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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Зарубежные стандарты по информационной безопасности

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1. Цели и задачи дисциплины

Целями и задачами освоения дисциплины «Зарубежные стандарты в области информационной безопасности» являются:

– сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;

– сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;

– организационно-методическое обеспечение информационной безопасности автоматизированных систем.

Поставленная цель достигается решением следующих задач: изучением зарубежных стандартов в области ИБ;

– изучением методов и процедур анализа угроз ИБ и оценки степени их опасности, применяемых в международных стандартах;

– освоением способов и порядка анализа исков ИБ и методов управления системой защиты информации от несанкционированного доступа в соответствии с методами и процедурами применяемыми в зарубежных стандартах.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

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

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Основные понятия и методы проведения экспериментально-исследовательских работ при аттестации автоматизированных систем, содержащиеся в зарубежных стандартах.	Пользоваться расчетными соотношениями и используемым и в зарубежных стандартах при определении показателей защищенности от утечки информации по техническим каналам.	Навыками применения технических средств проведения контроля защищенности и обеспечения защиты информации от утечки по техническим каналам, используемых в зарубежных стандартах.
	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Основные стандарты в области проектирования информационных систем	Применять основные положения стандартов в области проектирования информационных систем	Навыками применения стандартов в области проектирования информационных систем
	ОК-3	способностью анализировать основные этапы	Основные понятия и закономер-	Использовать основные закономер-	Навыками применения закономерности

		и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития	ности исторического развития России	ности развития России при Формировании политики информационной безопасности	развития России при формировании политики информационной безопасности

3. Место дисциплины в структуре ОП ВО (СПО)

Дисциплина «Зарубежные стандарты по информационной безопасности» относится к блоку 1 ОП и ее вариативной части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплины «История».

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Управление информационной безопасностью;
- Организационное и правовое обеспечение информационной безопасности;
- Основы управленческой деятельности;
- Учебная практика, практика по получению первичных профессиональных умений;
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;
- Производственная практика, преддипломная практика;

защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 2 зачетных единицы.

Виды учебной работы	**Всего часов часов**	Семестр
		3
	акад. ч	акад. ч
Общая трудоемкость дисциплины	**72**	**72**
Контактная работа, *в т.ч. аудиторные занятия:*	**61,6**	**61,6**
Лекции	30	30
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	30	30
в том числе в форме практической подготовки	30	30
Консультации текущие	1,5	1,5
Виды аттестации – зачет	0,1	0,1
Самостоятельная работа:	**10,4**	**10,4**
Подготовка доклада	10,4	10,4

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

5.1 Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, час
1	Международные стандарты в области обоснования требований к информационной безопасности информационных	Система документов в области компьютерной безопасности, разработанная Министерством обороны США: Критерии оценки безопасности компьютерных систем (оранжевая книга); Руководство по применению критерия оценки безопасности компьютерных систем в специфических средах (желтая книга); Разъяснение критерия оценки безопасности	45

	систем	компьютерных систем для безопасных сетей (красная книга); Разъяснение критерия оценки безопасности компьютерных систем для СУБД. Критерии безопасности информационных технологий разработки стран Евросоюза (Европейские критерии). Международный стандарт «Общие критерии оценки безопасности информационных технологий» ISO/IEC 15408 «Информационная технология — Методы и средства защиты информации — Критерии оценки безопасности информационных технологий» (Общие критерии). Международный стандарт ISO/IEC 13335 и концепция остаточного риска. Организации, регулирующие вопросы обеспечения информационной безопасности ведущих зарубежных стран.	
2	Международные стандарты в области управления системами защиты информации от несанкционированного доступа	Международный стандарт ИСО/МЭК 21827 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса». Международный стандарт ИСО/МЭК 17799«Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности». Обзор серии международных стандартов в области системы менеджмента информационной безопасности ИСО/МЭК 27000.	15

