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

Защита конфиденциальной информации

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 «Защита конфиденциальной информации» являются:

реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;

организационно-методическое обеспечение информационной безопасности автоматизированных систем;

выполнение проектов по созданию программ, комплексов программ, программно- аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем.

Поставленная цель достигается решением следующих задач:

изучением нормативно-методической документации в области ИБ конфиденциальной информации;

изучением методов и процедур построения модели угроз ИБ конфиденциальной информации и оценки степени их опасности;

ознакомлением с основами теории построения моделей и методов защиты конфиденциальной информации.

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-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Основные понятия и методы обеспечения ИБ конфиденциальной информации.	Пользоваться нормативно-методическими документами в области ИБ конфиденциально й информации, а также расчетными соотношениями используемыми в модели защиты конфиденциальной информации.	Навыками применения модели защиты при обосновании требований к ИБ информационных систем.
2	ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности	Основные нормативные правовые акты применяемые при обеспечении ИБ конфиденциальной информации	Пользоваться нормативно-методическими документами по технической защите информации	Навыками применения специальных требований и рекомендаций по защите информации от утечки по техническим каналам
3	ПСК-4.2	Способностью	Основные норма-	Пользоваться норматив-	Навыками при-

		разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	тивные правовые акты применяемые при формировании политик информационной безопасности	но-методическими документами регламентирующими процессы формирования политик информационной безопасности	менения приказов директора ФСТЭК России, содержащими требования к политикам информационной безопасности

3 Место дисциплины в структуре ОП ВО (СПО)

Дисциплина «Защита конфиденциальной информации» относится к блоку 1 ОП и ее базовой части. Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин:

- Безопасность сетей ЭВМ;
- Безопасность систем баз данных;
- Основы информационной безопасности;
- Организационное и правовое обеспечение информационной безопасности;
- Система обнаружения компьютерных атак;
- Технологии разработки защищенного документооборота;
- Управление информационной безопасностью;
- Разработка и эксплуатация защищенных автоматизированных систем;
- Учебная практика, практика по получению первичных профессиональных умений;
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности.

Дисциплина является предшествующей для защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4 Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 3 зачетных единицы.

Виды учебной работы	**Всего часов**	**Семестр**
		10
	акад.	**акад.**
Общая трудоемкость дисциплины	**108**	**108**
Контактная работа, *в т.ч. аудиторные занятия:*	**40**	**40**
Лекции	20	20
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	20	20
в том числе в форме практической подготовки	20	20
Консультации текущие	1	1
Вид аттестации – зачет	0,1	0,1
Самостоятельная работа:	**66,9**	**66,9**
Аналитические обзоры по темам №1	38	38
Аналитический обзор №2	30	30

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

5.1Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, час
1	Нормативно-правовая база защиты конфиденциальной информации.	Перечень и содержание основных документов регламентирующих вопросы обеспечения конфиденциальной информации: Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Руководящие документы ФСТЭК России.	32
2	Современные модели и методы построения модели защиты конфиденциальной информации.	Антагонистический конфликт субъектов в информационной сфере. Теоретические основы построения модели угроз ИБ с использованием математического аппарата логических деревьев. Марковская модель защиты конфиденциальной информации.	8

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СРС, час
1	Нормативно-правовая база защиты конфиденциальной информации.	16	16	28
2	Современные модели и методы построения модели защиты конфиденциальной информации.	4	4	40

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Нормативно-правовая база защиты конфиденциальной информации.	Перечень сведений конфиденциального характера. Перечень нормативных правовых актов, нормативно-методических документов, необходимых для осуществления деятельности по технической защите конфиденциальной информации.	4
		Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К).	2
		Классификация по уровню контроля отсутствия недекларированных возможностей.	4
		Разработка профилей защиты и заданий по безопасности в соответствии с ГОСТ 15408. Перечень и содержание зарегистрированных в Российской федерации профилей защиты.	2
		Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	2
2	Современные модели и методы построения модели защиты конфиденциальной информации.	Основы теории динамического конфликта. Антагонистический конфликт субъектов в информационной сфере.	2
		Теоретические основы построения модели угроз ИБ с использованием математического аппарата логических деревьев.	2
		Типовая последовательность реализации угрозы ИБ конфиденциальной информации. Марковская модель защиты конфиденциальной информации.	2

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Нормативно-правовая база защиты конфиденциальной информации.	Разработка перечня сведений конфиденциального характера, обрабатываемых в Университете.	2
		Изучение требований и рекомендаций по защите речевой информации, циркулирующей в защищаемых помещениях.	2
		Изучение требований и рекомендаций по защите информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов.	2
		Защита речевой информации, при ее передаче по каналам связи.	4
		Основные требования и рекомендации по защите служебной тайны и персональных данных. Основные рекомендации по защите информации составляющей коммерческую тайну.	2
		Порядок обеспечения защиты конфиденциальной информации при эксплуатации информационных систем.	4
2	Современные модели и методы построения модели защиты конфиденциальной информации.	Разработка модели реализации конкретных видов угроз ИБ конфиденциальной информации с использованием математического аппарата логических деревьев.	2
		Проведение анализа вероятностно-временных характеристик типовой последовательности реализации угроз ИБ конфиденциальной информации с использованием Марковской модели защиты.	2

5.2.3 Лабораторный практикум не предусмотрен.

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Нормативно-правовая база защиты конфиденциальной информации.	Аналитический обзор по теме №1 «Система документов по защите конфиденциальной информации в Российской Федерации».	38
2	Современные модели и методы построения модели защиты конфиденциальной информации.	Аналитический обзор по теме №2: «Угрозы безопасности конфиденциальной, организационные меры, технические и программные средства защиты информации от несанкционированного доступа»	30

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.

Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. - РнД: Феникс, 2017. - 347 с

6.2 Дополнительная литература

Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2018. - 352 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Щербаков А.Ю. Издательство: Книжный мир,

2009 г. http://www.knigafund.ru/books/88712

Служба защиты информации: организация и управление: учебное пособие для вузов: Аверченков В.И., Рытов М.Ю. Издательство: Флинта, 2011 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

Безопасность конфиденциальной информации [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. - 9 с. *http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/2549*

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; 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 Pas- calБесплатное 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 «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.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают:

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

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

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

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

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Безопасность конфиденциальной информации

(шифр дисциплины) (наименование дисциплины, практики в соответствии с учебным планом)

–

1 Требования к результатам освоения дисциплины

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Основные понятия и методы обеспечения ИБ конфиденциальной информации.	Пользоваться нормативно-методическими документами в области ИБ конфиденциальной информации, а также расчетными соотношениями используемыми в модели защиты конфиденциальной информации.	Навыками применения модели защиты при обосновании требований к ИБ информационных систем.
	ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности	Основные нормативные правовые акты применяемые при обеспечении ИБ конфиденциальной информации	Пользоваться нормативно-методическими документами по технической защите информации	Навыками применения специальных требований и рекомендаций по защите информации от утечки по техническим каналам
	ПСК-4.2	Способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	Основные нормативные правовые акты применяемые при формировании политик информационной безопасности	Пользоваться нормативно-методическими документами регламентирующими процессы формирования политик информационной безопасности	Навыками применения приказов директора ФСТЭК России, содержащими требования к политикам 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	Нормативно-правовая база защиты конфиденциальной информации.	ПК-22	Зачет с оценкой	Уровневая шкала
			Задания к практическим работам	Уровневая шкала

			Аналитический обзор	Уровневая шкала
2 4	Нормативно-правовая база защиты конфиденциальной информации. Современные модели и методы построения модели защиты конфиденциальной информации.	ОПК-6	Зачет с оценкой	Уровневая шкала
			Задания к практическим работам	Уровневая шкала
			Аналитический обзор	Уровневая шкала
3	Современные модели и методы построения модели защиты конфиденциальной информации.	ПСК-4,2	Зачет с оценкой	Уровневая шкала
			Задания к практическим работам	Уровневая шкала
			Аналитический обзор	Уровневая шкала

3 Оценочные средства для промежуточной аттестации

3.1 Вопросы к зачету

ПК-22 - Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

	Что понимается под термином защита информации?
2	В чем суть и содержание термина защита информации?
3	Что понимается под термином защищаемая информация?
4	Что понимается под термином угроза безопасности информации?
5	Что понимается под термином естественная угроза безопасности информации?
6	Что понимается под термином искусственная угроза безопасности информации?
7	Каковы отличия непреднамеренных и преднамеренных угроз безопасности конфиденциальной информации?
8	Какие виды преднамеренных угроз безопасности информации вы знаете?
9	Какими основными законами Российской федерации регламентирована защита конфиденциальной информации?
10	Какие основные виды конфиденциальной информации, обрабатываются в информационных системах?
11	Какие объекты из состава информационных систем в учреждении требуют реализации организационных и технических мероприятий по защите конфиденциальной информации?
12	Какая информация должна быть отнесена к категории конфиденциальная информация?
13	Какая информация о сотрудниках организации должна быть отнесена к категории конфиденциальная информация?
14	Какая технологическая информация информационной системы должна быть отнесена к категории конфиденциальная информация?
15	Какая информация требует выполнения мероприятий по защите информации в организации кроме конфиденциальной?

ОПК-6 Способность применять нормативные правовые акты в профессиональной деятельности.

16	Какие данные являются информационным основанием функционирования организации различной ведомственной принадлежности?

17	Какой состав общесистемного и специального программного обеспечения типовой информационной системы?
18	Какой состав аппаратного обеспечения персональных ЭВМ и локальной вычислительной сети?
19	Какими свойствами обладают информационные системы с точки зрения решения задачи обеспечения защиты конфиденциальной информации?
20	Основные способы защиты информации при обработке конфиденциальной информации.
21	Основные средства защиты информации при обработке конфиденциальной информации.
22	Состав и основные функции систем обеспечения безопасности информации уровня отдельных ЭВМ.
23	Какие основные принципы построения и эксплуатации систем защиты информации?
24	Назовите основные типы систем защиты информации, используемые для защиты конфиденциальной информации?
25	Какими защитными функциями обеспечения безопасности информации наиболее распространенных операционных систем можно воспользоваться при организации обработки конфиденциальной информации?
26	Какой главный недостаток защитных функций обеспечения безопасности информации наиболее распространенных операционных систем с точки зрения защиты конфиденциальной информации?
27	Назовите основные защитные функции, реализуемые операционной системой WINDOWS XP.
28	Назовите основные защитные функции, реализуемые операционной системой LINUX.
29	Какой состав системы защиты информации уровня отдельной ЭВМ?
30	Назовите назначение подсистемы управления доступом системы защиты информации уровня отдельного ЭВМ.
31	Назовите назначение подсистемы регистрации и учета системы защиты информации уровня отдельного ЭВМ.
32	Назовите назначение криптографической подсистемы системы защиты информации уровня отдельного ЭВМ.
33	Назовите назначение подсистемы контроля целостности системы защиты информации уровня отдельного ЭВМ.
34	Назовите назначение и основные функции межсетевого экрана.

ПСК-4,2 Способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем

35	Какие параметры могут использоваться в качестве критериев анализа межсетевых экранов.
36	Назовите цели построения систем обнаружения вторжений.
37	Назовите назначение средств построения виртуальных частных сетей.
38	Назовите цели построения средств централизованного управления информационной безопасностью.
39	Назовите цели построения средств анализа защищенности информационных систем.
40	Назовите наиболее распространенные системы защиты информации уровня отдельных ЭВМ и их функции
41	Назовите наиболее распространенные системы защиты информации уровня локальной вычислительной сети и их функции
42	Назовите наиболее распространенные системы защиты информации, применяемые при подключении к Интернет и их функции
43	Какие основные признаки классификации информационных систем при обработке конфиденциальной информации?
44	Какая последовательность действий при проведении классификации информационных систем?
45	Какие основные классы конфиденциальности информационных систем существуют?
46	Что такое акт классификации информационной системы?
47	Что такое программа и методика сертификационных испытаний?

48	Что такое модель угроз информационной безопасности?
51	Что такое сертификат ФСТЭК России на устанавливаемые системы защиты?
52	Назовите основное содержание проверки эффективности мероприятий по защите персональных данных?
53	На какие виды деятельности должна иметь лицензию организация, привлекаемая для проверки эффективности мероприятий по защите информации?
54	В чем заключается процесс аттестации?
55	В чем заключается процесс сертификации?
56	Какой срок действия Аттестата соответствия?
57	В чем заключается управление системой защиты информации?
58	В чем заключается управление подсистемой управления доступом?
59	В чем заключается управление подсистемой контроля целостности?
60	В чем заключается управление криптографической подсистемой?
61	В чем заключается управление подсистемой регистрации и учета?
62	В чем заключается управление межсетевым экраном?

3.2 Задания к практическим работам

ПК-22 - Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

№ задания	Условие задачи (формулировка задания)
1	Разработайте классификационную схему преднамеренных угроз информационной безопасности для отдельно стоящей ЭВМ
2	Разработайте классификационную схему преднамеренных угроз информационной безопасности для локальной вычислительной сети
3	Разработайте классификационную схему преднамеренных угроз информационной безопасности для локальной вычислительной сети при подключении к сети Интернет
4	Проведите анализ возможностей получения несанкционированного доступа к отдельно стоящей ЭВМ
5	Проведите анализ возможностей получения несанкционированного доступа к локальной вычислительной сети.
6	Проведите анализ возможностей получения несанкционированного доступа к локальной вычислительной сети при подключении к сети Интернет.
7	Назовите известные вам программные средства сканирования уязвимостей сети.
4	Назовите известные вам программные средства, применяемые для расширения привилегий.
5	Назовите известные вам комплекты, содержащие експлойтов, их основные возможности для реализации несанкционированного доступа
6	Назовите известные вам руткиты и их основные возможности по организации скрытых каналов несанкционированного доступа.
7	Оцените возможности различных категорий нарушителей реализовать угрозы информационной безопасности.

ОПК-6 Способность применять нормативные правовые акты в профессиональной деятельности.

8	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «идентификация и аутентификация»
9	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «управление доступом»
10	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «контроль целостности»
11	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «маркировка документов»
12	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «сопоставления пользователя с устройством»
13	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «мандатный принцип управления доступом»

14	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «дискретный принцип управления доступом»
15	Проведите анализ содержания и сущности функционального требования Руководящих документов ФСТЭК России «регистрация и учет»
16	Назовите основные классы защищенности средств вычислительной техники, введенные Руководящими документами ФСТЭК России
17	Назовите основные классы защищенности автоматизированных систем, введенные Руководящими документами ФСТЭК России
18	Назовите основные классы уровней контроля недекларированных функций, введенные Руководящими документами ФСТЭК России
19	Назовите основные классы защищенности межсетевых экранов, введенные Руководящими документами ФСТЭК России

ПСК-4,2 Способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем

20	Постройте логическое дерево атак на отдельную ЭВМ с использованием типового сканера сети и портов.
21	Постройте логическое дерево атак на локальную вычислительную сеть с использованием типового сканера сети и портов.
22	Постройте логическое дерево атак удаленного определения типа операционной системы.
23	Рассчитайте вероятность реализации угрозы информационной безопасности «Сканирование сети» с использованием математического выражения марковской модели защиты.
24	Рассчитайте вероятность реализации угрозы информационной безопасности «Расширение привилегий в системе» с использованием математического выражения марковской модели защиты.
25	Рассчитайте вероятность реализации угрозы информационной безопасности «Захват контроля над системой» с использованием математического выражения марковской модели защиты.
26	Рассчитайте вероятность реализации угрозы информационной безопасности «Отказ в обслуживании» с использованием математического выражения марковской модели защиты.

3.3. Темы аналитического обзора

ПК-22 - Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

№ задания	Тема доклада
1	«Система документов по защите конфиденциальной информации в Российской федерации»

ОПК-6 Способность применять нормативные правовые акты в профессиональной деятельности.

2	«Угрозы безопасности конфиденциальной, организационные меры, технические и программные средства защиты информации от несанкционированного доступа».

Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ЗНАТЬ Основные средства и системы защиты информации, используемые при защите персональных данных. Основные угрозы безопасности персональных данных. Научные и организационные основы защиты информации в информационных системах персональных данных. Информационную систему персональных данных как объект реализации угроз информационной безопасности, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; методы, способы, средства, последовательность и содержание этапов разработки информационных систем персональных данных и подсистем защиты. Методологии и методы проектирования систем защиты персональных данных.	Зачет с оценкой	Уровень владения материалом	ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена
			ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена
			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
УМЕТЬ Анализировать программные, архитектурно-технические и схемотехнические решения компонентов информационных систем персональных данных с целью разработки модели угроз. Проводить классификацию информационных систем персональных данных. Разрабатывать техническое задание на разработку системы защиты персональных	Задания к практическим работам	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена

данных			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетвори тельно	Не освоена
ВЛАДЕТЬ Навыками разработки технического задания на разработку системы защиты в информационных системах персональных данных. Навыками выбора организационных и технических мероприятий по защите информации персональных данных. Навыками контроля защищенности персональных данных в информационных системах при эксплуатации.	Аналитический обзор	Уровень владения	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена