

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

СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ
ГУМАНИТАРНОЙ СФЕРЫ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) подготовки
Прикладная информатика в гуманитарной сфере
Уровень квалификации выпускника бакалавр

Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Системы комплексной безопасности организаций гуманитарной сферы

Рабочая программа дисциплины

Составитель(и):

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры

комплексной защиты информации

№12 от 10.06.2021 г

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

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

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

9. Методические материалы

9.1. Планы практических (семинарских, лабораторных) занятий

9.2. Методические рекомендации по подготовке письменных работ

Приложения

Приложение 1. Аннотация дисциплины

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – подготовить выпускника, умеющего разрабатывать систему по обеспечению безопасности информационных ресурсов, как для автономных, так и распределённых вычислительных систем организаций гуманитарной сферы.

Задачи дисциплины:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения информационной безопасности в информационных системах различного назначения;
- изучение теоретических основ информационной безопасности;
- формирование умений использовать основные достижения в области информационной безопасности при реализации своей профессиональной деятельности;
- владение навыками обеспечения защиты информации в информационных системах различного назначения;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-8 – способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-8.1 – Знает способы организации ИТ-инфраструктуры, методы и приёмы управления информационной безопасностью	Знать: способы организации ИТ-инфраструктуры и защиты информации, методы и приёмы управления информационной безопасностью организаций гуманитарной сферы
	ПК-8.2 – Умеет организовывать ИТ-инфраструктуру предприятия и процессы управления информационной безопасностью	Уметь: организовать ИТ-инфраструктуру предприятия гуманитарной сферы и защиты информации, в том числе циркулирующей по каналам связи.
	ПК-8.3 – Владеет навыками организации ИТ-инфраструктуры и управления информационной безопасностью	Владеть: навыками организации ИТ-инфраструктуры предприятия гуманитарной сферы и управления информационной безопасностью, навыками защиты информации, циркулирующей в информационной системе предприятия.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Системы комплексной безопасности организаций гуманитарной сферы» относится к дисциплинам части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Информатика» «Информационно-вычислительные сети и телекоммуникационные технологии», «Информационные системы», «Информационные технологии».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Проектный практикум в информатизации гуманитарной сферы», «Управление проектами информационных систем гуманитарной сферы».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 з.е., 114 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., промежуточная аттестация 18 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Тема 1. Понятие, сущность и угрозы информационной безопасности	5	2	–				4	Опрос.
2	Тема 2. Законодательный, административный и процедурный уровни уровня обеспечения информационной безопасности	5	2					4	Опрос.
3	Тема 3. Программно-технический уровень обеспечения информационной безопасности	5							
4	<i>Тема 3.1. Разграничение доступа к информации</i>	5	2					2	
5	<i>Тема 3.2. Криптографическая защита информации</i>	5	2					2	
6	<i>Тема 3.3. Основы организации сетей. Межсетевое экранирование</i>	5	4					2	
7	<i>Тема 3.4. Прочие сервисы защиты информации</i>	5	2					2	Опрос.
8	Практическое занятие 1. Разворачивание сети предприятия	5			4			6	Защита практического занятия
9	Практическое занятие 2. Разграничение	5			4			8	Защита практического занятия

	доступа в сегментах сети								
10	Практическое занятие 3. Настройка списков контроля доступа	5			6			8	Защита практического занятия
11	Практическое занятие 4. Межсетевое экранирование	5			8			8	Защита практического занятия
12	Практическое занятие 5. Создание VPN-канала	5			6			8	Защита практического занятия
13	<i>Экзамен</i>	5					18		<i>Экзамен по билетам</i>
	итого:		14		28		18	54	

3. Содержание дисциплины

Тема 1. Понятие, сущность и угрозы информационной безопасности

Понятие безопасности объекта (государства, предприятия и информационной системы). Основные компоненты безопасности государства и доминирующая роль информационной безопасности (ИБ). Становление и развитие понятия «информационная безопасность». Сущность и понятия ИБ и защиты информации. Необходимость и значение нормативно-правового определения основных понятий. Связь ИБ с информатизацией общества. Базовые уровни обеспечения информационной безопасности и защиты информации.

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в ИС. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите информационных систем от реализации угроз.

