проверки работоспособности систем защиты информации и автоматизированных систем управления, обосновывать выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований
			РД3	Навык	способностью проведения проверок работоспособности систем защиты информации и автоматизированных систем управления, методологиями оценки рисков и активов информационной безопасности

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		

Воспитание уважения к Конституции и законам Российской Федерации	Высокие нравственные идеалы	Внимательность к деталям
Формирование духовно-нравственных ценностей		
Формирование ответственного отношения к труду	Служение Отечеству и ответственность за его судьбу	Ответственность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Справедливость	Внимательность к деталям
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Взаимопомощь и взаимоуважение	Внимательность к деталям

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится в части, формируемая участниками образовательных отношений и опирается на дисциплины: Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности и небходимо для изучения дисциплин: Бизнес-процессы предприятия и их защита

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.В	9	4	55	36	0	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Общая модель процесса аудита информационной безопасности объекта	РД1	10	0	0	23	Контрольная работа, тестирование
2	Оценка безопасности информационных технологий на основе «Общих критериев»	РД2, РД3	8	0	0	22	Контрольная работа, тестирование
3	Оценка безопасности на основе Международного стандарта по управлению информационной безопасностью ISO 17799	РД4, РД5	10	0	0	22	Контрольная работа, тестирование
4	Программные средства для проведения аудита информационной безопасности	РД6	8	0	0	22	Контрольная работа, тестирование
Итого по таблице			**36**	**0**	**0**	**89**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Общая модель процесса аудита информационной безопасности объекта .

Содержание темы: Аудит безопасности и методы его проведения. Понятие аудита безопасности. Методы анализа данных при аудите ИБ. Понятие критически важного объекта. Назначение, цель аудита информационной безопасности (ИБ) объекта. Необходимость аудита ИБ. Виды аудита ИБ. Критерии аудита ИБ. Принципы аудита ИБ. Роли при проведении аудита ИБ. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Анализ информационных рисков предприятия. Методы оценивания информационных рисков. Управление информационными рисками.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

Тема 2 Оценка безопасности информационных технологий на основе «Общих критериев» .

Содержание темы: Стандарты информационной безопасности. Предпосылки создания стандартов ИБ. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии Европейских стран. Германский стандарт BS1. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT. Стандарты по безопасности информационных технологий в России Оценка безопасности информационных технологий на основе «Общих критериев» Предпосылки введения международного стандарта ISO 15408. Основные понятия общих критериев. Методология оценки безопасности информационных технологий по общим критериям Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств ОК.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: активные, интерактивные формы проведения занятий - собеседование.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

Тема 3 Оценка безопасности на основе Международного стандарта по управлению информационной безопасностью ISO 17799 .

Содержание темы: Международный стандарт управления информационной безопасностью ISO 17799Назначение стандарта ISO 17799 для управления информационной безопасностью. Практика прохождения аудита и получения сертификата ISO 17799. Международный стандарт управления информационной безопасностью ISO 17799. Политика безопасности. Организационные меры по обеспечению информационной безопасности. Классификация ресурсов и их контроль. Безопасность персонала. Физическая безопасность. Администрирование компьютерных систем и вычислительных сетей. Управление доступом к системам. Разработка и сопровождение информационных систем. Планирование бесперебойной работы организации. Соответствие системы основным требованиям.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: активные, интерактивные формы проведения занятий - собеседование.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

Тема 4 Программные средства для проведения аудита информационной безопасности.

Содержание темы: Программные средства для проведения аудита информационной безопасности. Анализ видов используемых программных продуктов. Программные средства для проведения аудита информационной безопасности. Система КОНДОР. Сетевые сканеры. Сравнительный анализ программных средств для проведения аудита ИБ.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: активные, интерактивные формы проведения занятий - собеседование.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на

всех лекционных занятиях, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, выполнение тестов, самостоятельное изучение некоторых разделов курса.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843184 (Дата обращения - 05.09.2025)
2. Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2025. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581505 (дата обращения: 01.09.2025).
3. Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 190 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581501 (дата обращения: 01.09.2025).

7.2 Дополнительная литература

1. Дронова Г. А. Аттестация и аудит информационной безопасности : Учебники [Электронный ресурс] - Новосибирск : Новосибирский государственный технический университет , 2016 - 19 - Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=575351

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронная библиотечная система «Университетская библиотека онлайн» - Режим доступа: http://biblioclub.ru/
3. Электронно-библиотечная система "ZNANIUM.COM"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Office 2010 Standard Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-1 «Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности	РД 4	Знание	национальные и международные стандарты в области аудита и оценки информационной безопасности; типовые проектные решения по созданию систем обеспечения безопасности информации	решение тестовых заданий
	РД 5	Умение	применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем	выполнение контрольной работы
	РД 6	Навык	способами оценки защищённости автоматизированной системы; методами мониторинга и аудита, выявления угроз ин	выполнение контрольной работы

			формационной безопасности автоматизированных систем	

Компетенция ПКВ-2 «Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах	РД 1	Знание	особенности проведения проверок работоспособности систем защиты информации и автоматизированных систем управления	ответы на вопросы
	РД 2	Умение	проводить проверки работоспособности систем защиты информации и автоматизированных систем управления, обосновывать выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований	выполнение контрольной работы
	РД 3	Навык	способностью проведения проверок работоспособности систем защиты информации и автоматизированных систем управления, методологиями оценки рисков и активов информационной безопасности	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : особенности проведения проверок работоспособности систем защиты информации и автоматизированных систем управления	1.1. Общая модель процесса аудита информационной безопасности объекта	Тест	Опрос

РД2	Умение : проводить проверки работоспособности систем защиты информации и автоматизированных систем управления, обосновывать выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований	1.2. Оценка безопасности информационных технологий на основе «Общих критериев»	Контрольная работа	Опрос
РД3	Навык : способностью проведения проверок работоспособности систем защиты информации и автоматизированных систем управления, методологиями оценки рисков и активов информационной безопасности	1.2. Оценка безопасности информационных технологий на основе «Общих критериев»	Контрольная работа	Опрос
РД4	Знание : национальные и международные стандарты в области аудита и оценки информационной безопасности; типовые проектные решения по созданию систем обеспечения безопасности информации	1.3. Оценка безопасности на основе Международного стандарта по управлению информационной безопасностью ISO 17799	Тест	Опрос
РД5	Умение : применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем	1.3. Оценка безопасности на основе Международного стандарта по управлению информационной безопасностью ISO 17799	Контрольная работа	Опрос
РД6	Навык : способами оценки защищённости автоматизированной системы; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	1.4. Программные средства для проведения аудита информационной безопасности	Контрольная работа	Опрос

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Самостоятельная работа	Экзамен	Итого

Лекционные занятия	22			22
Контрольная работа		58		58
Промежуточная аттестация			20	20
Итого	22	58	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примерные темы для опроса

1. Определить термины: аудит информационной безопасности объекта (организации, автоматизированной системы), свидетельство аудита информационной безопасности
2. Назначение, цель аудита ИБ объекта.
3. Принципы аудита ИБ.
4. Роли при проведении аудита ИБ В чём заключается взаимодействие аудиторской организации с проверяемой организацией?
5. Каковы методы сбора и получения свидетельств аудита ИБ?
6. Способы проведения анализа свидетельств аудита ИБ Каково содержание отчёта и заключения по результатам аудита ИБ?
7. Методы измерения атрибутов оценки. Способы формирования основной меры
8. Привести примеры формирования производной меры
9. Привести примеры формирования аналитической модели
10. Способы интерпретации результатов оценки
11. Построить фрагмент методики оценки соответствия ИБ требованиям нормативных документов с использованием анкет для измерения атрибутов объекта оценки (для выбранной области обеспечения ИБ)
12. Построить фрагмент методики оценки соответствия ИБ требованиям нормативных документов с использованием метрик для измерения атрибутов объекта оценки (для выбранной области обеспечения ИБ)

13. Построить фрагмент методики процессно-ориентированной оценки ИБ (для различных уровней возможности процессов)
14. Процессы планирования программы аудита ИБ
15. Процессы реализации и поддержки программы аудита ИБ.
16. Процессы контроля и совершенствование программы аудита ИБ

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.

5.2 Примеры тестовых заданий

1. Что является главной задачей аудита информационной безопасности?
- A) Проверка соблюдения налогового законодательства.
- B) Проверка соответствия уровня защиты информации нормативным актам и стандартам.
- C) Контроль доходов и расходов компании.
- D) Проверка личной жизни сотрудников.

2. Кто вправе осуществлять аудит информационной безопасности в компании?
- A) Только государственные органы.
- B) Только аккредитованные иностранные компании.
- C) Любые третьи лица без специальной аккредитации.
- D) Специально обученные специалисты, обладающие необходимыми квалификационными характеристиками.

3. Какие из перечисленных этапов НЕ входят в классический процесс аудита информационной безопасности?
- A) Планирование аудита.
- B) Сбор и анализ доказательств.
- C) Составление акта приема-передачи имущества.
- D) Подготовка и презентация отчета руководству.

4. Какой международный стандарт преимущественно используется для оценки и аудита систем информационной безопасности?
- A) ISO 9001.
- B) ISO 27001.
- C) ISO 14001.
- D) ISO 31000.

5. Что такое Gap Analysis в аудите информационной безопасности?
- A) Анализ рыночных тенденций.
- B) Метод анализа разрыва между текущим положением дел и установленными требованиями или целями.
- C) Анализ рисков сотрудников компании.

- D) Оценка производительности серверов.

6. Какая модель информационной безопасности предусмотрена стандартом ISO 27001?

- A) PBAC (Policy Based Access Control).
- B) ABAC (Attribute Based Access Control).
- C) MAC (Mandatory Access Control).
- D) SMART (Specific Measurable Achievable Realistic Time-bound).

7. Что такое Risk Heat Map (карта рисков) в аудите информационной безопасности?

- A) Карта территории с зонами максимальной концентрации персонала.
- B) Графическое представление приоритетов и интенсивности рисков.
- C) Диаграмма расхода электроэнергии в здании.
- D) Тепловой график нагрузки на серверы.

8. В чем заключается обязанность руководителя компании по закону РФ в области защиты информации?

- A) Предоставлять отчетность в налоговые органы.
- B) Обеспечивать защиту информации и исполнение нормативных требований.
- C) Организовывать курсы повышения квалификации сотрудников.
- D) Поддерживать чистую окружающую среду.

9. Почему необходимо периодически повторять аудит информационной безопасности?

- A) Потому что это улучшает репутацию компании.
- B) Чтобы подтвердить соответствие актуальным нормативным требованиям и своевременно устранять выявленные недостатки.
- C) Для экономии средств компании.
- D) Чтобы увеличить долю рынка.

10. Зачем нужен аудит информационной безопасности перед покупкой крупного пакета программных средств или аппаратных комплексов?

- A) Для уменьшения налога на имущество.
- B) Для оптимизации штата сотрудников.
- C) Для оценки рисков и уязвимостей будущего комплекса и соответствия новым требованиям безопасности.
- D) Для облегчения процесса закупки.

11. Какие из перечисленных методов используются для оценки информационной безопасности?

- A) Benchmarking.
- B) Penetration testing.
- C) Risk matrix approach.
- D) Zero-day exploits discovery.

12. Какие угрозы информационной безопасности выделяет закон РФ «О персональных данных»?

- A) Потеря или повреждение информации.
- B) Неправомерный доступ третьих лиц.
- C) Утечка информации.
- D) Неблагоприятные погодные условия.

13. Какие этапы включает процесс аудита информационной безопасности согласно стандарту ISO 27001?

- A) Планирование аудита.
- B) Согласование сроков и бюджетов.
- C) Проведение обследования и интервью.
- D) Подготовка и выпуск отчета.

14. Какие методы и приемы используются для аудита защиты персональных данных?

- A) Анализ договорных отношений с контрагентами.

- B) Изучение технических средств защиты.
- C) Проверка уровня подготовки сотрудников в области информационной безопасности.
- D) Экспериментальное разрушение систем.

15. Какие инструменты используются для тестирования защищенности web-сервисов?

- A) Wireshark.
- B) Metasploit Framework.
- C) OpenVAS.
- D) Notepad++.

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.3 Итоговая контрольная работа

Представьте, что вы назначены ведущим специалистом по аудиту информационной безопасности крупной торговой компании. Вам поручено составить план первого этапа аудита. Какие основные задачи и этапы должны быть включены в ваш план? Приведите краткий перечень (примерно пять пунктов).

Краткие методические указания

Необходимо представить себя в роли ведущего специалиста по аудиту информационной безопасности крупной торговой компании и сформировать первый этап плана аудита. Ниже приводится краткий перечень задач и этапов, которые должны быть включены в план.

Ваш план должен содержать следующие основные задачи и этапы:

1. **Ознакомление с объектом аудита:**
   - Изучение структуры компании, профиля деятельности, географии филиалов и технологических процессов.
2. **Сбор и анализ первичной документации:**
   - Ознакомление с действующей политикой информационной безопасности, внутренними приказами, положениями и должностными инструкциями.
3. **Интервьюирование сотрудников:**
   - Проведение бесед с ключевыми лицами (ИТ-отдел, служба безопасности, администрация, менеджеры отделов) для выяснения текущей ситуации и проблемных моментов.
4. **Первичное обследование информационной инфраструктуры:**
   - Оценка текущего состояния серверов, сетевого оборудования, систем видеонаблюдения, охраны и прочих средств защиты.
5. **Определение ключевых рисков и угроз:**
   - Предварительная оценка основных рисков и уязвимостей, связанных с обработкой и хранением информации компании.

Шкала оценки

Оценка	Баллы	Описание

5	45-58	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	30-44	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	14-29	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-13	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.