МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра комплексной защиты информации

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
Код и наименование направления подготовки

Организация и технологии защиты государственной тайны
Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

Технология построения защищенных систем обработки информации
Рабочая программа дисциплины

Составитель:
Кандидат военных наук, доцент кафедры комплексной защиты информации
Д.Н. Баранников

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры КЗИ
№ 8 от 23.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: формирование у обучающихся знаний и навыков в сфере обеспечения защиты информации на объекте информатизации, способности оценивать эффективность защиты, а также принимать эффективные управленческие решения при выборе проектов построения защищённых систем обработки информации.

Задачи дисциплины: освоение основных понятий и терминологии в области построения защищённых систем обработки информации, анализ угроз информационной безопасности, приобретение навыков в системном подходе к построению защищенных систем обработки информации.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-1 – Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-1.1 – Знает разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении	*Знать:* • разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении
	ПК-1.2 – Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении	*Уметь:* • разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении
	ПК-1.3 – Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении	*Владеть:* • навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении
ПК-2 – Способен оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов	ПК-2.1 – Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на	*Знать:* • процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации

	соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД	
	ПК-2.2 – Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищённом исполнении	*Уметь:* • разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
	ПК-2.3 – Владеет навыками разработки технического проекта средства и/или системы информатизации в защищённом исполнении	*Владеть:* • навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Технология построения защищённых систем обработки информации» к части, формируемой участниками образовательных отношений блока дисциплин учебного плана к элективным дисциплинам.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Инженерно-техническая защита информации», «Технологии обеспечения информационной безопасности», «Защищённые информационные системы».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения преддипломной практики.

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 з. е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
4	Лекции	32
4	Практические работы	46
	Всего:	78

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _66__ академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Основные понятия, определения и проблемы в области построения защищённых систем обработки информации**	Предмет и содержание дисциплины, основная литература, контроль освоения дисциплины. Правовая основа построения защищённых систем обработки информации. Термины и определения. безопасности. Основные термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
2	**Анализ угроз информационной безопасности**	Особенности классы угроз информационной безопасности систем. Классификация случайных угроз. Классификация преднамеренных угроз. Возможности несанкционированного доступа к информации. Классификация вредоносных программ. Модели нарушителя информационной безопасности.
3	**Концептуальная модель информационной безопасности**	Основные уровни обеспечения информационной безопасности. Особенности правового уровня обеспечения информационной безопасности. Основные элементы административного уровня. Базовые группы процедурных мер защиты информации. Основные механизмы программно-технического уровня обеспечения информационной безопасности.
4	**Системный подход к построению защищенных систем обработки информации**	Базовые принципы построения системы защиты. Основные методы защиты информации. Особенности оптимизации взаимодействия пользователей и обслуживающего персонала. Методы и средства защиты информации от традиционного шпионажа и инсайдерства. Методы и средства защиты от электромагнитных излучений и наводок.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Основные понятия, определения и проблемы в области построения защищённых систем обработки информации	Лекция 1 Практическое занятие 1 Самостоятельная работа	Вводная лекция с использованием видеопроектора Опрос Выполнение задания Подготовка к занятию с использованием электронного курса лекций
2.	Анализ угроз информационной безопасности	Лекция 2 Практическое занятие 2 Самостоятельная работа	Лекция с использованием видеопроектора Опрос Выполнение задания Подготовка к занятию с использованием электронного курса лекций
3.	Концептуальная модель информационной безопасности	Лекция 3 Практическое занятие 3 Самостоятельная работа	Лекция с использованием видеопроектора Опрос Выполнение задания Подготовка к занятию с использованием электронного курса лекций
4.	Системный подход к построению защищенных систем обработки информации	Лекция 4 Практическое занятие 4 Самостоятельная работа	Лекция с использованием видеопроектора Опрос Выполнение задания Подготовка к занятию с использованием электронного курса лекций

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения
5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- опрос (темы 1-4)	*5 баллов*	*20 баллов*
- практические занятия 1-4	*10 баллов*	*40 баллов*
Промежуточная аттестация - *зачет с оценкой*		40 баллов
Итого за семестр		100 баллов

5.2. Критерии выставления оценок

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A, B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	удовлетворительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	неудовлетворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос
1.	Современные проблемы развития теории и практики информационной безопасности
2.	Основные элементы, определяющие меры безопасности системы.
3.	Классификация угроз информационной безопасности систем.
4.	Основные уровни обеспечения информационной безопасности.
5.	В каком нормативно-правовом документе России даётся определение информации как товара?
6.	Понятие объекта защиты.
7.	В чём заключается системный подход к обеспечению информационной безопасности объекта защиты?
8.	Особенности биометрической системы защиты информации
9.	Понятие информационной системы.
10.	Понятие объекта защиты.
11.	Основные подходы к измерению количества информации.
12.	Понятие информационной системы.
13.	Основные принципы построения защищённых систем обработки информации.
14.	Характеристика случайных угроз информационной безопасности.