Тема 2. Законодательный, административный и процедурный уровни обеспечения информационной безопасности

Предпосылки создания международных стандартов по обеспечению информационной безопасности. Назначение стандартов и какие задачи решаются при использовании стандартов в области информационной безопасности: в определении цели обеспечения информационной безопасности компьютерных систем, создания эффективной системы управления информационной безопасностью, критерии оценки соответствия информационной безопасности заявленным целям, создания условий применения, имеющегося инструментария (программных средств) обеспечения информационной безопасности и оценки ее текущего состояния.

Назначение и основные положения международных стандартов: «Критерии оценки надежности компьютерных систем» («Оранжевая книга»), «Информационная безопасность распределённых систем. Рекомендации X.800», ISO 15408 – «Общие критерии». Международные стандарты семейства 27000.

Основные федеральные органы, разрабатывающие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации. Государственная система по обеспечению безопасности и защиты информации (ГСЗИ). Основные законодательные акты РФ в области информационной безопасности и защиты информации. Руководящие документы ФСБ России, ФСТЭК России в области ИБ и защиты информации от несанкционированного доступа при ее обработке с использованием СВТ.

Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки ПИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.

Назначение и задачи процедурного уровня по обеспечению информационной безопасности. Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Тема 3. Программно-технический уровень обеспечения информационной безопасности

Технология обеспечения ИБ, цели и принципы построения архитектуры ИБ. Основные понятия программно-технического уровня обеспечения информационной безопасности.

Особенности современных информационных систем, существенные с точки зрения обеспечения информационной безопасности. Архитектурная безопасность.

Меры безопасности: превентивные, препятствующие нарушениям информационной безопасности, меры обнаружения нарушений, меры локализирующие, сужающие зону воздействия нарушений, меры по прослеживанию нарушителя, меры восстановления режима безопасности.

Программные сервисы защиты информации в информационных системах. Идентификация и аутентификация пользователей. Базовые методы парольной аутентификации. Модели разграничения доступа к информации.

Протоколирование и аудит (активный и пассивный) информационной системы, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потокное и блочное шифрование. Процедура формирования электронной подписи.

Виды сетей и сетевые топологии. Базовая эталонная модель Взаимосвязи открытых систем (ISO/OSI). Основные протоколы сетей Ethernet.

Межсетевое экранирование. Виды межсетевых экранов. Основные сервисы защиты в информационно-телекоммуникационных сетях (ИТС).

Виртуальные частные сети. Виды сетей. Работа VPN на различных уровнях модели OSI.

Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Тема 1. Понятие, сущность и угрозы информационной безопасности	Лекция 1	Традиционная с использованием презентаций Консультирование посредством электронной почты
2	Тема 2. Законодательный, административный и процедурный уровни уровня обеспечения информационной безопасности	Лекция 2	Традиционная с использованием презентаций Консультирование посредством электронной почты
3	Тема 3. Программно-технический уровень обеспечения информационной безопасности	Лекция 3.1 Лекция 3.3 Лекция 3.3 Лекция 3.4	Традиционная с использованием презентаций Консультирование посредством электронной почты
8	Разворачивание сети предприятия	Практическое занятие 1.	Выполнение и защита практической работы Консультирование посредством электронной почты
9	Разграничение доступа в сегментах сети	Практическое занятие 2.	Выполнение и защита практической работы Консультирование посредством электронной почты
10	Настройка списков контроля доступа	Практическое занятие 3.	Выполнение и защита практической работы Консультирование посредством электронной почты
11	Межсетевое экранирование	Практическое занятие 4.	Выполнение и защита практической работы Консультирование посредством электронной почты
12	Создание VPN-канала	Практическое занятие 5.	Выполнение и защита практической работы Консультирование посредством электронной почты

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну ра- боту	Всего
Текущий контроль:		
– <i>Опрос</i>	<i>5 баллов</i>	<i>15 баллов</i>
– <i>Защита практического занятия 1</i>	<i>5 баллов</i>	<i>5 баллов</i>
– <i>Защита практических занятий 2-5</i>	<i>10 баллов</i>	<i>40 баллов</i>
Промежуточная аттестация		<i>40 баллов</i>
<i>Экзамен</i>		
Итого за дисциплину		<i>100 баллов</i>
<i>Экзамен</i>		

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шка- ла	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ А, В	«отлично» / «зачтено (отлично)» / «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	«хорошо» / «зачтено (хорошо)» / «зачтено»	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D, E	«удовлетворительно» / «зачтено (удовлетворительно)» / «зачтено»	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		станции. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	«неудовлетворительно» / не зачтено	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 выставляется 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

1. Основные составляющие информационной безопасности (ИБ).
2. Характеристика проблем ИБ.
3. Концепция объектно-ориентированного подхода к обеспечению ИБ.
4. Недостатки традиционного подхода к обеспечению ИБ.
5. Характеристика наиболее распространённых угроз.
6. Критерии классификации угроз.
7. Примеры угроз доступности.
8. Вредоносное программное обеспечение.
9. Основные угрозы целостности
10. Основные угрозы конфиденциальности.
11. Что такое законодательный уровень ИБ и почему он важен?
12. Основные законы РФ в области ИБ.
13. Основные зарубежные стандарты в области ИБ.
14. Что такое оценочные стандарты и технические спецификации?
15. Что такое оранжевая книга и для чего она применяется?
16. Рекомендации X.800.
17. Стандарт ISO/ IEC.
18. Что такое политика безопасности и ее актуальность?
19. Что такое программа безопасности и ее актуальность?
20. В чем проявляется административный уровень ИБ?

21. Как синхронизируется политика безопасности с жизненным циклом ИС?
22. Этапы управления рисками в системе защиты информации.
23. Основные программно-технические меры защиты.
24. Технология идентификации и аутентификации.
25. Технология управления доступом.
26. Протоколирование и аудит.
27. Технология шифрования.
28. Архитектурные аспекты экранирования.
29. Классификация межсетевых экранов.
30. Анализ защищённости.
31. Возможности типичные схем туннелирования.
32. Уровни модели OSI, на которых производится туннелирование
33. Задачи управления системой ИБ.

Примерные задания для тестирования

1. Целью защиты циркулирующей в информационной системе информации являются:

а) предотвращение утечки, искажения, утраты, блокирования или незаконного тиражирования информации.

б) предотвращение утечки, искажения, утраты, блокирования или незаконного тиражирования информации, а также несанкционированного доступа к информации.

в) предотвращение несанкционированного доступа к информации.

2. Шлюз безопасности VPN – это:

а) сетевое устройство, подключаемое к двум и более сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним.

б) сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним.

в) сетевое устройство, подключаемое к двум и более сетям и выполняющее функции шифрования и авторизации для различных хостов.

Примерные вопросы к экзамену

1. Сущность и понятия информационной безопасности и защиты информации.
2. Классификация угроз безопасности информации по цели реализации угрозы, принципу, характеру и способу её воздействия.
3. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки.
4. Основные методы и каналы несанкционированного доступа к информации в ИС
5. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России.
6. Структура политика информационной безопасности предприятия как документа и основные этапы её разработки.
7. Назначение и основные положения международных стандартов: «Критерии оценки надёжности компьютерных систем» («Оранжевая книга»), «Информационная безопасность распределённых систем. Рекомендации X.800», ISO 15408 – «Общие критерии».
8. Руководящие документы ФСБ России, ФСТЭК России в области информационной безопасности и защиты информации от несанкционированного доступа при ее обработке с использованием СВТ
9. Концепция информационной безопасности предприятия, её цели и этапы построения.
10. Задачи, решаемые при анализе рисков для информационной системы. Базовые методики, используемые для оценки рисков.
11. Назначение и задачи процедурного уровня по обеспечению информационной безопасности. Основные классы мер процедурного уровня.

12. Технология обеспечения информационной безопасности, цели и принципы построения архитектуры информационной безопасности.
13. Особенности современных информационных систем, существенные с точки зрения обеспечения информационной безопасности. Архитектурная безопасность.
14. Программные сервисы защиты информации в информационных системах.
15. Назначение и сущность идентификация и аутентификация пользователей в информационной системе.
16. Основные меры безопасности информационной системы
17. Базовые методы парольной аутентификации.
18. Модели разграничения доступа к информации и их краткая характеристика
19. Дискреционная модель разграничения доступа к информации
20. Мандатная модель разграничения доступа к информации
21. Ролевая разграничения доступа к информации
22. Протоколирование и аудит (активный и пассивный) информационной системы, их основные цели и особенности.
23. Базовые методы криптографического преобразования данных. Потокное и блочное шифрование.
24. Процедура формирования электронной подписи.
25. Виды сетей и сетевые топологии.
26. Модели ISO/OSI и TCP/IP сетей
27. Основные протоколы сетей Ethernet.
28. Беспроводные сети, их особенности и основные стандарты
29. Сущность межсетевого экранирования и виды межсетевых экранов.
30. Основные сервисы защиты в информационно-телекоммуникационных сетях
31. Понятие, назначение, структура и виды виртуальных частных сетей.
32. Работа VPN на различных уровнях модели OSI
33. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними.
34. Антивирусные программные комплексы, назначение и сравнительная характеристика

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. *Федеральный закон* от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., посл. от 01.05.2019). [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» (с изм. и доп., посл. от 31.12.2017). [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» (с изм. и доп., посл. от 23.06.2016). [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.
4. *Федеральный закон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» (с изм. и доп., посл. от 28.11.2018). [Электронный ресурс]: Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Дополнительные

5. *Постановление Правительства Российской Федерации* от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных(криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных(криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных(криптографических)средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных(криптографических) средств (за исключением случая, если техническое обслуживание шифровальных(криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных(криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». (с изм. и доп., посл. от 18.05.2017). [Электронный ресурс] : Режим доступа : <http://www.consultant.ru/cons/cgi/online.cgi?rnd=8BEAE327715772BF511477DA184EFA2&req=doc&base=LAW&n=217125&dst=100007&fld=134&stat=refcode%3D16876%3Bdstident%3D100007%3Bindex%3D0#rn1enft0qj>, свободный. – Загл. с экрана.
6. Положение о разработке, производстве, реализации и эксплуатации шифровальных(криптографических) средств защиты информации (Положение ПКЗ-2005), утв. Приказом Директора ФСБ России от 09 февраля 2005 года № 66. (с изм. и доп., посл. от 12.04.2010) [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_52098/, по нерабочим дням, но можно заказа документ на электронную почту. – Загл. с экрана.

Литература

Основная

1. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва: Издательство Юрайт, 2019. – 309 с. <https://www.biblio-online.ru/bcode/433715> (дата обращения: 23.08.2019).
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2019. – 592 с. – (Высшее образование: Бакалавриат). – Текст: электронный. – URL: <https://new.znaniium.com/catalog/product/996789>
3. Яновский Г.Г. Сети связи: Учебник / Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. – СПб:БХВ-Петербург, 2014. – 401 с. – Режим доступа: <http://znaniium.com/catalog/product/944261>
4. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва: Издательство Юрайт, 2019. – 309 с. <https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715>

Дополнительная

5. *Гришина Н. В.* Организация комплексной системы защиты информации / Н. В. Гришина. - М.: Гелиос АРВ, 2007. - 254 с.: рис., табл.; 20 см. - Экз. № 541-08 с автогр. авт. - Библиогр.: с. 248-252 (45 назв.).

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : <http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer>, свободный. – Загл. с экрана.
2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана

3. ОХРАНА.ru. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : <http://www.nicohrana.ru>, свободный. – Загл. с экрана.
4. Sec.ru. Портал по безопасности. [Электронный ресурс] : Режим доступа : <http://sec.ru/>, необходима регистрация. – Загл. с экрана.
5. Банк данных угроз безопасности информации. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : <http://sec.ru/>, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:

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

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Платформа ZOOM	ZOOM	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
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	Свободное
5.	Платформа ZOOM	ZOOM	лицензионное

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, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ПК-8

Практическое занятие 1 (4 ч) Разворачивание сети предприятия

Задания:

1. В симуляторе Cisco Packet Tracer создать сеть организации и её филиала.
2. Настроить сетевые и оконечные устройства.
3. Составить отчёт о практической работе

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому студенту адресное пространство IP-адресов и требования к подразделениям организации по структуре и количеству оконечных узлов в каждом отделе.
2. Студентам запрещается использовать не своё адресное пространство. За это снижается оценка.
3. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : <http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer>, свободный. – Загл. с экрана..
2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана.
3. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://www.biblio-online.ru/bcode/433715> (дата обращения: 23.08.2019).

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

Практическое занятие 2 (4 ч) Разграничение доступа в сегментах сети

Задания:

1. В симуляторе Cisco Packet Tracer в созданной сети предприятия произвести с помощью технологии VLAN разбиение сети на сегменты.
2. Составить отчёт о практической работе

Указания по выполнению заданий:

1. Работать строго в своём адресном пространстве.
2. Студентам запрещается использовать не своё адресное пространство. За это снижается оценка.
3. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : <http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer>, свободный. – Загл. с экрана..
2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана.
3. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://www.biblio-online.ru/bcode/433715> (дата обращения: 23.08.2019).

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

Практическое занятие 3 (6 ч) Настройка списков контроля доступа

Задания:

1. На маршрутизаторах внутренней сети организации и филиала настроить списки контроля доступа по заданным преподавателем требованиям.
2. Составить отчёт о практической работе.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому студенту данные о том, какую информацию следует заблокировать, а какую разрешить для каждого отдела организации и филиала.
2. Работать строго в своём адресном пространстве.
3. Студентам запрещается использовать не своё адресное пространство. За это снижается оценка.
4. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : <http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer>, свободный. – Загл. с экрана..
2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана.
3. *Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://www.biblio-online.ru/bcode/433715> (дата обращения: 23.08.2019).*

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

Практическое занятие 4 (8 ч) Межсетевое экранирование

Задания:

1. Провести межсетевое экранирование с использованием маршрутизаторов сети предприятия.
2. Добавить к сети предприятия и филиала межсетевые экраны Cisco ASA и выполнить экранирование сетей с учётом ограничений лицензии Cisco Packet Tracer для Cisco ASA
3. Составить отчёт о практической работе.

Указания по выполнению заданий:

5. Работать строго в своём адресном пространстве.
1. Студентам запрещается использовать не своё адресное пространство. За это снижается оценка.
2. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

4. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : <http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer>, свободный. – Загл. с экрана..
5. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана.
6. *Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://www.biblio-online.ru/bcode/433715> (дата обращения: 23.08.2019).*

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

Практическое занятие 5 (6 ч) Создание VPN-канала

Задания:

1. Создать защищённый туннель между организацией и филиалом.
2. Составить отчёт о практической работе.

Указания по выполнению заданий:

1. Работать строго в своём адресном пространстве.
2. Студентам запрещается использовать не своё адресное пространство. За это снижается оценка.
3. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : <http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer>, свободный. – Загл. с экрана..
2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijJLa94T9>, свободный. – Загл. с экрана.
3. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://www.biblio-online.ru/bcode/433715> (дата обращения: 23.08.2019).

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

По результатам практического занятия обучающиеся составляют отчёт, структура которого представлена ниже. Отчёт составляется в электронной форме с использованием MS Office 2007 и выше и передаётся преподавателю посредством оговорённой формы связи.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Системы комплексной безопасности организаций гуманитарной сферы» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе магистратуры по направлению подготовки 09.03.03 Прикладная информатика (профиль подготовки – Прикладная информатика в гуманитарной сфере) кафедрой комплексной защиты информации.

Цель дисциплины: подготовить выпускника, умеющего разрабатывать систему по обеспечению безопасности информационных ресурсов, как для автономных, так и распределённых вычислительных систем организаций гуманитарной сферы.

Задачи: получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения информационной безопасности в информационных системах различного назначения; изучение теоретических основ информационной безопасности; формирование умений использовать основные достижения в области информационной безопасности при реализации своей профессиональной деятельности; владение навыками обеспечения защиты информации в информационных системах различного назначения; развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения..

Дисциплина направлена на формирование следующих компетенций:

- ПК-8 – способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью

В результате освоения дисциплины обучающийся должен:

Знать: способы организации ИТ-инфраструктуры и защиты информации, методы и приёмы управления информационной безопасностью организаций гуманитарной сферы

Уметь: организовать ИТ-инфраструктуру предприятия гуманитарной сферы и защиты информации, в том числе циркулирующей по каналам связи.

Владеть: навыками организации ИТ-инфраструктуры предприятия гуманитарной сферы и управления информационной безопасностью, навыками защиты информации, циркулирующей в информационной системе предприятия.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы.