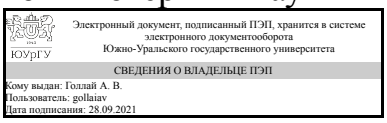
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



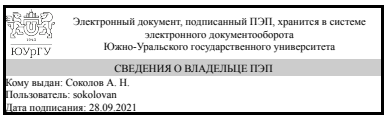
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.36 Информационная безопасность открытых систем
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

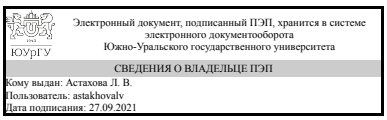
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
д.пед.н., проф., профессор



Л. В. Астахова

Челябинск

1. Цели и задачи дисциплины

Целью дисциплины является: изучение технологий, методов и средств создания защищенных открытых информационных систем (ИС) . Задачами дисциплины являются: - привитие обучаемым основ культуры обеспечения информационной безопасности (ИБ) в ОИС; - формирование у обучаемых понимания основ построения защищенных ОИС; - ознакомление обучаемых с основными уязвимостями, угроза ИБ и сетевыми атаками, ха-рактерными для современных ОИС; - обучение различным подходам и методам обеспечения ИБ ОИС.

Краткое содержание дисциплины

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:Основные угрозы безопасности информации и модели нарушителя в информационных (автоматизированных) систем
	Уметь:Анализировать и оценивать угрозы информационной безопасности объекта
	Владеть:
ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	Знать:эталонную модель взаимодействия открытых систем
	Уметь:
	Владеть:
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать:риски подсистемы защиты информации и экспериментальные методы их оценки; методы и средства контроля эффективности программно-аппаратной защиты информации
	Уметь:Анализировать и оценивать угрозы информационной безопасности объекта
	Владеть:
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Знать:принципы формирования политики информационной безопасности в информационных (автоматизированных) системах
	Уметь:разрабатывать частные политики информационной безопасности информационной безопасности информационных (автоматизированных) систем
	Владеть:навыками анализа информационной инфраструктуры информационных (автоматизированных) систем и их безопасности навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем

ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать:основные угрозы безопасности информации и модели нарушителя в информационных (автоматизированных) системах
	Уметь:
	Владеть:
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать:принципы формирования политики информационной безопасности в информационных (автоматизированных) системах
	Уметь:определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных (автоматизированных); разрабатывать частные политики информационной безопасности информационной безопасности информационных (автоматизированных) систем
	Владеть:навыками анализа информационной инфраструктуры информационных (автоматизированных) систем и их безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.27 Безопасность сетей электронных вычислительных машин, Б.1.28 Безопасность операционных систем	Б.1.24.01 Организационное обеспечение информационной безопасности

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.28 Безопасность операционных систем	Знать: принципы построения и функционирования, примеры реализаций современных операционных систем; критерии оценки эффективности и надежности средств защиты ОС; принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows; Уметь: планировать политику безопасности операционных систем; Владеть: навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности
Б.1.27 Безопасность сетей электронных вычислительных машин	Знать: эталонную модель взаимодействия открытых систем; принципы построения и функционирования, примеры реализаций современных локальных и глобальных

	компьютерных сетей; последовательность и содержание этапов построения компьютерных сетей; основные протоколы сетей ЭВМ; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ Уметь: проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; проводить мониторинг угроз безопасности компьютерных сетей; эффективно использовать различные методы и средства защиты информации для компьютерных сетей Владеть: навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС)	80	80
Подготовка курсовой работы	50	50
Выполнение 2 самостоятельных заданий (см. Содержание дисциплины)	30	30
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен,КР

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Нормативные и концептуальные основы ИБОС	10	2	0	8
2	Атаки по уровням иерархической системы OSI и	14	6	0	8

	защита от них				
3	Комплексное обеспечение ИБОС	20	12	0	8
4	Средства обеспечения ИБОС	20	12	0	8

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Нормативные и концептуальные основы ИБОС	2
2	2	Атаки по уровням иерархической системы OSI и защита от них	4
3	2	Атаки на беспроводные устройства	2
4	3	Комплексное обеспечение ИБОС: аутентификация, управление доступом, неотказуемость	4
5	3	Комплексное обеспечение ИБОС: конфиденциальность, целостность	2
6	3	Документационное сопровождение ИБОС: общие подходы	4
7	3	Документационное сопровождение обеспечения отдельных направлений ИБОС	2
8	4	Средства обеспечения ИБОС	4
9	4	Обеспечение сетевой безопасности	4
10	4	Инструментальные средства аудита ИБОС	4

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Нормативные и концептуальные основы ИБОС в России	4
2	1	Нормативные и концептуальные основы ИБОС за рубежом	4
3	2	Моделирование угроз ИБОС	4
4	2	Технологии защиты от атак	4
5	3	Аутентификация	4
6	3	Управление доступом к файловым ресурсам	4
7	4	Технологические процессы внедрения средств обеспечения ИБОС	4
8	4	Разработка политики ИБОС	4

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Документационное обеспечение ИБОС	Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопас-ность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 1 - Угрозы, уязвимости, атаки и подходы к защите. - М.: Горячая линия-	15

	Телеком, 2006, 538 с. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопас-ность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 2 - Средства защиты в сетях. - М.: Горячая линия-Телеком, 2008, 558 с. Информационные ресурсы Интернет.	
Подготовка курсовой работы	1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие / П.Н. Девянин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049. — Загл. с экрана. 2. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 2-е изд. — Москва : МГТУ им. Н.Э. Баумана, 2018. — 250 с. — ISBN 978-5-7038-4899-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172839 (дата обращения: 20.09.2021). — Режим доступа: для авториз. пользователей. 3. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана. 4. Мельников, Д.А. Информационная безопасность открытых систем. [Электронный ресурс] — Электрон. дан. — М. : ФЛИНТА, 2014. — 448 с. — Режим доступа: http://e.lanbook.com/book/48368 — Загл. с экрана 5. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопас-ность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 1 - Угрозы, уязвимости, атаки и подходы к защите. - М.: Горячая линия-Телеком, 2006, 538 с. 6. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопас-ность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 2 - Средства защиты в сетях. - М.: Горячая линия-Телеком, 2008, 558 с. Электронные ресурсы НБ ЮУрГУ	50
Новые технологии ИБОС	1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных	15

	информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с. 2. Ворона, В.А. Системы контроля и управления доступом [Электронный ресурс] / В.А. Ворона, В.А. Тихонов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2018. — 272 с. — Режим доступа: https://e.lanbook.com/book/111037. — Загл. с экрана. 3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие / П.Н. Девянин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049. — Загл. с экрана. 4. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана. 5. Электронные ресурсы НБ ЮУрГУ	

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Активные и интерактивные формы проведения занятий	Лекции	"Перевернутое" обучение с использованием экспертов по отдельным темам курса	28

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Проблемное обучение	Выявление проблем ИБОС и новых российских и зарубежных технологий их решения

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование	Контролируемая компетенция ЗУНы	Вид контроля	№№

разделов дисциплины		(включая текущий)	заданий
Все разделы	ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	письменный опрос (тестирование), отчет о лабораторных работах, защита курсовой работы	1-29
Все разделы	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	письменный опрос (тестирование), отчет о лабораторных работах, защита курсовой работы	1-29; Л31, Л33, Л34
Все разделы	ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	письменный опрос (тестирование), отчет о лабораторных работах, защита курсовой работы	1-29; Л31, Л33, Л34
Все разделы	ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	письменный опрос (тестирование), отчет о лабораторных работах, защита курсовой работы	1-29; Л34, Л35, Л36, Л37
Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	письменный опрос (тестирование), отчет о лабораторных работах, защита курсовой работы	1-29; Л38
Все разделы	ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	письменный опрос (тестирование), отчет о лабораторных работах, защита курсовой работы	1-29

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
	Письменный опрос осуществляется на последнем занятии изучаемого раздела. Студенту задаются 5 вопросов из списка контрольных вопросов. Время, отведенное на опрос -20 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Правильный ответ на вопрос соответствует 2 баллам. Частично правильный ответ соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов. Вместо	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %.

	письменного опроса может проводиться тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов – 10. Весовой коэффициент мероприятия (за каждый письменный опрос) – 0,05.	
	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, своевременность выполнения работы и ответы на вопросы (задаются 2-3 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей (за каждое практическое задание): - правильность оформления отчета, если отчет оформлен с недочетами из оценки вычитается 1 балл; - своевременность сдачи отчета, за каждую неделю просрочки отчета из оценки вычитается 0,5 балла; - ответы на вопросы, оценка снижается на 1 балл за каждый неправильный ответ на вопрос. Максимальное количество баллов за одну работу – 10. Весовой коэффициент мероприятия (за каждую работу) – 0,05.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %.
	Техническое задание выдается в первую неделю семестра. За две недели до окончания семестра студент демонстрирует и сдает преподавателю работу. В процессе проверки оценивается соответствие работы техническому заданию. Преподаватель выставляет предварительную оценку и допускает студента к защите. В последнюю неделю семестра проводится защита КР. На защиту студент предоставляет: 1. Задание на КР. 2. Пояснительную записку на 20-25 страницах в отпечатанном виде с приложениями. 4. Презентацию. На защите студент коротко (5-7 мин.) докладывает об основных проектных решениях, принятых в процессе разработки, и отвечает на вопросы. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: – Соответствие заданию: 3	Отлично: Величина рейтинга обучающегося по курсовой работе 85…100 % Работа соответствует заданию, пояснительная записка имеет логичное, последовательное изложение материала с соответствующими выводами и обоснованными положениями. Хорошо: Величина рейтинга обучающегося по курсовой работе 75…84 % Работа полностью соответствует техническому заданию, работоспособна при большинстве попыток нарушения, пояснительная записка имеет грамотно изложенную теоретическую главу, в ней представлены достаточно подробный анализ и критический разбор практической деятельности, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными положениями. При ее защите студент показывает знание вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, без особых

	балла – полное соответствие заданию. 2 балла – в основном полное соответствие заданию. 1 балл – неполное соответствие заданию. 0 баллов – несоответствие заданию. – Качество пояснительной записки: 3 балла – 2 балла – пояснительная записка имеет грамотно изложенную теоретическую главу, в ней представлены достаточно подробный анализ и критический разбор практической деятельности, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными положениями. 1 балл – пояснительная записка имеет теоретическую главу, базируется на практическом материале, но имеет поверхностный анализ, в ней просматривается непоследовательность изложения материала, представлены необоснованные положения 0 балл – пояснительная записка не имеет анализа, не отвечает требованиям, изложенным в методических рекомендациях кафедры. В работе нет выводов либо они носят декларативный характер. – Защита курсовой работы: 3 балла – при защите студент показывает глубокое знание вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, легко отвечает на поставленные вопросы 2 балла – при защите студент показывает знание вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, без особых затруднений отвечает на поставленные вопросы 1 балл – при защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы 0 баллов – при защите студент затрудняется отвечать на поставленные вопросы по ее теме, не знает теории вопроса, при ответе допускает существенные ошибки Максимальное количество баллов – 9.	затруднений отвечает на поставленные вопросы. Удовлетворительно: Величина рейтинга обучающегося по курсовой работе 60…74 % Работа полностью соответствует техническому заданию, внедрение работоспособно только в части попыток нарушения политики, пояснительная записка имеет теоретическую главу, базируется на практическом материале, но имеет поверхностный анализ, в ней просматривается непоследовательность изложения материала, представлены необоснованные положения. При ее защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы. Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 %Работа не соответствует техническому заданию, не работоспособна или работоспособна только в малой части попыток нарушения политики, пояснительная записка не имеет анализа, не отвечает требованиям, изложенным в методических рекомендациях кафедры. В работе нет выводов либо они носят декларативный характер. При защите работы студент затрудняется отвечать на поставленные вопросы по ее теме, не знает теории вопроса, при ответе допускает существенные ошибки
	На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности	Отлично: 85…100 % Оценка «Отлично» выставляется за ответ, который полностью раскрывает поставленный вопрос. Студент показывает глубокое знание вопросов темы, свободно оперирует терминами предметной области и легко отвечает на поставленные вопросы. Хорошо: 75…84 % Оценка «Хорошо» выставляется за ответ, который полностью соответствует

	обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Отлично: Величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: Величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 % Если рейтинг обучающегося по дисциплине ниже 60%, то он сдает экзамен с целью возможного повышения рейтинга. По результатам сдачи экзамена выставляется оценка, которая учитывается при определении рейтинга.	поставленному вопросу. Ответ демонстрирует хорошее владение материалом и наличие навыков решения поставленных задач. Ответ содержит последовательное изложение материала с соответствующими выводами, однако, положения ответа не всегда достаточной степени обоснованы, а используемая терминология не всегда корректна. Удовлетворительно: 60…74 % Оценка «Удовлетворительно» выставляется за ответ, который не полностью соответствует поставленному вопросу, содержит незначительные пробелы в излагаемом материале. Студент в недостаточной степени владеет общепринятой терминологией, а также слабыми навыками решения прикладных задач. Неудовлетворительно: 0…59 % Оценка «Неудовлетворительно» выставляется за ответ, который не соответствует поставленному вопросу. Студент демонстрирует существенные пробелы в знаниях и недостаточный уровень навыков при решении практических задач. В ответе допускаются существенные ошибки.
	Отмечается присутствие студента на занятиях. За каждое посещение прибавляется 0,4 балла. Максимальное количество баллов за равно 25,6	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
	1. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и системное ПО сервера. 2. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и системное ПО клиентов. 3. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на системное ПО сервера и СУБД. 4. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на СУБД и прикладное ПО клиентов. 5. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на СУБД и прикладное ПО сервера. 6. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на СУБД и системное и прикладное ПО клиентов. 7. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на гипервизор и ОС. 8. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и ОС клиента. 9. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и ОС сервера. 10. Опишите процедуру разработки и примерное содержимое политики использования

	ресурсов интранета торговой организации 11. Опишите процедуру разработки и примерное содержимое политики в отношении паролей клиентов банка. 12. Опишите процедуру разработки и примерное содержимое политики шифрования для долговременного хранения резервных копий баз данных о клиентах интернет-провайдера на «облачном» хостинге. 13. Опишите процедуру разработки и примерное содержимое антивирусной политики для информационных стендов самообслуживания в торговом зале магазина. 14. Опишите процедуру разработки и примерное содержимое политики оценки рисков для малой АСУ ТП управления скважиной. 15. Опишите процедуру разработки и примерное содержимое политики аудита для информационной системы вуза. 16. Опишите процедуру разработки и примерное содержимое политики для пограничных маршрутизаторов ЦОД. 17. Опишите процедуру разработки и примерное содержимое политики удаленного доступа к информационным ресурсам корпоративной сети для менеджмента авиакомпании. 18. Опишите процедуру разработки и примерное содержимое политики построения виртуальных частных сетей для организации, использующей вычислительные мощности у нескольких «облачных» поставщиков. 19. Опишите процедуру разработки и примерное содержимое политики для экстранета акционерного общества, в части предоставления обязательной к распространению информации. 20. Опишите процедуру разработки и примерное содержимое политики для оборудования пограничной демилитаризованной зоны туроператорора с поддержкой интернет-продаж. 21. Опишите процедуру разработки и примерное содержимое политики для подключения подразделений МВД к интранету главного управления. 22. Опишите процедуру разработки и примерное содержимое политики подключения к интранету с применением модема для удалённой одиночной метеостанции. 23. Опишите процедуру разработки и примерное содержимое политики для конфиденциальной информации, обрабатываемой в бюро кредитных историй. 24. Опишите процедуру разработки и примерное содержимое политики для веб-сервера, участвующего в структуре CDN распространения статического контента, в качестве регионального КЭШа. 25. Опишите процедуру разработки и примерное содержимое политики для веб-сервера, участвующего в структуре CDN распространения потокового контента, в качестве сервера первичного распространения. 26. Опишите процедуру разработки и примерное содержимое политики автоматизированной маршрутизации электронной почты внутри производственной организации. 27. Опишите процедуру разработки и примерное содержимое политики архивного хранения электронной почты для транспортной компании 28. Опишите процедуру разработки и примерное содержимое политики для межсетевого экранирования для ЦОД с резервируемыми подключениями. 29. Опишите процедуру разработки и примерное содержимое политики специального доступа для кадастровой организации. 30. Опишите процедуру разработки и примерное содержимое политики подключения новых устройств в интранет склада. тесты.docx
	1. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и системное ПО сервера. 2. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и системное ПО клиентов. 3. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на системное ПО сервера и СУБД.

	4. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на СУБД и прикладное ПО клиентов. 5. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на СУБД и прикладное ПО сервера. 6. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на СУБД и системное и прикладное ПО клиентов. 7. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на гипервизор и ОС. 8. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и ОС клиента. 9. Рассчитайте риски, вызванные взаимным влиянием уязвимостей, влияющих на сетевое оборудование и ОС сервера. 10. Опишите процедуру разработки и примерное содержимое политики использования ресурсов интранета торговой организации 11. Опишите процедуру разработки и примерное содержимое политики в отношении паролей клиентов банка. 12. Опишите процедуру разработки и примерное содержимое политики шифрования для долговременного хранения резервных копий баз данных о клиентах интернет-провайдера на «облачном» хостинге. 13. Опишите процедуру разработки и примерное содержимое антивирусной политики для информационных стендов самообслуживания в торговом зале магазина. 14. Опишите процедуру разработки и примерное содержимое политики оценки рисков для малой АСУ ТП управления скважиной. 15. Опишите процедуру разработки и примерное содержимое политики аудита для информационной системы вуза. 16. Опишите процедуру разработки и примерное содержимое политики для пограничных маршрутизаторов ЦОД. 17. Опишите процедуру разработки и примерное содержимое политики удаленного доступа к информационным ресурсам корпоративной сети для менеджмента авиакомпании. 18. Опишите процедуру разработки и примерное содержимое политики построения виртуальных частных сетей для организации, использующей вычислительные мощности у нескольких «облачных» поставщиков. 19. Опишите процедуру разработки и примерное содержимое политики для экстранета акционерного общества, в части предоставления обязательной к распространению информации. 20. Опишите процедуру разработки и примерное содержимое политики для оборудования пограничной демилитаризованной зоны туроператорора с поддержкой интернет-продаж. 21. Опишите процедуру разработки и примерное содержимое политики для подключения подразделений МВД к интранету главного управления. 22. Опишите процедуру разработки и примерное содержимое политики подключения к интранету с применением модема для удалённой одиночной метеостанции. 23. Опишите процедуру разработки и примерное содержимое политики для конфиденциальной информации, обрабатываемой в бюро кредитных историй. 24. Опишите процедуру разработки и примерное содержимое политики для веб-сервера, участвующего в структуре CDN распространения статического контента, в качестве регионального КЭШа. 25. Опишите процедуру разработки и примерное содержимое политики для веб-сервера, участвующего в структуре CDN распространения потокового контента, в качестве сервера первичного распространения. 26. Опишите процедуру разработки и примерное содержимое политики автоматизированной маршрутизации электронной почты внутри производственной организации. 27. Опишите процедуру разработки и примерное содержимое политики архивного хранения электронной почты для транспортной компании

	28. Опишите процедуру разработки и примерное содержимое политики для межсетевого экранирования для ЦОД с резервируемыми подключениями. 29. Опишите процедуру разработки и примерное содержимое политики специального доступа для кадастровой организации. 30. Опишите процедуру разработки и примерное содержимое политики подключения новых устройств в интранет склада.
	Темы курсовых работ: Характеристика ГОСТ Р ИСО/МЭК серии 7498 Архитектура безопасности ИТС Общие концепции и средства обеспечения информационной безопасности Аутентификация: общая характеристика, способы и их свойства Парольная аутентификация Биометрическая аутентификация Аутентификация с помощью одноразовых паролей Аутентификация с помощью криптографии с открытым ключом Протоколы аутентификации в локальной сети Механизмы аутентификации при осуществлении подключений Аутентификация в защищенных соединениях Аппаратные средства аутентификации Обеспечение аутентификации на основе рекомендаций и продуктов MICROSOFT Обеспечение аутентификации на основе рекомендаций и продуктов ORACLE И ALADDIN. Обеспечение аутентификации на основе рекомендаций и продуктов CITRIX SYSTEMS Российский рынок средств аутентификации Управления доступом: общая характеристика, политики и средства Дискреционное управление доступом Модели изолированной программной среды Мандатное управлением доступом Модели безопасности информационных потоков Ролевое управлением доступом Управление доступом в ЭМВОС и Интернет-архитектуре Неотказуемость: общая характеристика, политики и средства обеспечения Неотказуемость: способы обеспечения Конфиденциальность: общая характеристика, политики и средства Конфиденциальность: способы обеспечения Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре Целостность: общая характеристика, политики и средства обеспечения Целостность: способы обеспечения Обеспечение целостности в ЭМВОС и Интернет-архитектуре Аудит безопасности открытых систем и оповещение об опасности: способы и средства Обеспечение ключами: общая и концептуальные модели, классы прикладных криптографических систем, жизненный цикл Атаки по уровням иерархической системы OSI: сравнительная характеристика, способы и средства защиты Атаки на беспроводные устройства (Wi-Fi, Bluetoth и др.) и защита от них Атаки в виртуальной среде. Характеристика и средства защиты Облачные технологии и безопасность облачных систем Средства обнаружения и предотвращения вторжений Средства предотвращения утечек Межсетевое экранирование Антивирусная защита открытой информационной системы Информационная безопасность IoT Информационная безопасность мобильных систем Информационная безопасность IP-телефонии:

	Информационная безопасность электронной почты Информационная безопасность WWW Информационная безопасность DNS Анализ удаленных сетевых служб Социально-инженерные атаки и защита от них Работа с пользователями защищаемой информационной системы Классические и современные методы, используемые нападающими для проникновения в открытые информационные системы Классические и современные методы, используемые для защиты от проникновений в открытые информационные системы Документационное обеспечение ИБОС
	1. Протокол Syslog. Особенности сбора событий в ОС Unix и Windows. 2. Протокол SNMP. Архитектура, виды запросов. 3. Инициатива WBEM. Область применения. Преимущества. 4. Назначение, технологии и классификация VPN. 5. Назначение и особенности виртуальных устройств tun/tap. 6. Протокол PPP. Особенности инкапсуляции. Поддержка шифрования и аутентификации. 7. Протокол PPTP. Архитектура и особенности реализации. 8. Протокол IPSec. Режимы работы. Процесс установления сессий. 9. НазначениеNAT. Классификация. Адаптация NAT для приложений(ALG). Автонастройка NAT(Upnp, NAT-PMP). 10. Протоколы обхода NAT(STUN, TURN). Инфраструктура ICE. Особенности обработки пакетов (Hairpin, Random port). 11. Прокси-серверы. Классификация. Схемы внедрения. Использование GRE для реализации прямого прозрачного Proxy. 12. Проксификаторы. Протокол SOCKS. Назначение, реализация. 13. Протоколы автообнаружения Proxy.(WPAD, WCCP) 14. Межсетевые экраны. Классификация, назначение. Особенности реализации. 15. Понятие узла бастиона, DMZ их назначение. Основные топологии построения DMZ. Понятие сетевого периметра. 16. Проблемы контроля доступа и аутентификации в локальных сетях. Стандарт 802.1x. Протокол EAP. 17. Протокол TACACS. Цели, режимы работы, архитектура. 18. Модификации протокола TACACS. Их соответствие концепции AAA. 19. Концепция AAA. Цели и задачи. 20. Протокол RADIUS. 21. Протокол DIAMETR. 22. Протоколы STP и RSTP. 23. Алгоритм шифрования RC4. 24. Алгоритм Michael. Формирование MIC. 25. Стандарт формирования ключа PBKDF2. Использование в WPA, параметры. 26. Блочные и потоковые шифры. Применимость к беспроводным технологиям. 27. Протокол CCMP. Формат кадра. Процесс формирования и обработки кадра. 28. Алгоритм подписи HMAC-MD5. 29. Алгоритм подписи HMAC-SHA1.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. 1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"
2. 2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн
3. 3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"
4. 4. Безопасность информационных технологий ,12+ ,М-во образования и науки Рос. Федерации, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ
5. 5. Вестник УрФО : Безопасность в информационной сфере ,Юж.-Урал. гос. ун-т; ЮУрГУ
6. 6. Информационные ресурсы России
7. 7. Информационное общество
8. 8. Информационное право
9. 9. Информационные процессы и системы
10. 10. Управление риском

г) методические указания для студентов по освоению дисциплины:

1. ИБОС_Лекционный материал
2. ИБОС_Лекционный материал
3. Астахова Л.В. Методическое пособие по курсу ИБОС

из них: учебно-методическое обеспечение самостоятельной работы студента:

4. ИБОС_Лекционный материал
5. ИБОС_Лекционный материал
6. Астахова Л.В. Методическое пособие по курсу ИБОС

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Мельников, Д.А. Информационная безопасность открытых систем. [Электронный ресурс] — Электрон. дан. — М. : ФЛИНТА, 2014. — 448 с. — Режим доступа: http://e.lanbook.com/book/48368 — Загл. с экрана	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев [и др.] ; под ред. А.А.Шелупанова, С.Л.Груздева, Ю.С.Нахаева. — Электрон.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

		дан. — Москва : Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: https://e.lanbook.com/book/5114. — Загл. с экрана.		
3	Основная литература	Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие / П.Н. Девянин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049. — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
4	Основная литература	Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 2-е изд. — Москва : МГТУ им. Н.Э. Баумана, 2018. — 250 с. — ISBN 978-5-7038-4899-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172839 (дата обращения: 20.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
5	Основная литература	Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
6	Дополнительная литература	Ворона, В.А. Системы контроля и управления доступом [Электронный ресурс] / В.А. Ворона, В.А. Тихонов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2018. — 272 с. — Режим доступа: https://e.lanbook.com/book/111037. — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. -Python(бессрочно)
4. -IDA pro free(бессрочно)

Перечень используемых информационных справочных систем:

1. -База данных polpred (обзор СМИ)(бессрочно)
2. ООО "ГарантУралСервис"-Гарант(бессрочно)

3. -Стандартинформ(бессрочно)
4. -База данных ВИНИТИ РАН(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox,.
Лабораторные занятия	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2