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СРС, час
1	Международные стандарты в области обоснования требований к информационной безопасности информационных систем.	20	20	6
2	Международные стандарты в области управления системами защиты информации от несанкционированного доступа	10	10	6

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Международные стандарты в области обоснования требований к информационной безопасности информационных систем	Система документов в области компьютерной безопасности, разработанная Министерством обороны США: Критерии оценки безопасности компьютерных систем (оранжевая книга); Руководство по применению критерия оценки безопасности компьютерных систем в специфических средах (желтая книга); Разъяснение критерия оценки безопасности компьютерных систем для безопасных сетей (красная книга); Разъяснение критерия оценки безопасности компьютерных систем для СУБД.	2
		Критерии безопасности информационных технологий разработки стран Евросоюза (Европейские критерии).	2
		Международный стандарт «Общие критерии оценки безопасности информационных технологий» ISO/IEC 15408 «Информационная технология — Методы и средства защиты информации — Критерии оценки безопасности информационных технологий» (Общие критерии).	8
		Международный стандарт ISO/IEC 13335 и концепция остаточного риска.	4
		Организации, регулирующие вопросы обеспечения информационной безопасности ведущих зарубежных	4

		стран.	
2	Международные стандарты в области управления системами защиты информации от несанкционированного доступа	Методы проектирования информационных систем в защищенном исполнении с использованием международного стандарта ИСО/МЭК 21827 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса»	2
		Методы обеспечения эффективной эксплуатации систем защиты информации от несанкционированного доступа в соответствии с международным стандартом ИСО/МЭК 17799 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности».	2
		Система менеджмента информационной безопасности в соответствие с системой международных стандартов серии ИСО/МЭК 27000.	6

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость, час
1	Международные стандарты в области обоснования	Классификация информационных систем в соответствии с системой	4
	требований к информационной безопасности информационных систем	документов в области компьютерной безопасности, разработанной Министерством обороны США. Функциональные требования к информационной безопасности для различных классов.	
		Классификация информационных систем использующих технологии локальных вычислительных сетей в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США. Функциональные требования к информационной безопасности для различных классов.	4
		Классификация информационных систем в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза. Функциональные требования к информационной безопасности для различных классов.	4
		Международный стандарт «Общие критерии оценки безопасности информационных технологий» ISO/IEC 15408 ч.1 Общие положения.	4
		Международный стандарт «Общие критерии оценки безопасности информационных технологий» ISO/IEC 15408 ч.2, 3 Функциональные требования. Профиль защиты. Задание по безопасности. Классификация оценочных уровней доверия.	4
		Типовые профили защиты. Содержание и последовательность разработки.	4
2	Международные стандарты в области управления системами защиты информации от несанкционированного доступа	Модели зрелости процесса проектирования информационных систем. Методы и средства обеспечения информационной безопасности	4
		Система менеджмента информационной безопасности в соответствии с международными стандартами. Соответствие Российским нормативнометодическим документам в области информационной безопасности.	4

5.2.3 Лабораторный практикум не предусмотрен.

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Международные стандарты в области обоснования требований к информационной безопасности информационных систем	Доклад	12
2	Международные стандарты в области управления системами защиты информации от несанкционированного доступа		

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

6.2 Дополнительная литература

2. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

3. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Щербаков А.Ю. Издательство: Книжный мир, 2016 г. http://www.knigafund.ru/books/88712

4. Служба защиты информации: организация и управление: учебное пособие для вузов: Аверченков В.И., Рытов М.Ю. Издательство: Флинта, 2014 г. http://www.knigafund.ru/books/116368

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Методические указания для обучающихся по освоению дисциплины

Зарубежные стандарты в области 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, В. А. Хвостов; ВГУИТ, Кафедра информационной безопасности. Воронеж : ВГУИТ, 2016. – 10 с. <*http://biblos.vsuet.ru/ProtectedView/Book/View- Book/2548*>

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

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 ReaderБесплатное 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 PlayerБесплатное 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 № 2145 30.07.2013 г. Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г. Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г. СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015 СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013

7 Материально-техническое обеспечение дисциплины

Комплекты мебели для учебного процесса.

ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, 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-РЗ.1»; система защиты речевой информации «СонатаАВ-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 замо5к Samsung SHS-2920.

ОЦЕНОЧНЫЕ СРЕДСТВА
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине/практике

___ **Зарубежные стандарты по информационной безопасности** ___

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Перечень компетенций		Этапы формирования компетенций		
	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Основные понятия и методы проведения экспериментально-исследовательских работ при аттестации автоматизированных систем, содержащиеся в зарубежных стандартах.	Пользоваться расчетными соотношениями и используемыми в зарубежных стандартах при определении показателей защищенности от утечки информации по техническим каналам.	Навыками применения технических средств проведения контроля защищенности и обеспечения защиты информации от утечки по техническим каналам, используемых в зарубежных стандартах.
2	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Основные стандарты в области проектирования информационных систем	Применять основные положения стандартов в области проектирования информационных систем	Навыками применения стандартов в области проектирования информационных систем
3	ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития	Основные понятия и закономерности исторического развития России	Использовать основные закономерности развития России при формировании политики информационной безопасности	Навыками применения закономерности развития России при формировании политики информационной безопасности

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства		Технология оценки (способ контроля)
1 2	Международные стандарты в области обоснования требований к информационной безопасности информационных систем Международные стандарты в области управления системами защиты информации от несанкционированного доступа	ПК-16 ПК-12 ОК-3	Зачет	№ 1-69	Отметка «зачтено- не зачтено»
			Контрольные вопросы к текущим опросам на практических работах	№ 1-36	Уровневая шкала
			Задания к практическим работам	№ 1-40	Уровневая шкала
			Доклад	№ 1	Уровневая шкала
			Доклад	№2	Уровневая шкала

3 Оценочные средства для промежуточной аттестации.

Вопросы к зачету

3.1.1 Шифр и наименование компетенции ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития

1	Какие виды зарубежных стандартов в области информационной безопасности существуют
2	По каким критериям оценивается степень доверия в стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
3	Что понимается под термином Политика безопасности в стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
4	Что понимается под термином Уровень гарантированности в стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
5	Что такое Доверенная вычислительная база в терминах стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем»
6	Что такое доверенный монитор обращений, в терминах стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем»
7	Какими качествами должен обладать монитора обращений в соответствии с требованиями стандарта Министерства обороны США "Критерии оценки доверенных компьютерных систем "
8	Какие элементы составляют понятие политика безопасности в соответствии с требованиями стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем»
9	Что понимается под термином метки безопасности в стандарте Министерства обороны США "Критерии оценки доверенных компьютерных систем " (Оранжевая книга)
10	Какие категории составляют понятие подотчетности в стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
11	Что понимается под термином Операционная гарантированность в стандарте Министерства обороны США "Критерии оценки доверенных компьютерных систем" (Оранжевая книга)
12	Какие элементы составляют понятие Операционная гарантированность в стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
13	Какие уровни доверия содержатся содержаться в стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
14	Какие основные требования к информационной безопасности содержатся в классе безопасности С1 стандарта Министерства обороны США «Критерии

	оценки доверенных компьютерных систем» (Оранжевая книга)
15	Какие основные требования к информационной безопасности содержатся в классе безопасности С2 стандарта Министерства обороны США "Критерии оценки доверенных компьютерных систем " (Оранжевая книга)
16	Какие основные требования к информационной безопасности содержатся в классе безопасности В1 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
17	Какие основные требования к информационной безопасности содержатся в классе безопасности В2 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
18	Какие основные требования к информационной безопасности содержатся в классе безопасности В3 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
19	Какие основные требования к информационной безопасности содержатся в классе безопасности А1 стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
20	В существенное отличие Гармонизированных критериев Европейских стран от стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем»
21	Что понимается под термином сетевая доверенная вычислительная база в стандарт Министерства обороны США «Разъяснение критерия оценки безопасности компьютерных систем для безопасных сетей» (красная книга)
22	Какие меры по обеспечению непрерывности функционирования могут применяться в стандарт Министерства обороны США «Разъяснение критерия оценки безопасности компьютерных систем для безопасных сетей» (красная книга)
23	Какие составляющие информационной безопасности рассматриваются в Гармонизированных критериях Европейских стран
24	Что понимается под термином система в Гармонизированных критериях Европейских стран
25	Что понимается под термином продукт в Гармонизированных критериях Европейских стран
26	Что понимается под термином функция (сервис) безопасности в Гармонизированных критериях Европейских стран
27	Какие аспекты безопасности составляют существо понятия гарантированность в Гармонизированных критериях Европейских стран
28	Какие классы гарантированности содержатся в Гармонизированных критериях Европейских стран
29	В каких терминах оценивается понятие мощность механизма защиты в Гармонизированных критериях Европейских стран
30	Какое основное отличие стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» от остальных существующих зарубежных стандартов в области информационной безопасности
31	Какие основные виды требований к информационной безопасности содержит ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"
32	Какие этапы жизненного цикла безопасности информации рассматривает стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
33	Что понимается под термином среда безопасности в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»

34	Какими параметрами характеризуются угрозы информационной безопасности в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
35	Какими параметрами характеризуются уязвимости информационной системы в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
36	Что определяет понятие «Класс» в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
37	Что определяет понятие «Семейства» в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
38	Что определяет понятие «Компонент» в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
39	Что определяет понятие «Элемент» в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
40	Какие виды нормативных документов могут формироваться с использованием библиотек функциональных требований в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
41	Что представляет собой профиль защиты в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
42	Что представляет собой задание по безопасности в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
43	Что представляет собой функциональный пакет в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
44	Что такое базовый профиль защиты в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
45	Что такое производный профиль защиты в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
46	Что включает в себя класс функциональных требований идентификация и аутентификация в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
47	Что включает в себя класс функциональных требований защита данных пользователя в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
48	Что включает в себя класс функциональных требований защита данных пользователя в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
51	Что включает в себя класс функциональных требований защита функций безопасности в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
52	Что включает в себя класс функциональных требований управление безопасностью в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
53	Что включает в себя класс функциональных требований аудит безопасности в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
54	Что включает в себя класс функциональных требований доступ к объекту оценки в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
55	Что включает в себя класс функциональных требований приватность в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»

56	Что включает в себя класс функциональных требований использование ресурсов в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
57	Что включает в себя класс функциональных требований криптографическая поддержка в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
58	Что включает в себя класс функциональных требований связь в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
59	Что включает в себя класс функциональных требований доверенный маршрут/канал в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
60	Назовите оценочные уровни доверия, содержащиеся в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
61	Что понимается под термином «Риск» в стандарте ISO/IEC 13335 «Информационная технология. Методы и средства обеспечения информационной безопасности. Часть 1.»
62	Отобразите взаимосвязь компонентов безопасности в стандарте ISO/IEC 13335 «Информационная технология. Методы и средства обеспечения информационной безопасности. Часть 1.»
63	Назовите организации, регулирующие вопросы обеспечения информационной безопасности ведущих зарубежных стран.
64	Что понимается под термином «Архитектура модели в стандарте» ISO/IEC 21827 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса»
65	Что понимается под термином «Базовые практики обеспечения безопасности» ISO/IEC 21827 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса»
66	Кратко перечислите разделы и содержание стандарта ИСО/МЭК 17799 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности»
67	Кратко охарактеризуйте методы контроля доступа, используемые в стандарте ИСО/МЭК 17799 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности»
68	Какие действия реализуются при организации защиты информации в соответствии со стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
69	Какие требования к документации, описывающей политику безопасности информационной системы, содержатся в стандарте ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

3.2 Контрольные вопросы к текущим опросам на практических работах

3.2.1 Шифр и наименование компетенции ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития

1.	Какие классы защищенности информационных систем введены в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
2.	Назовите функциональные требования к информационной безопасности для класса С1 в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
3.	Назовите функциональные требования к информационной безопасности для класса С2 в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
4.	Назовите функциональные требования к информационной безопасности для класса В1 в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
5.	Назовите функциональные требования к информационной безопасности для класса В2 в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
6.	Назовите функциональные требования к информационной безопасности для класса В3 в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
7.	Назовите функциональные требования к информационной безопасности для класса А1 в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США.
8.	Какие классы защищенности информационных систем использующих технологии локальных вычислительных сетей введены в соответствии с системой документов в области компьютерной безопасности, разработанной Министерством обороны США
9.	Назовите классы защищенности, содержащиеся в Гармонизированных критериях Европейских стран
10.	Назовите функциональные требования к информационной безопасности для класса Е0Гармонизированных критериев Европейских стран
11.	Назовите функциональные требования к информационной безопасности для класса Е1Гармонизированных критериев Европейских стран

12.	Назовите функциональные требования к информационной безопасности для класса Е2Гармонизированных критериев Европейских стран
13.	Назовите функциональные требования к информационной безопасности для класса Е3 Гармонизированных критериев Европейских стран
14.	Назовите функциональные требования к информационной безопасности для класса Е4Гармонизированных критериев Европейских стран
15.	Назовите функциональные требования к информационной безопасности для класса Е5 Гармонизированных критериев Европейских стран
16.	Назовите функциональные требования к информационной безопасности для класса Е6Гармонизированных критериев Европейских стран
17.	Назовите функциональные требования к безопасности информации, содержащиеся в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
18.	Назовите оценочные уровни доверия, содержащиеся в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
19.	Какие документы регламентируют порядок разработки и регистрации профилей защиты в стандарте ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
20.	Перечислите типовые профили защиты, разработанные и зарегистрированные в зарубежных странах, в настоящее время.
21.	Что подразумевает начальный уровень зрелости процесса проектирования информационных систем.
22.	Что подразумевает повторяемый уровень зрелости процесса проектирования информационных систем.
23.	Что подразумевает определенный уровень зрелости процесса проектирования информационных систем.
24.	Что подразумевает управляемый уровень зрелости процесса проектирования информационных систем.

25.	Что подразумевает оптимизирующий уровень зрелости процесса проектирования информационных систем.
26.	Назовите группы факторов, которые необходимо учитывать при формировании требований в области информационной безопасности в соответствии с требованиями стандарта ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
27.	Перечислите последовательность этапов классификации и управления активами в соответствии с требованиями стандарта ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
28.	Назовите меры физической защиты, рекомендуемые стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
29.	Назовите обязанности и процедуры, связанные с функционированием всех средств обработки информации, рекомендуемые стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
30.	Назовите меры контроля доступа, рекомендуемые стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
31.	Назовите меры криптографической защиты, рекомендуемые стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
32.	Назовите меры обеспечения целостности, рекомендуемые стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
33.	Назовите меры управления непрерывностью бизнеса, рекомендуемые стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
34.	Изложите основные положения процессного подхода для разработки системы менеджмента информационной безопасности в соответствии со стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
35.	Какие этапы разработки системы менеджмента информационной безопасности реализуются в соответствии со стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
36	Какие меры управления информационной безопасностью рекомендуются в соответствии со стандартом ИСО/МЭК 27001 «Информационная

	технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

3.3 Задания к практическим работам

3.3.1 Шифр и наименование компетенции ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития

№ задания	Условие задачи (формулировка задания)
1	Функциональные требования к информационной безопасности информационной системы класса С1стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
2	Функциональные требования к информационной безопасности информационной системы класса С2стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
3	Функциональные требования к информационной безопасности информационной системы класса В1 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
4	Функциональные требования к информационной безопасности информационной системы класса В2 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
5	Функциональные требования к информационной безопасности информационной системы класса В3 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
6	Функциональные требования к информационной безопасности информационной системы класса А1 стандарта Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга)
7	Функциональные требования к информационной безопасности информационной системы класса Е0 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.
8	Функциональные требования к информационной безопасности информационной системы класса Е1 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.
9	Функциональные требования к информационной безопасности информационной системы класса Е2 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.
10	Функциональные требования к информационной безопасности информационной системы класса Е3 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.
11	Функциональные требования к информационной безопасности информационной системы класса Е4 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.
12	Функциональные требования к информационной безопасности информационной системы класса Е5 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.
13	Функциональные требования к информационной безопасности информационной системы класса Е6 в соответствии с системой документов в области компьютерной безопасности, разработанной в странах Евросоюза.

14	Содержание, функциональные требования и требования доверия профиля, разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
15	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
16	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
17	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
18	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
19	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
20	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
21	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
22	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
23	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
24	Содержание, функциональные требования и требования доверия профиля « », разработанного в соответствии с требованиями стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
25	Цель процесса анализа рисков ИБ.
26	Этапы и участники процесса анализа рисков ИБ.
27	Разработка Методики анализа рисков ИБ.
28	Понятие актива. Типы активов.
29	Основные процессы управления информационной безопасностью.
30	Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами)
31	Процессы улучшения управления информационной безопасностью («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»)
32	Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса».
33	Процесс «Анализ со стороны высшего руководства».
34	Процесс «Обучение и обеспечение осведомленности».
35	Ввод системы в эксплуатацию. Возможные проблемы и способы их решения.
36	Внешние аудиты ИБ на соответствие требованиям нормативных документов.
37	Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.

38	Сертификация системы менеджмента информационной безопасностью по требованиям международного стандарта ISO/IEC 27001
39	Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
40	Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

3.4 Темы докладов и презентаций

3.4.1 Шифр и наименование компетенции ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития

№ задания	Тема доклада
1	Система зарубежных документов в области информационной безопасности

3.4.2 Шифр и наименование компетенции ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации

2	Система зарубежных документов в области управления информационной безопасностью

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 – 2015 Положение о курсовых экзаменах и зачетах;
- П ВГУИТ 4.1.02 – 2012 Положение о рейтинговой оценке текущей успеваемости, а также методическими указаниями …(*перечислить если имеются в наличии*).

В методических указаниях указывается порядок проведения оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, и выставления оценки по дисциплине (средневзвешенная – среднеарифметическое из всех оценок в течение периода изучения дисциплины; с использованием штрафных баллов за недочеты; интегральная – суммирование набранных баллов за каждое задание и пр.) **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 ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.					
ЗНАТЬ: Основные понятия и методы обеспечения информационной безопасности, применяемые в зарубежных стандартах.	Зачет	Уровень владения материалом	ответил не на все вопросы, допустил более 5 ошибок	Не зачтено	Не освоена (недостаточный)
			ответил на все вопросы, допустил не более 1 ошибки в ответе	Зачтено	Освоена (базовый, повышенный)
УМЕТЬ: Пользоваться расчетными соотношениями и используемыми в зарубежных стандартах в области информационной безопасности.	Контрольные вопросы к текущим опросам по практическим работам	Уровень умения	выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена
			выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
	Задания к практическим работам	Уровень умения	выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена

			выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
ВЛАДЕТЬ: Навыками применения математического аппарата для решения прикладных задач обеспечения информационной безопасности, используемых в зарубежных стандартах.	Доклад	Уровень владения	выставляется обучающемуся при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена
			выставляется обучающемуся при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
	Задания к практическим работам	Уровень умения	выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена
			выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена
			выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
ВЛАДЕТЬ: Навыками	Доклад	Уровень	выставляется обучающемуся при	Зачтено	Освоена

анализа и управления информационной безопасностью с использованием стандартного инструментария используемого в международных стандартах.		владения	наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме		
			выставляется обучающемуся при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена