МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ

Проректор по учебной работе

_____ ___Василенко В.Н.__
(подпись) (Ф.И.О.)

«25» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Аудит информационных технологий и систем обеспечения информационной безопасности

(наименование дисциплины)

Направление подготовки (специальность)

10.05.03 – Информационная безопасность автоматизированных систем
(шифр и наименование направления подготовки/специальности)

Направленность (профиль)

Безопасность открытых информационных систем
(наименование профиля/специализации)

Квалификация выпускника

Специалист по защите информации

(в соответствии с Приказом Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изменениями и дополнениями)

Воронеж

1. Цели и задачи дисциплины

1. Целью освоения дисциплины (модуля) является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

- 06.033 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах) и *Разработка систем защиты информации автоматизированных систем, формирование требований к защите информации в автоматизированных системах*.

Дисциплина направлена на решение задач профессиональной деятельности следующих типов:

- *эксплуатационного типа:*
  - *разработка эксплуатационной документации на системы защиты информации автоматизированных систем;*
- *проектного типа:*
  - *разработка проектных решений по защите информации в автоматизированных системах;*
  - *разработка архитектуры системы защиты информации автоматизированной системы;*
- *научно-исследовательского типа:*
  - *обоснование необходимости защиты информации в автоматизированной системе.*

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 10.05.03 – Информационная безопасность автоматизированных систем

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	*ПКв-7*	*Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем*	*ИД2 $_{ПКВ-7}$ - владеет навыками оценки технико-экономической целесообразности создания системы защиты информации автоматизированной системы*
			ИД3 $_{ПКВ-7}$ - формировать научно-техническую документацию для создания систем защиты информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2 $_{ПКВ-7}$ - владеет навыками оценки технико-экономической	Знает: организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны,

целесообразности создания системы защиты информации автоматизированной системы	технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	Умеет: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности
	Владеет: методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ИДЗ $_{ПКВ-7}$ - формировать научно-техническую документацию для создания систем защиты информации	Знает: методики формирования научно-технической документации при создании систем защиты информации
	Умеет: выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем
	Владеет: навыками проведения лицензирования и сертификации средств защиты информации

3. Место дисциплины (модуля) в структуре ООП ВО/СПО

Дисциплина относится к *обязательной части и ОП ВО* . Дисциплина является обязательнойк изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин: *«Информационная безопасность», «Криптографические протоколы и стандарты», «Организационное и правовое обеспечение информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем», «Защита конфиденциальной информации»*.

Знания, полученные в ходе изучения дисциплины, используются при подготовке к ГИА.

4. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины (модуля) составляет __4__ зачетные единицы.

Виды учебной работы	**Всего астрономических часов**	**Всего академических часов**	**Распределение трудоемкости по семестрам, ак. ч**
			Семестр А
			Акад. ч
Общая трудоемкость дисциплины (модуля)	**108**	**144**	**144**
Контактная работа в т. ч. аудиторные занятия:	**68,25**	**91**	**91**
Лекции	13,5	18	18
в том числе в форме практической подготовки	-	-	-
Практические занятия	27	36	36
в том числе в форме практической подготовки	27	36	36
лабораторные занятия	27	36	36
в том числе в форме практической подготовки	27	36	36
Консультации текущие	0,675	0,9	0,9
Вид аттестации: зачет	**0,075**	0,1	0,1
Самостоятельная работа:	**39,75**	**53**	**53**
Проработка материалов по лекциям, учебным пособиям	18,75	25	25
Подготовка к практическим и лабораторным занятиям	18,75	25	25
Домашнее задание, реферат,	2,25	3	3

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, ак.ч

1	Введение. Виды аудита ИТ и СОИБ	Исследование процесса возникновения и развития аудита информационных технологий и систем обеспечения информационной безопасности. Определение аудита ИТ и СОИБ. Активный аудит: внешний и внутренний. Экспертный аудит. Аудит на соответствие стандартам. Комплексный аудит. Основные виды ИТ-аудита: цели, задачи, краткая характеристика. ИТ-аудит при подготовке компании к сертификации по международным стандартам. ИТ-аудит перед реструктуризацией ИТ-подразделений. ИТ-аудит перед внедрением информационной системы. ИТ-аудит перед внедрением систем управления конфигурацией ИТ-инфраструктуры.	14,3
2	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской Федерации. Обзор зарубежного законодательства в области аудита ИТ и СОИБ	Обзор российского законодательства в области аудита ИТ. Обзор российского законодательства в области информационной безопасности. Закон "Об информации, информационных технологиях и о защите информации". Обзор зарубежного законодательства в области аудита: COBIT. Уровни описания процедуры аудита по COBIT. Основные критерии оценки процессов управления ИТ. Обзор зарубежного законодательства в области информационной безопасности	14,3
3	Международная ассоциация аудита и контроля информационных систем ISACA. Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.	История возникновения ISACA. Этапы развития. Роль в системе аудита за рубежом. Основные выполняемые функции. Проводимые сертификации. Институт управления ИТ. История. Определение. Стратегии Cobit. Политики Cobit. Стандарты Cobit. Процедуры Cobit. Этапы построения работы по Cobit.	14,3
4	Методики проведения аудита	Четыре подхода к созданию методик аудиторских проверок. Основные положения методики. Особенности проведения аудита в условиях компьютерной обработки данных	14,3
5	Организация работы ИТ-отдела. Организация управления аппаратными и программными ресурсами в организации	Методологии и подходы к организации ИТ инфраструктуры. Существующие подходы к управлению ИТ отделом. Система управления проектами. Scrum. Категоризация проблем ИТ-службы. Оптимизация работы ИТ-отдела. Управление аппаратными ресурсами. Управление программным обеспечением. Прикладное ПО.	14,3
6	Аудит информационных систем как часть ИТ-стратегии фирмы	Типы предприятий и фирм. Планирование развития предприятия. Миссия предприятия. Стратегия развития информационных технологий на предприятии. Структура процесса инвестирования в информационные технологии. Использование стандарта ISO/IEC 15288. Метод «выбор/контроль/оценка». Использование модели зрелости. ИТ-стратегия.	14,3
7	Характеристика систем управления конфигурацией ИТ-инфраструктуры: Systems Management Server 2003, HP OpenView, IT ServiceBridge.	Продукты для управления ИТ-инфраструктурой: System Center Configuration Manager, IT Service Bridge, IBM Tivoli Business Systems Manager.	14,3
8	Организация аудита информационных систем с помощью ITIL.	История возникновения библиотеки ITIL. Структура ITIL. Процесс управления инцидентами. Процесс управления проблемами. Процесс управления конфигурациями. Процесс управления изменениями. Процесс управления релизами. Процесс управления уровнем услуг. Процесс управления мощностями (ёмкостью). Процесс управления доступностью. Процесс управления непрерывностью. Процесс управления финансами.IT Service Management.	14,3
9	Оценка рисков ИТ и информационной безопасности	Определение риска ИТ и риска СОИБ. Отличия. Риски ИТ: риск несущественный, риск умеренный, риск средний, риск высокий. Критерии аудита. Методика Frap. Методика CRAMM. Методика	14,3

		Microsoft. Методика RiskWatch. Методология OCTAVE.	
10	Автоматизированные решения аудита ИТ и СОИБ. Отчет по итогам аудита информационных систем.	«RA2 the art of risk». Структура отчета по аудиту.	14,3
	Консультации текущие		0,9
	Зачет		0,1

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	Практические занятия, ак. ч	Лабораторные занятия, ак. ч	СРО, ак. ч
1	Введение.	1	2	2	5
2	Виды аудита ИТ и СОИБ	1	2	2	5
3	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской Федерации.	2	4	4	5
4	Обзор зарубежного законодательства в области аудита ИТ и СОИБ	2	4	4	5
5	Международная ассоциация аудита и контроля информационных систем ISACA.	2	4	4	5
6	Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.	2	4	4	5
7	Методики проведения аудита	2	4	4	5
8	Организация работы ИТ-отдела.	2	4	4	6
9	Организация управления аппаратными и программными ресурсами в организации	2	4	4	6
10	Аудит информационных систем как часть ИТ- стратегии фирмы	2	4	4	6
	Консультации текущие	0,9			
	Зачет,	0,1			

*****в форме практической подготовки

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Введение. Виды аудита ИТ и СОИБ	Исследование процесса возникновения и развития аудита информационных технологий и систем обеспечения информационной безопасности. Определение аудита ИТ и СОИБ. Активный аудит: внешний и внутренний. Экспертный аудит. Аудит на соответствие стандартам. Комплексный аудит. Основные виды ИТ-аудита: цели, задачи, краткая характеристика. ИТ-аудит при подготовке компании к сертификации по международным стандартам. ИТ-аудит перед реструктуризацией ИТ-подразделений. ИТ-аудит перед внедрением информационной системы. ИТ-аудит перед внедрением систем управления конфигурацией ИТ-инфраструктуры.	1
2	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской	Обзор российского законодательства в области аудита ИТ. Обзор российского законодательства в области информационной безопасности. Закон "Об информации, информационных технологиях и о защите информации".	1

	Федерации. Обзор зарубежного законодательства в области аудита ИТ и СОИБ	Обзор зарубежного законодательства в области аудита: COBIT. Уровни описания процедуры аудита по COBIT. Основные критерии оценки процессов управления ИТ. Обзор зарубежного законодательства в области информационной безопасности	
3	Международная ассоциация аудита и контроля информационных систем ISACA. Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.	История возникновения ISACA. Этапы развития. Роль в системе аудита за рубежом. Основные выполняемые функции. Проводимые сертификации. Институт управления ИТ. История. Определение. Стратегии Cobit. Политики Cobit. Стандарты Cobit. Процедуры Cobit. Этапы построения работы по Cobit.	2
4	Методики проведения аудита	Четыре подхода к созданию методик аудиторских проверок. Основные положения методики. Особенности проведения аудита в условиях компьютерной обработки данных	2
5	Организация работы ИТ-отдела. Организация управления аппаратными и программными ресурсами в организации	Методологии и подходы к организации ИТ инфраструктуры. Существующие подходы к управлению ИТ отделом. Система управления проектами. Scrum. Категоризация проблем ИТ-службы. Оптимизация работы ИТ-отдела. Управление аппаратными ресурсами. Управление программным обеспечением. Прикладное ПО.	2
6	Аудит информационных систем как часть ИТ-стратегии фирмы	Типы предприятий и фирм. Планирование развития предприятия. Миссия предприятия. Стратегия развития информационных технологий на предприятии. Структура процесса инвестирования в информационные технологии. Использование стандарта ISO/IEC 15288. Метод «выбор/контроль/оценка». Использование модели зрелости. ИТ-стратегия.	2
7	Характеристика систем управления конфигурацией ИТ-инфраструктуры: Systems Management Server 2003, HP OpenView, IT ServiceBridge.	Продукты для управления ИТ-инфраструктурой: System Center Configuration Manager, IT Service Bridge, IBM Tivoli Business Systems Manager.	2
8	Организация аудита информационных систем с помощью ITIL.	История возникновения библиотеки ITIL. Структура ITIL. Процесс управления инцидентами. Процесс управления проблемами. Процесс управления конфигурациями. Процесс управления изменениями. Процесс управления релизами. Процесс управления уровнем услуг. Процесс управления мощностями (ёмкостью). Процесс управления доступностью. Процесс управления непрерывностью. Процесс управления финансами.IT Service Management.	2
9	Оценка рисков ИТ и информационной безопасности	Определение риска ИТ и риска СОИБ. Отличия. Риски ИТ: риск несущественный, риск умеренный, риск средний, риск высокий. Критерии аудита. Методика Frap. Методика CRAMM. Методика Microsoft. Методика RiskWatch. Методология OCTAVE.	2
10	Автоматизированные решения аудита ИТ и СОИБ. Отчет по итогам аудита информационных систем.	«RA2 the art of risk». Структура отчета по аудиту.	2

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Наименование лабораторных работ	Трудоемкость, ак. ч

1	Введение. Виды аудита ИТ и СОИБ	Исследование процесса возникновения и развития аудита информационных технологий и систем обеспечения информационной безопасности. Определение аудита ИТ и СОИБ. Активный аудит: внешний и внутренний. Экспертный аудит. Аудит на соответствие стандартам. Комплексный аудит. Основные виды ИТ-аудита: цели, задачи, краткая характеристика	1
		ИТ-аудит при подготовке компании к сертификации по международным стандартам. ИТ-аудит перед реструктуризацией ИТ-подразделений. ИТ-аудит перед внедрением информационной системы. ИТ-аудит перед внедрением систем управления конфигурацией ИТ-инфраструктуры.	1
2	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской Федерации. Обзор зарубежного законодательства в области аудита ИТ и СОИБ	Обзор российского законодательства в области аудита ИТ. Обзор российского законодательства в области информационной безопасности. Закон "Об информации, информационных технологиях и о защите информации". Обзор зарубежного законодательства в области аудита:	1
		COBIT. Уровни описания процедуры аудита по COBIT.Основные критерии оценки процессов управления ИТ. Обзор зарубежного законодательства в области информационной безопасности	1
3	Международная ассоциация аудита и контроля информационных систем ISACA. Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.	История возникновения ISACA. Этапы развития. Роль в системе аудита за рубежом.	1
		Основные выполняемые функции. Проводимые сертификации. Институт управления ИТ. История.	1
		Определение. Стратегии Cobit. Политики Cobit. Стандарты Cobit..	1
		Процедуры Cobit. Этапы построения работы по Cobit	1
4	Методики проведения аудита	Четыре подхода к созданию методик аудиторских проверок. Основные положения методики.	2
		Особенности проведения аудита в условиях компьютерной обработки данных	2
5	Организация работы ИТ-отдела. Организация управления аппаратными и программными ресурсами в организации	Методологии и подходы к организации ИТ инфраструктуры. Существующие подходы к управлению ИТ отделом..	1
		Система управления проектами. Scrum. Категоризация проблем ИТ-службы. Оптимизация работы ИТ-отдела	1
		Управление аппаратными ресурсами.	1
		Управление программным обеспечением. Прикладное ПО.	1
6	Аудит информационных систем как часть ИТ-стратегии фирмы	Типы предприятий и фирм. Планирование развития предприятия. Миссия предприятия.	1
		Стратегия развития информационных технологий на предприятии.	1
		Структура процесса инвестирования в информационные технологии.	1
		Использование стандарта ISO/IEC 15288. Метод «выбор/контроль/оценка». Использование модели зрелости. ИТ-стратегия.	1
7	Характеристика систем управления конфигурацией ИТ-инфраструктуры: Systems Management Server 2003, HP OpenView, IT ServiceBridge.	Продукты для управления ИТ-инфраструктурой: System Center Configuration Manager, IT Service Bridge, IBM Tivoli Business Systems Manager.	4
8	Организация аудита информационных систем с помощью ITIL.	История возникновения библиотеки ITIL. Структура ITIL. Процесс управления инцидентами.	1
		Процесс управления проблемами. Процесс управления	1

		конфигурациями. Процесс управления изменениями.	
		Процесс управления релизами. Процесс управления уровнем услуг. Процесс управления мощностями (ёмкостью).	1
		Процесс управления доступностью. Процесс управления непрерывностью. Процесс управления финансами.IT ServiceManagement.	1
9	Оценка рисков ИТ и информационной безопасности	Определение риска ИТ и риска СОИБ.	1
		Отличия. Риски ИТ: риск несущественный, риск умеренный, риск средний, риск высокий.	1
		Критерии аудита. Методика Frap. Методика CRAMM.	1
		Методика Microsoft. Методика RiskWatch. Методология OCTAVE.	1
10	Автоматизированные решения аудита ИТ и СОИБ. Отчет по итогам аудита информационных	«RA2 the art of risk». Структура отчета по аудиту.	4

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Наименование лабораторных работ	Трудоемкость, ак. ч
1	Введение. Виды аудита ИТ и СОИБ	Исследование процесса возникновения и развития аудита информационных технологий и систем обеспечения информационной безопасности. Определение аудита ИТ и СОИБ. Активный аудит: внешний и внутренний. Экспертный аудит. Аудит на соответствие стандартам. Комплексный аудит. Основные виды ИТ-аудита: цели, задачи, краткая характеристика	1
		ИТ-аудит при подготовке компании к сертификации по международным стандартам. ИТ-аудит перед реструктуризацией ИТ-подразделений. ИТ-аудит перед внедрением информационной системы. ИТ-аудит перед внедрением систем управления конфигурацией ИТ-инфраструктуры.	1
2	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской Федерации. Обзор зарубежного законодательства в области аудита ИТ и СОИБ	Обзор российского законодательства в области аудита ИТ. Обзор российского законодательства в области информационной безопасности. Закон "Об информации, информационных технологиях и о защите информации". Обзор зарубежного законодательства в области аудита:	1
		COBIT. Уровни описания процедуры аудита по COBIT.Основные критерии оценки процессов управления ИТ. Обзор зарубежного законодательства в области информационной безопасности	1
3	Международная ассоциация аудита и контроля информационных систем ISACA. Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.	История возникновения ISACA. Этапы развития. Роль в системе аудита за рубежом.	1
		Основные выполняемые функции. Проводимые сертификации. Институт управления ИТ. История.	1
		Определение. Стратегии Cobit. Политики Cobit. Стандарты Cobit..	1
		Процедуры Cobit. Этапы построения работы по Cobit	1
4	Методики проведения аудита	Четыре подхода к созданию методик аудиторских проверок. Основные положения методики.	2
		Особенности проведения аудита в условиях компьютерной обработки данных	2

5	Организация работы ИТ-отдела. Организация управления аппаратными и программными ресурсами в организации	Методологии и подходы к организации ИТ инфраструктуры. Существующие подходы к управлению ИТ отделом..	1
		Система управления проектами. Scrum. Категоризация проблем ИТ-службы. Оптимизация работы ИТ-отдела	1
		Управление аппаратными ресурсами.	1
		Управление программным обеспечением. Прикладное ПО.	1
6	Аудит информационных систем как часть ИТ- стратегии фирмы	Типы предприятий и фирм. Планирование развития предприятия. Миссия предприятия.	1
		Стратегия развития информационных технологий на предприятии.	1
		Структура процесса инвестирования в информационные технологии.	1
		Использование стандарта ISO/IEC 15288. Метод «выбор/контроль/оценка». Использование модели зрелости. ИТ-стратегия.	1
7	Характеристика систем управления конфигурацией ИТ-инфраструктуры: Systems Management Server 2003, HP OpenView, IT ServiceBridge.	Продукты для управления ИТ-инфраструктурой: System Center Configuration Manager, IT Service Bridge, IBM Tivoli Business Systems Manager.	4
8	Организация аудита информационных систем с помощью ITIL.	История возникновения библиотеки ITIL. Структура ITIL. Процесс управления инцидентами.	1
		Процесс управления проблемами. Процесс управления конфигурациями. Процесс управления изменениями.	1
		Процесс управления релизами. Процесс управления уровнем услуг. Процесс управления мощностями (ёмкостью).	1
		Процесс управления доступностью. Процесс управления непрерывностью. Процесс управления финансами.IT ServiceManagement.	1
9	Оценка рисков ИТ и информационной безопасности	Определение риска ИТ и риска СОИБ.	1
		Отличия. Риски ИТ: риск несущественный, риск умеренный, риск средний, риск высокий.	1
		Критерии аудита. Методика Frap. Методика CRAMM.	1
		Методика Microsoft. Методика RiskWatch. Методология OCTAVE.	1
10	Автоматизированные решения аудита ИТ и СОИБ. Отчет по итогам аудита информационных	«RA2 the art of risk». Структура отчета по аудиту.	4

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Введение.	Проработка материалов по лекциям, учебникам, учебным пособиям	2

	Виды аудита ИТ и СОИБ	Подготовка к практическим/лабораторным занятиям	2
		Домашнее задание, реферат	1
2	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской Федерации. Обзор зарубежного законодательства в области аудита ИТ и СОИБ	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
3	Международная ассоциация аудита и контроля информационных систем ISACA. Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
4	Методики проведения аудита	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
5	Организация работы ИТ-отдела. Организация управления аппаратными и программными ресурсами в организации	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
6	Аудит информационных систем как часть ИТ-стратегии фирмы	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
7	Характеристика систем управления конфигурацией ИТ-инфраструктуры: Systems Management Server 2003, HP OpenView, IT ServiceBridge.	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
8	Организация аудита информационных систем с помощью ITIL.	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
		Домашнее задание, реферат	1
9	Оценка рисков ИТ и информационной безопасности	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
		Домашнее задание, реферат	1
10	Автоматизированные решения аудита ИТ и СОИБ. Отчет по итогам аудита информационных	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим/лабораторным занятиям	3
		Домашнее задание, реферат	1

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

Для освоения дисциплины обучающийся может использовать:

6.1 Основная литература

1. Защита Web-приложений [Текст] : учебное пособие / А. В. Скрыпников [и др.] ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2020. - 75 с. - 25 экз. + Электрон. ресурс. - http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1766. - Библиогр.: с. 73-74. - ISBN 978-5-00032-469-1

2. Безопасность систем баз данных [Текст] : учебное пособие / А. В. Скрыпников [и др.] ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2015. - 139 с. - 55 экз. + Электрон. ресурс. - http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1098. - http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1098. - Библиогр.: с. 140. - ISBN 978-5-00032-122-5

3. Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2016. — 201 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155246 (дата обращения: 11.09.2021). — Режим доступа: для авториз. пользователей.

4. Безопасность систем баз данных [Текст] : учебное пособие / А. В. Скрыпников [и др.] ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2015. - 139 с. - 55 экз. + Электрон. ресурс. - http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1098. - http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1098. - Библиогр.: с. 140. - ISBN 978-5-00032-122-5

5. Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 269 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 11.09.2021). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.

6.2 Дополнительная литература

1. Арабян, К. К. Аудит: теория, организация, методика и практика / К. К. Арабян. – Москва : Юнити-Дана, 2020. – 480 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615684 (дата обращения: 11.09.2021). – Библиогр: 409-426. – ISBN 978-5-238-03310-5. – Текст : электронный.

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 11.09.2021). – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Аудит информационных технологий и систем обеспечения информационной безопасности [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 – «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2016. - 20 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1420.

2. Данылив, М. М. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс]: методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж: ВГУИТ, 2016. – 32 с. Режим доступа в электронной среде:

http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813.

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*http://www.edu.ru/index.php*
Научная электронная библиотека	*http://www.elibrary.ru/defaulttx.asp?*
Федеральная университетская компьютерная сеть России	*http://www.runnet.ru/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://www.window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*http://minobrnauki.gow.ru*
Портал открытого on-line образования	*http://npoed.ru*
Информационно-коммуникационные технологии в образовании. Система федеральных образовательных порталов	*http://www.ict.edu.ru/*
Электронная образовательная среда ФГБОУ ВО «ВГУИТ	*http://education.vsuet.ru*

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – *ОС Windows; Microsoft Office, LibreOffice, Альт-образование 8.2.*

7 Материально-техническое обеспечение дисциплины (модуля)

Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий	*Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГА-ТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920*	*Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор)Бесплатное ПО; Adobe Acrobat Reader (Бесплатное ПО); Adobe Flash Player (Бесплатное ПО); FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12(Заменен на AVP Kaspersky)Бесплатное ПО; VMWare Player (Бесплатное ПО); Антивирус "Зоркий глаз" (Бесплатное ПО); Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free Pascal (Бесплатное ПО); Страж NT вер.3.0 Сертификат ФСТЭК No 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК No 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК No 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК No1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК No3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК No1973*

		09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013
Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий	*Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570),средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума, стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2шт.; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920*	*Microsoft Windows 7 (64 разрядная) Профессинальная Лицензия (DreamSpark); Microsoft Windows 2003 Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор) Бесплатное ПО; Adobe Acrobat Reader Бесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file manager Бесплатное ПО; Google Chrome Бесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec Pack Бесплатное ПО; Mozilla Firefox Бесплатное ПО; Oracle VM VirtualBox Бесплатное ПО; Sublime Text Бесплатное ПО; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky) Бесплатное ПО; VMWare Player Бесплатное ПО; Антивирус "Зоркий глаз" Бесплатное ПО; Lazarus (аналог Delphi) Бесплатное ПО; Smath Studio (аналог Mathcad) Бесплатное ПО; NanoCAD (аналог Autocad) Бесплатное ПО; Gimp (графичский редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор) Бесплатное ПО; Virtual Dub (видео редактор) Бесплатное ПО; Free Pascal Бесплатное ПО (ауд.420) Страж NT вер.3.0 Сертификат ФСТЭК No 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК No 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК No 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК No1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК No3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК No1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013*
Аудитории для самостоятельной работы, курсового и дипломного проектирования	*Читальные залы библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами; Ауд.424: Комплекты мебели для учебного процесса. Количество ПЭВМ – 12 (рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2 шт.), стенды – 3*	

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине (модулю)

Оценочные материалы (ОМ) для дисциплины (модуля) включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины (модуля).**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Аудит информационных технологий и систем обеспечения информационной безопасности

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	*ПКв-7*	*Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем*	*ИД2 $_{ПКВ-7}$ - владеет навыками оценки технико-экономической целесообразности создания системы защиты информации автоматизированной системы*
			ИД3 $_{ПКВ-7}$ - формировать научно-техническую документацию для создания систем защиты информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2 $_{ПКВ-7}$ - владеет навыками оценки технико-экономической целесообразности создания системы защиты информации автоматизированной системы	Знает: организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.
	Умеет: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности
	Владеет: методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
ИД3 $_{ПКВ-7}$ - формировать научно-техническую документацию для создания систем защиты информации	Знает: методики формирования научно-технической документации при создании систем защиты информации
	Умеет: выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.
	Владеет: навыками проведения лицензирования и сертификации средств защиты информации.

№ п/п	Перечень компетенций		Этапы формирования компетенций		
	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПКв-7	Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; методики формирования научно-технической документации при создании систем защиты информации	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.	методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыками проведения лицензирования и сертификации средств защиты информации.

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Введение. Виды аудита ИТ и СОИБ	ПКв-7	Банк тестовых заданий (промежуточное тестирование, зачет)	1-5	Проверка преподавателем
			Реферат	53-55	Контроль преподавателем
			Кейс-задание(тестирование, зачет)	71	Проверка преподавателем
			Вопросы к зачету	81-82	
2	Обзор нормативно-правовой базы в области аудита ИТ и СОИБ в Российской Федерации. Обзор зарубежного законодательства в области аудита ИТ и СОИБ		Банк тестовых заданий (промежуточное тестирование, зачет)	6-10	Проверка преподавателем
			Реферат	56-58	Контроль преподавателем
			Кейс-задание	72	Проверка преподавателем
			Вопросы к зачету	83-84	
3	Международная ассоциация аудита и контроля информационных систем ISACA. Стандарт COBIT: основные понятия, структура стандарта, цели, задачи, показатели.		Банк тестовых заданий (промежуточное тестирование, зачет)	11-15	Проверка преподавателем
			Реферат	59-60	Контроль преподавателем
			Кейс-задание	73	Проверка преподавателем
			Вопросы к зачету	85-86	
4	Методики проведения аудита		Банк тестовых заданий (промежуточное тестирование, зачет)	16-20	Проверка преподавателем
			Реферат	61-62	Контроль преподавателем
			Кейс-задание	74	Проверка преподавателем
			Вопросы к зачету	87-88	
5	Организация работы ИТ-отдела. Организация управления аппаратными и программными ресурсами в организации		Банк тестовых заданий (промежуточное тестирование, зачет)	21-25	Проверка преподавателем
			Реферат	63-64	Контроль преподавателем

			Кейс-задание	75	Проверка преподавателем
			Вопросы к зачету	89-90	
6	Аудит информационных систем как часть ИТ- стратегии фирмы		Банк тестовых заданий (промежуточное тестирование, зачет)	25-30	Проверка преподавателем
			Реферат	65-66	Контроль преподавателем
			Кейс-задание	76	Проверка преподавателем
			Вопросы к зачету	91-92	
7	Характеристика систем управления конфигурацией ИТ-инфраструктуры: Systems Management Server 2003, HP OpenView, IT ServiceBridge.		Банк тестовых заданий (промежуточное тестирование, зачет)	31-35	Проверка преподавателем
			Реферат	67	Контроль преподавателем
			Кейс-задание	77	Проверка преподавателем
			Вопросы к зачету	93-94	
8	Организация аудита информационных систем с помощью ITIL.		Банк тестовых заданий (промежуточное тестирование, зачет)	36-40	Проверка преподавателем
			Реферат	68	Контроль преподавателем
			Кейс-задание	78	Проверка преподавателем
			Вопросы к зачету	95-96	
9	Оценка рисков ИТ и информационной безопасности		Банк тестовых заданий (промежуточное тестирование, зачет)	41-45	Проверка преподавателем
			Реферат	69	Контроль преподавателем
			Кейс-задание	79	Проверка преподавателем
			Вопросы к зачету	97	
10	Автоматизированные решения аудита ИТ и СОИБ. Отчет по итогам аудита информационных систем.		Банк тестовых заданий (промежуточное тестирование, зачет)	46-52	Проверка преподавателем
			Реферат	70	Контроль преподавателем
			Кейс-задание	80	Проверка преподавателем
			Вопросы к зачету	98	

3 Оценочные материалы для промежуточной аттестации.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной дисциплины.

Испытание промежуточной аттестации обучающегося по дисциплине «Аудит информационных технологий и систем обеспечения информационной безопасности» в форме тестирования, решения кейс-заданий, собеседования и выполнения реферата. Собеседование применяется при защите лабораторных работ. В течение семестра проводятся промежуточные тестирования.

Аттестация обучающегося по дисциплине проводится в форме собеседования (зачета).

Каждый вариант тестовых заданий включает в себя:

- 15 контрольных тестовых заданий, из них 8 на проверку знаний, 4 на проверку умений и 3 на проверку навыков;
- одну кейс-задачу на проверку умений или навыков.

Зачет проводится в форме теста.

Каждый билет включает в себя:

- 30 контрольных тестовых заданий, из них 20 на проверку знаний, 5 на проверку умений и 5 на проверку навыков;
- Одно кейс-задание на проверку умений.

3.1 Тесты (задания для промежуточного тестирования)

3.1.1 ***Шифр и наименование компетенции*** **ПКв-7** – Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем

№ зада-ния	примеры тестовых заданий
1	Внедрение информационных технологий требует четкого осознания: **а) Сущности деятельности хозяйствующего субъекта в целом и его бизнес-операций в частности.** b) Причин внедрения. c) Целевых установок хозяйствующего субъекта. d) Последствий от такого внедрения.
2	2. Недооценка важности информационных технологий приводит: **а) К резкому дефициту квалифицированных специалистов, способных выявлять степень их надежности.** b) К ненадлежащему их применению. c) К отказу от их использования в современных условиях развития общества. d) К потребности привлечения сторонних специалистов.
3	Цель аудита информационной инфраструктуры -это: **а) Обследование и описание ее состояния во взаимосвязи с целями управления информационными технологиями.** b) Выявление, оценка и подтверждение надлежащего характера знаний о ней. c) Выявление потоков циркуляции информационных потоков, а также подтверждение достоверности информации. d) Подтверждение достоверности информации.
4	Аудит информационной инфраструктуры - это: **а) Один из первостепенных шагов в совершенствовании современных хозяйствующих субъектов.** b) Сопутствующая аудиту услуга. c) Проверка информации, поддерживаемой ею. d) Инвентаризация аппаратно-программных средств хозяйствующего субъекта.
5	Аудит информационных технологий регламентируется: a) Международными стандартами аудита. **b) Федеральными правилами (стандартами) аудиторской деятельности.** c) Внутрифирменными стандартами аудиторской организации. d) Стандартом Cobit.
6	Продолжите фразу: «Стандарт Cobit раскрывает лучший практический опыт ...».

	a) ... на уровне управления аппаратными средствами b) ... на уровне доменов и отдельных процессов; **c) ... на уровне доменов и отдельных процессов, а также регламентирует действия в виде управляемой и логичной структуры.** **d)** ... на уровне управления программными средствами
7	В сфере информационных технологий представление сервисов предполагает: **a) наличие надлежащей системы и методологии внутреннего контроля;** b) только управление ими; c) любые действия управленческого характера. d) оказание всех видов услуг.
8	Система контроля, основанная на требованиях Стандарта Cobit: **a) Определяет основные ресурсы информационных технологий, на которые должны осуществляться воздействия.** b) Не предполагает функции контроля. c) Направлена только на проектирование информационной инфраструктуры. d) Направлена только на контроль информационной инфраструктуры
9	Первая версия стандарта Cobit выпущена: a) В 1973 г. b) В 1980 г. c) В 1998 г. **d) В 1996 г.**
10	Концептуальное ядро стандарта Cobit определяет: **a) набор основополагающих принципов и понятий в области управления информационными технологиями;** b) объекты контроля; c) объекты и задачи управления. d) контролирующие субъекты.
11	Концептуальное ядро стандарта Cobit сгруппировано: **a) В 4 домена.** b) В 34 домена. c) В 6 доменов. d) В 8 доменов.
12	Набор инструментов внедрения в стандарте Cobit содержит: **a) разъяснение ключевых положений стандарта, а также алгоритм процесса их внедрения;** b) перечень инструментов внедрения информационных технологий; c) перечень инструментов внедрения программных средств. d) перечень инструментов внедрения аппаратных средств.
13	«Руководство по аудиту» стандарта Cobit представляет собой: **a) Книгу, ориентированную на аудит ИТ-процессов.** b) Книгу, ориентированную на осуществление инвентаризации аппаратных средств. c) Требования к аудиторским процедурам проверки информации. d) Критерии к аудиторским процедурам проверки информации.
14	Информационная инфраструктура - это: **a) Технология и устройства, которые обеспечивают работу приложений.** b) Набор аппаратных средств, применяемых хозяйствующим субъектом. c) Организационная структура персонала, обслуживающего информационные технологии.
15	Сохранение неадекватного уровня информационных технологий влечет за собой: **a) Принятие неадекватных или несвоевременных управленческих решений и полному разрушению бизнеса.** b) Только трудности в управлении бизнес-процессами. c) Хаотичность в информационных потоках. d) Лишние затраты на ручную обработку информации.
16	Какое количество видов услуг предлагают аудиторские компании по аудиту информационной инфраструктуры? a) 4 вида. b) 1 вид. c) Не предлагают вообще. **d) 6 видов.**
17	Обследование информационных технологий предполагает: **a) Всего лишь сбор информации (инвентаризация) для проведения последующих работ.** b) Оценку ИТ-проектов. c) Оценку возможности перепрофилирования информационной инфраструктуры.

	d) Сбор информации (инвентаризация) для последующего оформления отчета.
18	Аудит ИТ-процессов - это: **a) Аудит информационных технологий, критичных для выполнения конкретного бизнес-процесса, с заданными критериями качества и эффективности.** b) Оценка обоснованности инвестиций в информационные технологии. c) Подготовка рекомендаций по улучшению работы отдельного элемента информационной инфраструктуры. d)
19	Технический аудит информационных технологий предполагает: **a) Сбор и анализ информации, а также подготовку рекомендаций по улучшению работы отдельного технического элемента информационной инфраструктуры.** b) Выявление применяемых аппаратных средств. c) Оценку адекватности ИТ-операций. d) Выявление применяемых программных средств.
20	Выберите правильное окончание фразы: «Комплексный аудит информационной инфраструктуры предполагает ...». a) .. .проведение экспертизы ИТ-процессов; **b) ...определение и анализ взаимосвязей бизнес-процессов и их требований, информационных и смежных технологий, совокупности программно-аппаратных средств с целью выявления ее адекватности потребностям бизнеса;** c) ... исследование взаимосвязей бизнес-процессов и ИТ-процессов. d) .проведение экспертизы некоторых процессов;
21	Какие стандарты регламентируют аудит информационных технологий? **a) Cobit.** b) IAS. c) МСФО. d) ISA.
22	В ходе проведения аудита, основанного на стандарте Cobit, аудитор: **a) Содействует системе управления аудируемым субъектом в надлежащей организации управления информационными технологиями.** b) Выявляет недостатки в ИТ-процессах. c) Проводит экспертизу аппаратно-программных средств. d) Выдает рекомендации по устранению выявленных недостатков в ИТ-процессах.
23	Основной целью аудита информационных технологий, согласно требованиям стандарта Cobit, является: **a) Предоставление обоснованных гарантий эффективного выполнения задач управления этими технологиями.** b) Обеспечение менеджмента проверенной информацией. c) Выражение мнения о достоверности информации, выдаваемой с помощью этих технологий.
24	Для оценки механизма управления стандарт Cobit рекомендует использовать: a) Классическую модель аудиторского цикла. b) Модель анализа рисков. c) Оба утверждения не верны. **d) a) или b)**
25	Алгоритм модели анализа рисков, согласно требованиям Стандарта Cobit, начинается: **a) с оценки ИТ-ресурсов;** b) с анализа угроз и уязвимостей; c) с анализа уязвимостей; d) с анализа угроз.
26	На каких принципах основана классическая модель аудиторского цикла, рекомендованная стандартом Cobit? **a) В модели критерии аудиторского исследования определяются стандартами.** b) В модели методы и подходы к аудиту стандартизированы. **c) В модели даны лишь общие направления аудирования.** d) В модели критерии аудиторского исследования определяются политикой ИБ организации.
27	Приступая к аудиту информационных технологий, аудитор должен учитывать, что стандарт Cobit: **a) Служит лишь в качестве методологической основы разработки индивидуальных методик.** b) Регламентирует все процедуры аудита. c) Раскрывает все возможные критерии для аудиторских исследований. d) Раскрывает все возможные свидетельства.

28	В целях повышения эффективности проведения аудита информационных технологий аудитор должен в каждом конкретном случае аудирования: **a) Планировать выполнение задания.** b) Сформировать перечень необходимых мероприятий и процедур. c) Воспользоваться стандартизированной и унифицированной методикой исследования. d) Все утверждения не верны.
29	Основная роль руководства аудируемого субъекта при аудите информационных технологий: a) Оказывать всестороннюю поддержку аудирующему субъекту в уточнении наиболее значимых проблем. b) Оказывать всестороннюю поддержку аудирующему субъекту в подготовке информационного обеспечения аудиторского исследования. **c) Оба утверждения a) и c) верны.** d) Не оказывать всестороннюю поддержку аудирующему субъекту в уточнении наиболее значимых проблем.
30	Письмо согласования задания на аудит информационной инфраструктуры: a) Может иметь произвольный характер. b) Должно отразить понимание проблем клиента аудирующим субъектом. c) Должно отражать предметные области и объекты предстоящего исследования. d) Является основой для подготовки договора (контракта). **e) Все утверждения верны.**
31	На этапе подготовки проекта договора необходимо: a) Установить трудоемкость работ. b) Определить график выполнения работ. c) Определить сроки аудирования в целом и по этапам. **d) Все утверждения верны.**
32	Проект договора на аудит информационной инфраструктуры направляется: a) Акционерам субъекта. b) Собственникам аудируемого субъекта. **c) Руководству аудируемого субъекта.** d) Попечителям аудируемого субъекта.
33	Какие процедуры должен осуществить аудитор на этапе предварительного планирования аудита информационных технологий? **a) Уточнить цели аудиторского задания.** b) Подготовить письмо согласования задания. c) Уточнить задание. d) Подготовить договор на проведение аудита.
34	Выберите правильное окончание фразы «Этап предварительного планирования...». a) .. .по своему масштабу занимает значительный период планирования. **b) .. должен завершаться наиболее точной формулировкой основных проблем.** c) .. .следует завершать письмом согласования задания d) ...следует завершить подписанием договора (контракта).
35	В зависимости от целевой направленности на этапе предварительного планирования необходимо собрать информацию: a) О деятельности аудируемого субъекта и отдельных его структурных звеньях. b) О внешнем окружении аудируемого субъекта. c) О производственной сфере аудируемого субъекта. **d) Все утверждения верны.** e) Все утверждения не верны. f) Только a) и c).
36	На основании собранной на этапе предварительного планирования информации аудирующая группа проводит: a) Консультации со специалистами-экспертами. b) Обобщение и классификацию этой информации. d) Формирует программу всех аудитов. **c) a) и b).**
37	Для надлежащего планирования аудита информационных технологий наиболее значимым аспектом является: a) Оценка и анализ существующих бизнес-рисков. b) Оценка и анализ потенциальных бизнес-рисков. **c) a) и b).** d) Наличие группы специалистов-экспертов.
38	Принцип проверяемости предполагает:

	a) Наличие условий для аудирующей группы проводить достаточное и надлежащее аудиторское исследование. b) Наличие информации, которую можно проверить. c) Существование вероятности, что проведенное аудиторское исследование будет способствовать эффективности функционирования информационных технологий.
39	Логическим завершением этапа планирования аудита информационных технологий является: a) Разработка стратегической модели аудиторского исследования. **b) Формирование плана аудирования.** c) Разработка детальной программы аудита.
40	На этапе стратегического планирования аудита информационных технологий аудитору необходимо поняты a) Весь бизнес аудируемого субъекта. b) Основные бизнес-процессы аудируемого субъекта. **c) ИТ-процессы.** d) Бизнес-процессы и ИТ-процессы.
41	Под информационной безопасностью понимается: a) Формирование политики информационной безопасности. b) Выбор контрмер. **c) Защищенность информации и поддерживающей ее информационной инфраструктуры.** d) Оценка и управление рисками
42	При формировании политики информационной безопасности необходимо: a) Определить используемые нормативно-правовые акты, руководства и стандарты в области ИБ. b) Определить подходы к управлению рисками. c) Структурировать контрмеры по уровням. **d) Все утверждения верны.** e) Определить границы системы управления ИБ.
43	В соответствии с выбранной стратегией управления рисками аудитору необходимо: a) Определить комплекс контрмер, структурированных по уровням, а также отдельным аспектам ИБ. **b) Проверить соответствие выбранных контрмер декларированным в политике безопасности целям.** c) Оба утверждения верны. d) Оба утверждения не верны.
44	Основными целями аудита информационной безопасности являются: a) Исследование и анализ рисков, связанных с возможностью угроз безопасности в отношении ресурсов информационных технологий. b) Выражение мнения о достоверности финансовой отчетности. c) Оценка текущего уровня защищенности информационной инфраструктуры. **d) a) и c).**
45	Проводя интервьюирование ответственных лиц хозяйствующего субъекта, аудитор должен получить сведения: a) О владельцах и пользователях информации. b) Об основных видах функционирующих приложений. c) О входах в ИТ-процессы. **d) Все утверждения верны.**
46	Сколько подходов к анализу информационной безопасности рекомендует к применению международный опыт? a) 2 подхода. b) Базовый подход, основанный на стандартах. c) Подход, основанный на анализе рисков. **d) 3 подхода.**
47	Допустимо ли использование комбинации базового подхода и основанного на анализе рисков при аудите информационной безопасности? a) Да. **b) Нет.** c) Возможно. d) Не исключено.
48	Что должен выяснить аудитор при исследовании информационной безопасности? **a) Может ли быть нанесен ущерб аудируемому субъекту в результате прохождения удаленной или локальной атаки на ИТ-ресурсы.** b).

	c) Может ли быть нанесен ущерб субъекту в результате стихийных бедствий. d) а) и Ь).
49	Что является логическим завершением аудита информационной безопасности? a) Выводы, полученные по результатам аудита по существу проблем. b) Экспертное заключение. **c) Аудиторский отчет.** d) Взыскание.
50	Что представляет собой «адресат» в аудиторском отчете? a) Адрес аудиторской компании. b) Адрес аудируемого субъекта. **c) Указание на субъект, которому предоставляется отчет.** d) Адрес ИС в глобальной сети.
51	Что представляет раздел аудиторского отчета, раскрывающий масштаб аудита? a) В нем указывается то, что аудит выполнен на основе стандартов или соответствующих норм. b) В нем указываются места размещения аппаратно-программных средств. c) В нем указываются обоснованные классы угроз. **d) Все утверждения не верны.** e) Все утверждения верны.
52	Кто подписывает аудиторский отчет? a) Представитель аудируемого субъекта и аудирующего субъекта. **b) Аудитор, проводящий аудит.** c) Руководитель аудиторской компании. d) Директор.

3.2 Темы докладов

3.2.1 ***Шифр и наименование компетенции*** **ПКв-7** – Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем

53	Планирование аудита информационных систем
54	Виды аудита информационных систем и их характеристика.
55	Аудит информационных систем: понятие, цели, задачи, проблемы, этапы проведения.
56	Методика проведения аудита информационных систем.
57	История возникновения и развития аудита информационных систем.
58	ИТ- инфраструктура: понятие, цели, задачи, виды, состав, безопасность.
59	Регламентация аудита информационных систем
60	Обзор рынка аудита информационных систем в России
61	Аудит информационной безопасности: цели и задачи.
62	Методика проведения аудита информационной безопасности.
63	Организация управления аппаратными ресурсами в организации
64	Аудит информационных систем как часть ИТ- стратегии фирмы.
65	Интернет в инфраструктуре новых информационных технологий.
66	Международная ассоциация аудита и контроля информационных систем ISACA..
67	Компании – системные интеграторы.
68	Оформление результатов аудита информационной системы.
69	Ввод СОИБ в эксплуатацию: возможные проблемы и способы их решения
70	Методики оценки текущего состояния ИС.

3.3. Кейс-задания

3.2.1 ***Шифр и наименование компетенции*** **ПКв-7** – Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности

создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем

№ задания	Формулировка задания
71	К вам за аудитом ИБ обратился владелец Интернет-ресурса, на котором пользователи: - размещают свои личные объявления, в т.ч. загружают фалы и фотографии; - обмениваются контактными данными - не проводят платежи. Составьте: - список дополнительных вопросов, чтобы определить критерии аудита ИБ; - определите подходящие критерии аудита ИБ; - определите область аудита ИБ. Ответ: *Список доп. вопросов:* сколько локаций затрагивает Интернет-ресурс (хостинг, обслуживание); сколько человек его обслуживает (ИТ и ИБ); какой состав ИТ-инфраструктуры (узлы и их кол-во); есть ли аутсорсинг; есть ли локальные акты по ИБ; есть ли ограничения по времени? *Критерии аудита ИБ:* Локальные акты (если есть); Требования по линии персональных данных (ФЗ-152, ПП РФ № 1119); контроли из ISO/IEC 27001 (прил. А); OWASP Top Ten Proactive Controls 2018; отсутствие уязвимостей из OWASP Top 10 *Область аудита ИБ:* локаций (хостинг, обслуживание); разработчики, ИТ и ИБ персонал, аутсорсеры (если есть); процессы обработки и обеспечения ИБ; серверное оборудование, АРМ персонала, СЗИ; время
72	К вам за аудитом ИБ обратился руководитель компании по разработке iOS-приложений, в которой: - разрабатывается ПО. - обрабатываются персональные данные. Составьте: - список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным); - подготовьте план аудита ИБ (таблица); - определите состав группы по аудиту ИБ (количественный и ролевой состав). - определите какие способы сбора информации целесообразно было бы использовать (список)? - какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств Ответ: - Список доп. вопросов: какие каналы взаимодействия можно использовать, в т.ч. вопросы конфиденциальности; наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и т.п.)?

- План аудита ИБ: см. слайд № 25 из 2-ого занятия

N	Наименование этапа	Дата начала	Длительность, раб. дни	Примечание
1	Предварительное совещание	09.03.23	0,125	1 час
2	Получение документации	10.03.23	2	
3	Анализ полученной документации	12.03.23	2	
4	Проведение интервью	16.03.23	5	График интервью предоставляется отдельно, каждое интервью не более 45 мин.
5	Использование инструментальных средств	16.03.23	5	График использования инструментальных средств предоставляется отдельно
6	Подготовка отчета	22.03.23	5	
7	Заключительное совещание	29.03.23	0,125	1 час

- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных данных; аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018; тех. эксперт по OWASP Top 10
- Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа документов (если есть); получение данных от инструментальных средств
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.

73

К вам за аудитом ИБ обратился владелец, на котором пользователи:
- размещают свои личные объявления, в т.ч. загружают файлы и фотографии;
- обмениваются контактными данными
- не проводят платежи.

Составьте:
- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать (список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
- Список доп. вопросов: какие каналы взаимодействия можно использовать, в т.ч. вопросы конфиденциальности; наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и т.п.)?
- План аудита ИБ: см. слайд № 25 из 2-ого занятия

N	Наименование этапа	Дата начала	Длительность, раб. дни	Примечание
1	Предварительное совещание	09.03.23	0,125	1 час
2	Получение документации	10.03.23	2	
3	Анализ полученной документации	12.03.23	2	
4	Проведение интервью	16.03.23	5	График интервью предоставляется отдельно, каждое интервью не более 45 мин.
5	Использование инструментальных средств	16.03.23	5	График использования инструментальных средств предоставляется отдельно
6	Подготовка отчета	22.03.23	5	
7	Заключительное совещание	29.03.23	0,125	1 час

- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных

<table>
<tr><td></td><td>данных; аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018; тех. эксперт по OWASP Top 10
- Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа документов (если есть); получение данных от инструментальных средств
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.</td></tr>
<tr><td>74</td><td>К вам за аудитом ИБ обратился директор школы, в информационной системе которой обрабатываются персональные данные:
- ведется база данных обучающихся, в т.ч. загружают файлы и фотографии;
- контактные данные.
Составьте:
- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать (список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
- Список доп. вопросов: какие каналы взаимодействия можно использовать, в т.ч. вопросы конфиденциальности; наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и т.п.)?
- План аудита ИБ: см. слайд № 25 из 2-ого занятия
<table><tr><th>№</th><th>Наименование этапа</th><th>Дата начала</th><th>Длительность, раб. дни</th><th>Примечание</th></tr><tr><td>1</td><td>Предварительное совещание</td><td>09.03.23</td><td>0,125</td><td>1 час</td></tr><tr><td>2</td><td>Получение документации</td><td>10.03.23</td><td>2</td><td></td></tr><tr><td>3</td><td>Анализ полученной документации</td><td>12.03.23</td><td>2</td><td></td></tr><tr><td>4</td><td>Проведение интервью</td><td>16.03.23</td><td>5</td><td>График интервью предоставляется отдельно, каждое интервью не более 45 мин.</td></tr><tr><td>5</td><td>Использование инструментальных средств</td><td>16.03.23</td><td>5</td><td>График использования инструментальных средств предоставляется отдельно</td></tr><tr><td>6</td><td>Подготовка отчета</td><td>22.03.23</td><td>5</td><td></td></tr><tr><td>7</td><td>Заключительное совещание</td><td>29.03.23</td><td>0,125</td><td>1 час</td></tr></table>- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных данных; аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018; тех. эксперт по OWASP Top 10
- Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа документов (если есть); получение данных от инструментальных средств
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.</td></tr>
<tr><td>75</td><td>К вам за аудитом ИБ обратился владелец компании, которая предоставляет различные IT услуги:
- предоставление информации безопасности внутри компании;
- установка и поддержка аппаратного и программного обеспечения другим компаниям.
Составьте:
- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать</td></tr>
</table>

<table>
<tr><td></td><td>(список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
- Список доп. вопросов: какой состав ИТ-инфраструктуры наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам, есть ли локальные акты по ИБ?
- План аудита ИБ:

- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; помощник
<table>
<tr><th>№</th><th>Наименование этапа</th><th>Дата начала</th><th>Длительность раб. дни</th><th>Примечание</th></tr>
<tr><td></td><td>Предварительное совещание</td><td>07.02.23</td><td>0,125</td><td>1 час</td></tr>
<tr><td></td><td>Получение документации</td><td>08.02.23</td><td>2</td><td></td></tr>
<tr><td></td><td>Анализ полученной документации</td><td>10.02.23</td><td>2</td><td></td></tr>
<tr><td></td><td>Проведение интервью</td><td>12.02.23</td><td>5</td><td></td></tr>
<tr><td></td><td>Использование инструментальных средств</td><td>17.02.23</td><td>5</td><td></td></tr>
<tr><td></td><td>Подготовка отчёта</td><td>22.02.23</td><td>5</td><td></td></tr>
<tr><td></td><td>Заключительное совещание</td><td>27.02.23</td><td>0,125</td><td>1 час</td></tr>
</table>
руководителя по аудиту ИБ; технический эксперт.
- Способы сбора информации: проведение интервью с разработчиками, ИТ- и ИБ-специалистами; проведение анализа документов; получение данных от инструментальных средств.
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.</td></tr>
<tr><td>76</td><td>К вам за аудитом ИБ обратился владелец интернет-биржи труда.

Составьте:
- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать (список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных данных; аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018; тех. эксперт по OWASP Top 10
- Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа документов (если есть); получение данных от инструментальных средств
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.</td></tr>
<tr><td>77</td><td>К вам за аудитом ИБ обратился директор КБ, все технологические процессы которого автоматизированы.

Составьте:</td></tr>
</table>

<table>
<tr><td></td><td>- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать (список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
- Список доп. вопросов: какие каналы взаимодействия можно использовать, в т.ч. вопросы конфиденциальности; наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и т.п.)?
- План аудита ИБ: см. слайд № 25 из 2-ого занятия

<table>
<tr><th>№</th><th>Наименование этапа</th><th>Дата начала</th><th>Длительность, раб. дни</th><th>Примечание</th></tr>
<tr><td>1</td><td>Предварительное совещание</td><td>09.03.23</td><td>0,125</td><td>1 час</td></tr>
<tr><td>2</td><td>Получение документации</td><td>10.03.23</td><td>2</td><td></td></tr>
<tr><td>3</td><td>Анализ полученной документации</td><td>12.03.23</td><td>2</td><td></td></tr>
<tr><td>4</td><td>Проведение интервью</td><td>16.03.23</td><td>5</td><td>График интервью предоставляется отдельно, каждое интервью не более 45 мин.</td></tr>
<tr><td>5</td><td>Использование инструментальных средств</td><td>16.03.23</td><td>5</td><td>График использования инструментальных средств предоставляется отдельно</td></tr>
<tr><td>6</td><td>Подготовка отчета</td><td>22.03.23</td><td>5</td><td></td></tr>
<tr><td>7</td><td>Заключительное совещание</td><td>29.03.23</td><td>0,125</td><td>1 час</td></tr>
</table>

- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных данных; аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018; тех. эксперт по OWASP Top 10
- Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа документов (если есть); получение данных от инструментальных средств
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.</td></tr>
<tr><td>78</td><td>К вам за аудитом ИБ обратился владелец компании, в которой пользователи могут заказывать консультации по различным аспектам в сфере IT
- обрабатываются ПД
-

Составьте:
1. список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
2. подготовьте план аудита ИБ (таблица);
3. определите состав группы по аудиту ИБ (количественный и ролевой состав).
4. определите какие способы сбора информации целесообразно было бы использовать (список)?
5. какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
1. Список внешних доменов и поддоменов предприятия с указанием их назначения. Входят ли вопросы CEO в компетенцию ИТ-подразделения. Описание системы мониторинга, которое должно включать в себя должность ответственного сотрудника, перечень параметров для мониторинга, триггерные значения параметров, адреса и методы оповещения. Список глобальных</td></tr>
</table>

<table>
<tr><td></td><td>администраторов (например, администраторов AD). Список ресурсов для резервного копирования. Наличие штатной структуры предприятия с перечислением структурных единиц и указанием подчиненности. Должностные инструкции, подписанные каждым работающим сотрудником.
2.
<table>
<tr><th>№</th><th>Наименование этапа</th><th>Дата начала</th><th>Длительность, рабочие дни</th><th>Примечание</th></tr>
<tr><td>1</td><td>Предварительное совещание</td><td>02.02.23</td><td>0.125</td><td>1 час</td></tr>
<tr><td>2</td><td>Получение документации</td><td>03.02.20</td><td>1</td><td></td></tr>
<tr><td>3</td><td>Анализ полученной документации</td><td>03.02.20</td><td>0.125</td><td></td></tr>
<tr><td>4</td><td>Проведение интервью</td><td>04.02.20</td><td>1</td><td></td></tr>
<tr><td>5</td><td>Использование инструментальных средств</td><td>05.02.20</td><td>1</td><td></td></tr>
<tr><td>6</td><td>Подготовка отчёта</td><td>06.02.20</td><td>3</td><td></td></tr>
<tr><td>7</td><td>Заключительное совещание</td><td>09.02.20</td><td>0.125</td><td>1 час</td></tr>
</table>
3.Руководитель группы по аудиту ИБ, руководитель ИТ отдела, технический аудитор пентеста.
4.Способы сбора информации (методы аудита ИБ): проведение интервью с ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа.
5. Документ, определяющий антивирусную политику на предприятии. Документ, определяющий порядок удаленного доступа в сеть. Документ, определяющий порядок физического доступа в серверную.</td></tr>
<tr><td>79</td><td>К вам за аудитом ИБ обратился директор ТК, все технологические процессы которого автоматизированы.

Составьте:
- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать (список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

Ответ:
- Список доп. вопросов: какие каналы взаимодействия можно использовать, в т.ч. вопросы конфиденциальности; наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и т.п.)?</td></tr>
</table>

- План аудита ИБ: см. слайд № 25 из 2-ого занятия

№	Наименование этапа	Дата начала	Длительность, раб. дни	Примечание
1	Предварительное совещание	09.03.23	0,125	1 час
2	Получение документации	10.03.23	2	
3	Анализ полученной документации	12.03.23	2	
4	Проведение интервью	16.03.23	5	График интервью предоставляется отдельно, каждое интервью не более 45 мин.
5	Использование инструментальных средств	16.03.23	5	График использования инструментальных средств предоставляется отдельно
6	Подготовка отчета	22.03.23	5	
7	Заключительное совещание	29.03.23	0,125	1 час

- Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных данных; аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018; тех. эксперт по OWASP Top 10
- Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами (если есть); проведение анализа документов (если есть); получение данных от инструментальных средств
- Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.

80

К вам за аудитом ИБ обратилась компания, специализирующаяся на реализации комплексных ИТ- проектов и автомаизации бизнес-процессов на основе программных продуктов SAP и 1С:
- загружают файлы
- обмениваются контактными данными
- проводят платежи
- разрабатывают ПО
- работают с SAP
- работают с 1С

Составьте:
- список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ (если считаете нужным);
- подготовьте план аудита ИБ (таблица);
- определите состав группы по аудиту ИБ (количественный и ролевой состав).
- определите какие способы сбора информации целесообразно было бы использовать (список)?
- какие свидетельства Вы могли бы получить (список)? Документы; результаты работы инструментальных средств

1. Список вопросов: какая информация обрабатывается на предприятии и структурирована ли она; как обрабатывается информация, составляющая коммерческую тайну, и конфиденциальная информация; построена ли в компании схема обработки информации, определены ли основные и дополнительные ее потоки; какие информационные ресурсы для хранения информации использует предприятие; какие информационные каналы для перемещения информации использует предприятие; какое программное обеспечение использует предприятие для обработки информации; каковы средства физической защиты информации; наличие интервьюируемых лиц в период проведения аудита ИБ и их роли; наличие сопровождающих лиц; какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и т.п.)?

2. План аудита

	№	Наименование этапа	Дата начала	Длительность, раб. дни	Примечание
	1	Предварительное совещание	04.03.22	0,125	1 час
	2	Анализ полученной документации	05.03.22	2	
	3	Получение документации	07.03.22	2	
	4	Проведение интервью	11.03.22	5	График интервью предоставляется отдельно. Каждое интервью не более 45 минут.
	5	Использование инструментальных средств	11.03.22	5	График использования инструментальных средств предоставляется отдельно.
	6	Подготовка отчета	18.03.22	5	
	7	Заключительное совещание	25.03.22	0,125	1 час

3. Состав группы по аудиту ИБ: руководитель группы по аудиту ИБ; аудитор по линии персональных данных; аудитор по линии ISO/IEC 27001; аудитор по линии ISO/IEC 27014; аудитор по линии ISO/IEC 15408; аудитор по линии PCI DSS; аудитор по линии ГОСТ Р 51898-2002.

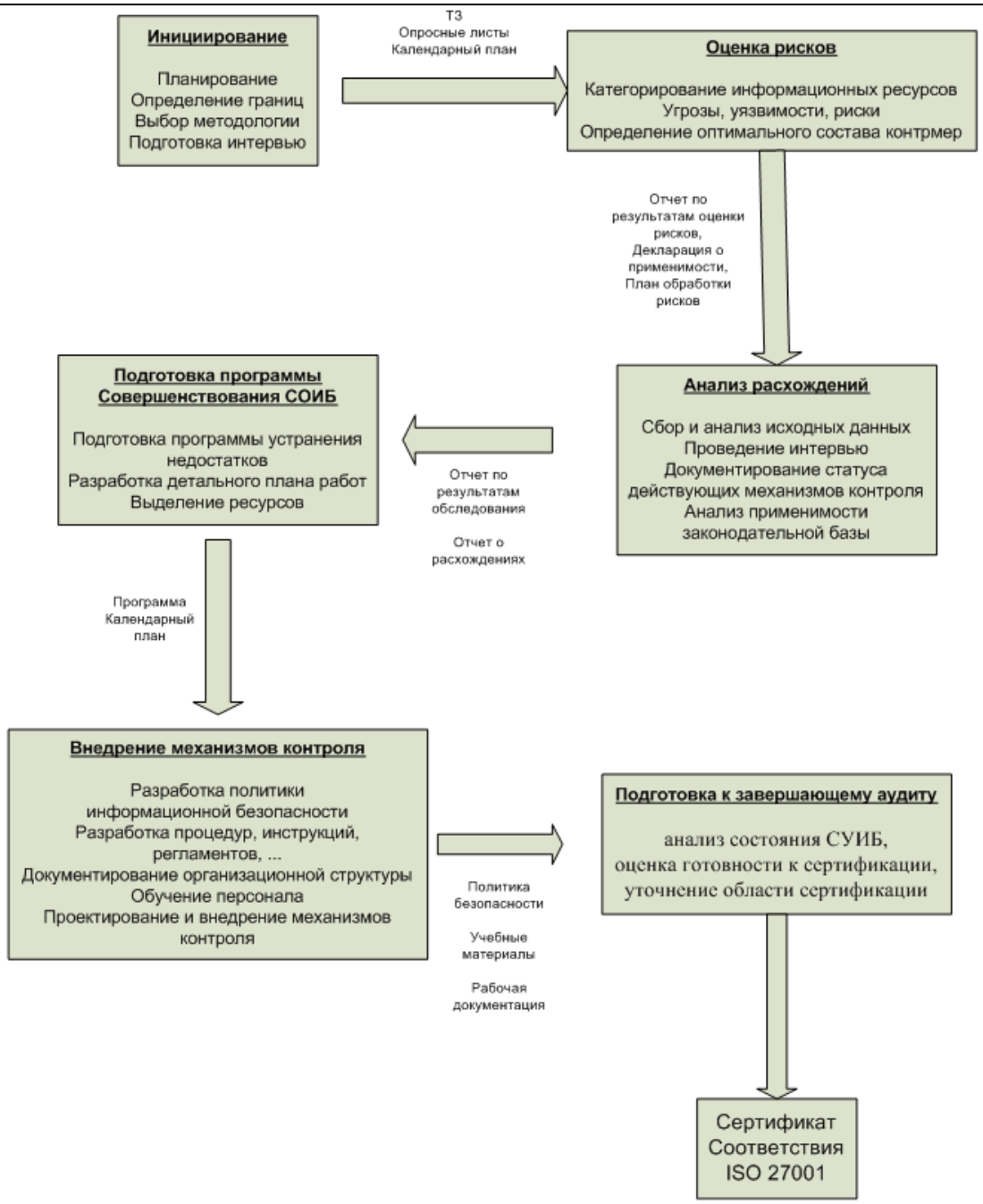
4. Способы сбора информации (методы аудита ИБ): проведение интервью с разработчиками на 1С и SAP ERP, ИТ- и ИБ-специалистами; заполнение опросных листов аутсорсерами; проведение анализа документов; получение данных от инструментальных средств.

5. Свидетельства аудита ИБ: записи аудиторов; заполненные опросные листы; представленные документы; результаты работы инструментальных средств.

3.4 Вопросы к собеседованию на зачете

81	Процессный подход к построению СУИБ и циклическая модель PDCA.
	Ответ: Процессный подход к управлению информационной безопасностью, представленный в международном стандарте, акцентирует внимание пользователей на важности: - понимания требований компании к информационной безопасности и необходимости определения политики и целей информационной безопасности; - обеспечения и функционирования требований к управлению рисками информационной безопасности как части процесса управления всеми рисками компании; - мониторинга и проверки выполнения и эффективности СУИБ; - постоянного улучшения, основанного на пересмотре бизнес- целей.
82	Цели и задачи, решаемые СУИБ.
	Ответ

	К главным целям функционирования современных СУИБ относятся: - обеспечение конфиденциальности данных за счет внедрения процедур ограничения доступа к закрытой информации для широкого круга лиц; - невозможность получения несанкционированного доступа к данным; - обеспечение целостности информации и процессов, с ней связанных (создание информации, её ввод, передача, ознакомление, обработка, вывод и т. п.); - обеспечение доступности информации (гарантия получения своевременного и неограниченного доступа к информации для ограниченного круга лиц, например, авторизованных пользователей); - сведение к минимуму рисков кибербезопасности; - учет всех процессов, которые связаны с рисками.
83	Стандартизация в области построения СУИБ: сходства и различия стандартов.
	- Стандарты для обзора и введения в терминологию; - Стандарты, определяющие обязательные требования к СУИБ (система управления информационной безопасностью); - Стандарты, определяющие требования и рекомендации для аудита СУИБ; - Стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ.
84	Стратегии выбора области деятельности СУИБ.
	Ответ 1.Распределение обязанностей между специалистами, которые отвечают за информационную безопасность. 2. Анализ рисков и бизнес-процессов. 3. Экспертная оценка состояния информационной безопасности. 4. Разработка политики информационной безопасности. 5. Контроль соблюдения регламента по уровням доступа к информации среди сотрудников. 6. Свод правил и методик, регламентирующих управление рисками, в том числе введение и соблюдение отчетности.
85	Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
	Ответ: Эффективная система управления ИБ включает в себя целый комплекс мер, направленных на сокращение потенциальных угроз и минимизацию ущерба. Для того, чтобы построить СУИБ необходимо описать жизненный цикл предприятия, бизнес-процессы и выявить возможные риски.



С учетом анализа и оценки рисков возможно определить уровень риска, приемлемый для конкретной организации, а также рассчитать технологические и финансовые возможности компании для обработки рисков и дальнейшей подготовки программы совершенствования СУИБ.

Процесс построения СУИБ можно представить в виде схемы.

86	Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
	Можно выделить следующие основные этапы разработки системы управления ИБ: - Инвентаризация активов. - Категорирование активов. - Оценка защищенности информационной системы. - Оценка информационных рисков. - Обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов). - Внедрение выбранных мер обработки рисков. - Контроль выполнения и эффективности выбранных мер.

	- Роль руководства компании в системе управления ИБ
87	Политика ИБ и политика СУИБ: сходства и различия.
	Ответ Политика информационной безопасности - самый важный документ в системе управления информационной безопасностью (СУИБ) организации, выступающий в качестве одного из ключевых механизмов безопасности. Согласно ISO 17799 документированная политика информационной безопасности должна заявлять о приверженности руководства и устанавливать подход к управлению информационной безопасностью, определять понятие информационной безопасности, ее основные цели и область действия, содержать основные положения для определения целей и механизмов контроля, включая структуру оценки и управления рисками и многое другое. Согласно ISO 27001 политика информационной безопасности является подмножеством более общего документа - политики СУИБ, включающей в себя основные положения для определения целей СУИБ и устанавливающей общее направление и принципы деятельности по отношению к информационной безопасности, учитывающей требования бизнеса, законодательной или нормативной базы, контрактные обязательства, устанавливаливающей критерии для оценивания рисков и т.д. Политика информационной безопасности и политика СУИБ организации могут быть описаны в одном документе. Разработка такого документа - задача непростая и очень ответственная. С одной стороны политика информационной безопасности должна быть достаточно емкой и понятной для всех сотрудников организации. С другой стороны, на основе этого документа строится вся система мер по обеспечению информационной безопасности, поэтому он должен быть досточно полным и всеохватывающим. Любые упущения и неоднозначности могут серьезным образом отразиться на функционировании СУИБ организации. Политика информационной безопасности должна полностью соответствовать требованиям международных стандартов ISO 27001/17799. Это необходимое условие для успешного прохождения сертификации.
88	Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
89	Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
90	Анализ рисков ИБ: основные подходы, основные этапы процесса.
91	Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
92	Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
	Ответ:

Стандарт ISO/IEC 27035-1:2016 вводит понятие *расследования информационной безопасности*, другой стандарт этой серии ISO/IEC 27043 Information technology − Security techniques − Incident investigation principles and processes использует понятие *процессы цифрового расследования* (digital investigation processes). При этом здесь смысл слова investigation ближе к понятию *исследование*, то есть стандарт описывает, в сущности процедуры сбора доказательств и процессы, характерные для проведения криминалистического исследования компьютерных систем и компьютерной экспертизы для понимания произошедшего.

Согласно ISO/IEC 27035-1:2016, **расследование информационной безопасности** (information security investigation) − применение экспертиз, анализов и интерпретации, для того, чтобы помочь понять инцидент ИБ.

Согласно ISO/IEC 27035-1:2016, расследование информационной безопасности (information security investigation) − применение экспертиз, анализов и интерпретации, для того, чтобы помочь понять инцидент ИБ.

Типовой сценарий при нарушениях ИБ может быть основан на приведенных ниже базовых действиях.

1. Идентифицировать инцидент и убедиться, что он действительно имеет место быть.
2. Локализовать область ИТ-инфраструктуры, задействованной в инциденте.
3. Ограничить доступ к объектам, задействованным в инциденте.
4. Оформить служебную записку на имя Генерального директора организации о факте возникновения инцидента.
5. Привлечь компетентных специалистов для консультации.
6. Создать группу по расследованию инцидента и составить план работ по сбору доказательств и восстановлению систем. Протоколировать все действия, которые осуществляются в ходе реагирования на инцидент.
7. Обеспечить сохранность и должное оформление доказательств.
7.1. Снять энергозависимую информацию с работающей системы.
7.2. Собрать информацию о протекающем в реальном времени инциденте (лог-файлы сетевого оборудования и сетевого трафика).
7.3. Отключить от сети питание.
8. В присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образов и другой информации для последующего анализа и сохранения.
8.1. Оформить протоколом все операции с носителями информации.
8.2. Провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения.
8.3. Задокументировать процесс на фото- и видеокамеру.
8.4. Сохранить опечатанные объекты вместе с протоколом в надежном месте до передачи носителей на исследование или в правоохранительные органы.
9. После сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем.
10. При проведении исследования источников информации обеспечить неизменность доказательств. Работать только с копией.
11. При проведении расследования обеспечить корректное взаимодействие с заинтересованными подразделениями правоохранительных органов (Управление «К», Центр информационной безопасности ФСБ РФ) и другими внешними организациями (компаниями, предоставляющими услуги в области расследования инцидентов и обеспечения ИБ).
12. По завершении расследования оформить соответствующий отчет и составить рекомендации по снижению рисков возникновения подобных инцидентов в будущем.
13. При обращении в правоохранительные органы представить им подробное описание инцидента, описание собранных доказательств и результаты их анализа.

93	Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
	Ответ: Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ. Внутренний аудит регламентируется внутренними документами и уставами компании. Они определяют порядок работы с данными и процессами. Внутренний аудит проводится собственными структурными подразделениями и выполняется на регулярной основе.  **Виды аудита ИБ** Можно выделить внутренний и внешний аудит информационной безопасности. • Внутренний аудит регламентируется внутренними документами и уставами компании. Они определяют порядок работы с данными и процессами. Внутренний аудит проводится собственными структурными подразделениями и выполняется на регулярной основе. • Внешний аудит проводится независимыми экспертами, которым по условиям договоров предоставляется доступ к внутренней сети компании. Он может проводиться по требованию руководства, акционеров и правоохранительных органов. Как правило, привлечение внешних аудиторов ведет к более объективной оценке существующей СУИБ, поскольку такие компании имеют штат квалифицированных аудиторов. Также у них есть соответствующие лицензии и сертификаты, подтверждающие их способность качественно Внутренний аудит направлен на выявление внутренних проблем, несоответствий и уязвимостей в системе безопасности. Он помогает обнаружить недостатки СУИБ, повлекшие за собой потерю данных, финансов, репутации и другой ущерб. Внутренний аудит бывает повседневным или проводимым по заранее согласованному плану специально определенным подразделением. За повседневный аудит отвечают сотрудники, связанные с процессом определения негативного воздействия на инфраструктуру организации. Среди них: инженеры, отвечающие за эксплуатацию инфраструктуры, сотрудники подразделений информационной безопасности, службы мониторинга, защиты активов и другие. Они отслеживают изменения в основных показателях, присущих информации (целостность, доступность, конфиденциальность), в своей зоне ответственности и оперативно вносят коррективы д **Для проведения внутреннего аудита ИБ требуется:** • предварительно определить список проверяемых процессов и сервисов,

	потенциально уязвимые места (стандарт, на основе которого проводится аудит, область действия, реализация системы защиты информации, привлекаемые ресурсы, формат и сроки проведения, ожидаемый результат и т. д.); • выбрать способ аудита (документальный, технический, в формате учений, комбинированный и т. д.). ля разрешения последствий.
94	Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
95	Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
96	Внедрение процессов управления ИБ: этапы и последовательность.
97	Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых экзаменах и зачетах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости.

Для оценки знаний, умений, навыков обучающихся по дисциплине применяется рейтинговая система. Итоговая оценка по дисциплине определяется на основании определения среднеарифметического значения баллов по каждому заданию.

Зачет по дисциплине выставляется в зачетную ведомость по результатам работы в семестре после выполнения всех видов учебной работы, предусмотренных рабочей программой дисциплины (с отметкой «зачтено») и получении по результатам тестирования по всем разделам дисциплины не менее 60 %.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине/практике

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
***Шифр и наименование компетенции* ПКв-7 –** Способен разрабатывать архитектуру системы защиты информации автоматизированной системы, проводить технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы, формировать разделы технических заданий на создание систем защиты информации автоматизированных систем					
ЗНАТЬ: организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; методики формирования научно-технической документации при создании систем защиты информации	Банк тестовых заданий (промежуточное тестирование, зачет)	Уровень знаний	60% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 60% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности; выявлять уязвимости информационно-	Реферат	Умение применять полученные знания	выставляется студенту при наличии доклада, преобразовании информации в единую	Зачтено	Освоена (повышенный)
			форму, т.е. презентации по выбранной теме	Не зачено	Не освоена (недостаточный)

технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.					
ВЛАДЕТЬ: методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыками проведения лицензирования и сертификации средств защиты информации.	Кейс-задание Собеседование (опрос на практическиxx занятиях)	Методика и правильность решения задачи	обучающийся выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе	Хорошо	Освоена (продвинутый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил не более 5 ошибок в ответе	Удовлетворительно	Освоена (базовый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе	Не удовлетворительно	Не освоена (недостаточный)

		Методик проведения аудита ИБ и ИТ в организациях	Обучающийся качественно выполнил практической работы. Оформил отчет в соответствии с методическими указаниями. Ответил на контрольные вопросы.	Зачтено	Освоена (повышенный, базовый)
			Обучающийся не выполнил задание лабораторной работы. Не оформил отчет в соответствии с методическими указаниями. Не ответил на контрольные вопросы.	Не зачтено	Не освоена (недостаточный)