15.	Классификация преднамеренных угроз информационной безопасности.
16.	Обобщённая схема обеспечения информационной безопасности системы.
17.	Надежность информационных систем по Шеннону
18.	Устойчивость информационных систем по Ляпунову
19.	Стандарт ISO/IEC 27799
20.	ГОСТ Р 34.10-2015
21.	Протоколы RADIUS,Kerberos
22.	Обобщённая схема обеспечения информационной безопасности системы.
23.	Надежность информационных систем по Шеннону

Промежуточная аттестация (зачёт с оценкой)

Примерные вопросы к **зачёту с оценкой**

№	Вопрос
1.	Понятие объекта защиты.
2.	Основные подходы к измерению количества информации.
3.	Понятие информационной системы.
4.	Основные принципы построения защищённых систем обработки информации.
5.	Характеристика случайных угроз информационной безопасности.
6.	Классификация преднамеренных угроз информационной безопасности.
7.	Основные методы шпионажа и инсайдерства.
8.	Базовые мотивы нарушений информационной безопасности.
9.	Классификация нарушителей информационной безопасности.
10.	Основные методы разграничения доступа.
11.	Базовые методы идентификации и аутентификации.
12.	Основные алгоритмы криптографической защиты информации.
13.	Особенности протоколирования и аудита.
14.	Базовые группы процедурных мер для обеспечения защиты автоматизированных систем.
15.	Основные механизмы программно-технического уровня обеспечения защиты автоматизированных систем.
16.	Классификация межсетевых экранов.
17.	Базовые мероприятия на административном уровне обеспечения информационной безопасности.
18.	Особенности административного уровня обеспечения информационной безопасности.
19.	Классификация вредоносных программ.
20.	Основные субъекты информационных отношений при построении защищённых систем обработки информации.
21.	Основные термины, определяющие характер деятельности по обеспечению информационной безопасности

22.	Протоколы CHAP и IPSec
23.	Модули доверенной загрузки ОС от ОКБ САПР
24.	Перехват информации по канал ПЭМИН
25.	Понятие энтропии. Теория надежности систем
26.	Доктрина информационной безопасности Российской Федерации утверждена Президентом Российской Федерации 05.12.2016 г
27.	Современные угрозы информационным системам. Понятие информационных войн
28.	Каскадная модель ЖЦ при технических проектировании систем в защищенном исполнении
29.	Спиральная модель ЖЦ
30.	Поэтапная модель ЖЦ с промежуточным контролем
31.	Интегрированные СКУД
32.	Внешняя защита и внутренняя защита объекта информатизации
33.	Особенности применения информационного оружия
34.	Подготовка специалистов по обеспечению ИБ
35.	Антивирусные средства защиты технических систем
36.	Системы охранной и пожарной сигнализации. Инфракрасные и электрические датчики. Световые установки
37.	Методы и технологии контроля за безопасностью этой информации
38.	Базовые понятия теории информации. Энтропия системы
39.	.Функция корреляция генератора псевдослучайных чисел. Дельта-функция.
40.	Методологии проектирования информационных систем
41.	Техническое обслуживание разработанной системы.
42.	Тестирование и пуско-наладочные работы
43.	Этапы проектирования технических систем в защищенном исполнении
44.	Требования ЕСКД, ЕСПД, ЕСТД.
45.	Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий
46.	Модели разграничения доступа: избирательная, полномочная и ролевая
47.	ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации»

Примерные задания для тестирования (*проверка сформированности компетенций – ПК-1, ПК-2)*

1. К выполняемой функции защиты относится какие два вида с точки зрения действия нарушителей и их проникновения на защищаемый объект ?

Внешняя защита и внутренняя защита

2. ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации» 2022 г. Какой у него номер ?

70262.1

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

основные

1. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.
4. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
5. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
6. *Приказ ФСТЭК России* от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214004&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#034991095371992622 по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время. – Загл. с экрана.
7. *Приказ ФСТЭК России* от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215976&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#08164959407738432 свободный. – Загл. с экрана.
8. *Национальный стандарт РФ ГОСТ Р 70262.1-2022* "Защита информации. Идентификация и аутентификация. Уровни доверия идентификации" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 5 августа 2022 г. N 740-ст) [Электронный ресурс] : Режим доступа : https://docs.cntd.ru/document/1200192541#, свободный. – Загл. с экрана.
9. *Национальный стандарт РФ ГОСТ Р 59453.1-2021* "Защита информации. Формальная модель управления доступом. Часть 1. Общие положения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22

апреля 2021 г. N 270-ст) [Электронный ресурс] : Режим доступа : https://docs.cntd.ru/document/1200179191, свободный. – Загл. с экрана.

10. *Национальный стандарт РФ ГОСТ Р 59453.1-2021* "Защита информации. Формальная модель управления доступом. Часть 2. Общие положения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 апреля 2021 г. N 270-ст) [Электронный ресурс] : Режим доступа : https://docs.cntd.ru/document/1200179192, свободный. – Загл. с экрана.

Литература

основная

1. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная си-стема. — URL: https://e.lanbook.com/book/288974

2. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная си-стема. — URL: https://e.lanbook.com/book/293009

4. Музипов, Х. Н. Программно-технические комплексы автоматизированных систем управления : учебное пособие / Х. Н. Музипов. — Санкт-Петербург : Лань, 2022. — 164 с. — ISBN 978-5-8114-3133-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/213098

5. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152

6. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770

Дополнительная

1. Защита информации в компьютерных системах / под ред. Е.В. *С*тельмашонок, И.Н. Васильевой. – СПб: Изд-во СПбГЭУ, 2017. – 163 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=32254007

2. Корякин С.В. Разработка концепции построения программно-аппаратного ядра универсальной среды проектирования автоматизированных систем защищенного исполнения // Проблемы автоматики и управления. 2020, №1 (38). - С. 60-69. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=43980501

6.2. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru
2. Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru
3. Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru
4. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС)

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases
Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010 или выше	Microsoft	лицензионное
2		Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	условно свободное (необходима регистрация в сетевой академии Cisco)
5	VMware Workstation 15 Player	VMware, Inc	свободное
6	или VirtualBox 6.0	Oracle	свободное
7	Дистрибутивы Linux (например Ubuntu 14)	Oracle	свободное

Средства вычислительной техники, сетевое оборудование, техническое, программное и программно-аппаратные средства защиты информации и средствами контроля защищённости информации.

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г.
3	Профессиональные полнотекстовые БД Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;

- в форме электронного документа;

- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;

- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;

- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
- устройством для сканирования и чтения с камерой SARA CE;
- дисплеем Брайля PAC Mate 20;
- принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения.
Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.
Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.
Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1

Тема – Доктрина информационной безопасности Российской Федерации

Задания:

1. Термины, определяющие научную основу информационной безопасности.
2. Термины, определяющие предметную основу информационной безопасности.
3. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
4. Национальные интересы России в информационной сфере.
5. Основные информационные угрозы РФ.
6. Основные направления обеспечения информационной безопасности.
7. Организационная основа системы обеспечения информационной безопасности РФ.
8. Участники системы обеспечения информационной безопасности РФ.

Практическое занятие 2

Тема – Классификация преднамеренных угроз информационной безопасности

Задания:

1. Базовые методы шпионажа и инсайдерства.
2. Основные причины несанкционированного доступа к информации;.
3. Особенности прослушивания объекта защиты.
4. Классификация нарушителей безопасности информационных систем.
5. Особенности инсайдеров и аутсайдеров.
6. Основные классы вредоносных программ.
7. Особенности побочных электромагнитных излучений и наводок (ПЭМИН).
8. Основные виды компьютерных вирусов.

Практическое занятие 3

Тема – Национальные стандарты России, созданные на основе международной серии стандартов ISO/IEC 27000

Задания:

1. ГОСТ Р ИСО/МЭК 27000-2012 как глоссарий терминов в области системы менеджмента информационной безопасности (СМИБ).

2. Нормативные требования для создания, внедрения и эксплуатации СМИБ (ГОСТ Р ИСО/МЭК 27001-2006).

3. Руководство по внедрению средств управления защитой информации (ГОСТ Р ИСО/МЭК 27002-2012).

4. Описание процессного подхода к внедрению СМИБ (ГОСТ Р ИСО/МЭК 27003-2012).

5. Система измерений, позволяющая оценивать эффективность СМИБ (ГОСТ Р ИСО/МЭК 27004-2011).

6. Руководство по внедрению процессного подхода к управлению рисками (ГОСТ Р ИСО/МЭК 27005-2010).

7. Руководство для органов, проводящих аудит и сертификацию СМИБ (ГОСТ Р 27006-2008).

8. Руководство для организаций, реализующих внутренний или внешний аудит СМИБ (ГОСТ Р 27007-2014).

Практическое занятие 4

Тема – Методы и средства защиты информации от шпионажа и инсайдерства

Задания:

1. Основные задачи защиты информации от шпионажа и инсайдерства.
2. Базовые рубежи защиты объекта от шпионажа и инсайдерства.
3. Состав системы охраны защищаемого объекта.
4. Основные требования к системам охранной сигнализации.
5. Базовые виды датчиков для выявления злоумышленников.
6. Основные элементы телевизионной системы видеоконтроля.
7. Основные методы борьбы с подслушиванием.
8. Методы и средства защиты от электромагнитных излучений и наводок.

Приложение 1 Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Технологии построения защищённых систем обработки информации» реализуется на факультете Информационных систем и безопасности для студентов 2-го курса, обучающихся по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность (профиль подготовки – Организация и технологии защиты государственной тайны) кафедрой комплексной защиты информации.

Цель дисциплины: формирование у обучающихся знаний и навыков в сфере обеспечения защиты информации на объекте информатизации, способности оценивать эффективность защиты, а также принимать эффективные управленческие решения при выборе проектов построения защищённых систем обработки информации.

Задачи дисциплины:

– освоение основных понятий и терминологии в области построения защищённых систем обработки информации,

– анализ угроз информационной безопасности,

– приобретение навыков в системном подходе к построению защищённых систем обработки информации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-1 – Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
- ПК-2 – Способен оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов

В результате освоения дисциплины обучающийся должен:

Знать*:*

- разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении
- процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации

Уметь*:*

- разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении;
- разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

Владеть*:*

- навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении
- навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой.
Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.