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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профили) подготовки:
Организация и технология защиты информации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Информационная безопасность автоматизированных систем
Рабочая программа дисциплины
Составитель:
Кандидат военных наук, доцент. кафедры КЗИ Д.Н. Баранников

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем (АС); навыков организации работы по оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.
Задачи дисциплины:
– рассмотрение понятийного базиса в области обеспечения информационной безопасности автоматизированных систем, классов и типовых моделей автоматизированных систем;
– рассмотрение причин нарушения безопасности систем, существа проблемы обеспечения информационной безопасности, концептуальной модели безопасности, формирования требований к безопасности;
– изучение основных механизмов обеспечения информационной безопасности систем;
– изучение безопасного доступа к информационным ресурсам, формирование доверенных сред.

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	*ОПК-2.1.1 Знает принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя*	*Знать:* • *принципы построения систем защиты информации;* • *критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем;* • *основные угрозы безопасности информации и модели нарушителя*
	ОПК-2.1.2 Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей	*Уметь:* • *анализировать угрозы безопасности информации* • *применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации с целью выявления уязвимостей*
	ОПК-2.1.3 Владеет навыками расчёта показателей эффективности защиты информации, обра-	*Владеть:* • *навыками расчётов показателей эффективности защиты информации, об-*

	батываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации	*рабатываемой в автоматизированных системах* • *проведением анализа уязвимости программного и программно-аппаратных средств защиты информации*
ПК-13 *Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации*	*ПК-13.1* *Знает 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*	*Знать:* • *процедуру организации установки и настройки технических, программных средств защиты информации* • *способы настройки сетевого оборудования*
	ПК-13.2 *Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации*	*Уметь:* • *навыками организации и сопровождения аттестации объектов вычислительной техники выделенных помещений на соответствии требованиям по защите информации*
	ПК-13.3 *Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации*	*Владеть:* • *навыками разработки и реализации организационных мер, обеспечивающих эффективность системы защиты информации*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность автоматизированных систем» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Защита информации от несанкционированного доступа», «Инфраструктура открытых ключей, удостоверяющие центры», «Программно-аппаратные средства защиты информации», «Системы электронного документооборота», «Безопасность операционных систем и программного обеспечения».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Системы управления информационной безопасностью», «Комплексная защита объектов информатизации. Управление службой защиты информации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация _ _ ч., самостоятельная работа обучающихся _36_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Введение в информационную безопасность автоматизированных систем*	**7**	**2**					**4**	Опрос.
2	*Организационно-правовые основы обеспечения информационной безопасности автоматизированных систем*	**7**	**2**					**4**	Опрос.
3	*Обеспечение безопасности автоматизированных систем*	**7**	**2**		**4**			**4**	Опрос. Оценка выполнения практических заданий
4	*Средства защиты информации от НСД*	**7**	**2**		**4**			**6**	Опрос. Оценка выполнения практических заданий
5	*Обеспечение безопасности компьютерных сетей*	**7**	**2**		**4**			**6**	Опрос. Оценка выполнения практических заданий
6	*Основы технологии виртуальных защищённых сетей VPN*	**7**	**2**		**6**			**6**	Опрос. Оценка выполнения практических заданий
7	*Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты веб-порталов*	**7**	**4**		**6**			**6**	Опрос. Оценка выполнения практических заданий
8	*зачёт*	**7**							*Зачёт по билетам*
9	итого:		**16**		**24**			**36**	

3. Содержание дисциплины

Тема 1. Введение в информационную безопасность автоматизированных систем

Актуальность проблемы защиты АС в современных условиях. Факторы, её определяющие. Защита АС как процесс управления рисками. Анализ рисков. Основные подходы к анализу рисков. Этапы анализа рисков и управления ими.
Методы оценки целесообразности затрат на обеспечение ИБ. Виды затрат на обеспечение ИБ. Особенности современных АС как объектов защиты.
Основные понятия в ИБ АС. Безопасность информации. Информация и её свойства. Цель защиты АС и циркулирующей в ней информации.
Угрозы безопасности АС. Основные структурно-функциональные элементы АС. Типы угроз безопасности. Несанкционированный доступ и несанкционированное воздействие на информацию.
Основные источники угроз безопасности АС. Классификация угроз по источнику возникновения. Критерии классификации и классификация каналов проникновения в АС и утечки информации. Неформальная модель нарушителя. Критерии классификации и классификация нарушителей.**Тема 2. Организационно-правовые основы обеспечения информационной безопасности автоматизированных систем**

Виды мер противодействия угрозам безопасности, их взаимосвязь, достоинства и недостатки. Принципы построения системы обеспечения безопасности информации в АС. Стратегия развития информационного общества в Российской Федерации, утверждённой Президентом РФ от 07.02.2008 № Пр-212. Стратегии национальной безопасности Российской Федерации до 2020 года. Нормативно-методические документы ФСТЭК России по обеспечению безопасности информации. Виды информации по федеральному закону «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
Понятие лицензии и лицензирования. Виды деятельности в области защиты информации, подлежащих лицензированию. Сертификация средств защиты информации и аттестация объектов информатизации. Термины и определения. Нормативно-правовые акты в области защиты информации от несанкционированного доступа. Классы защиты средств вычислительной техники, АС, межсетевых экранов. Недекларированные возможности. Классификация программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей.

Тема 3. Обеспечение безопасности автоматизированных систем

Организационная структура системы обеспечения безопасности АС. Технология управления безопасностью (обеспечения безопасности) информации и ресурсов в АС. Требования к технологии управления безопасностью. Мероприятия при реализации технологии управления безопасностью. Институт ответственных за обеспечение информационной безопасности. Влияние на безопасность ИТ разных субъектов организации ИБ. Цели регламентации действий пользователей и обслуживающего персонала АС. Составляющие эффективного функционирования системы безопасности ИТ. Политика безопасности организации в области ИТ, её цель, условия осуществления и проблемы. Уровни зрелости (в сфере обеспечения ИБ). Виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты. Распределение функций по обеспечению безопасности АС. Организационно-распорядительные документы по обеспечению безопасности АС. Обязанности пользователей и ответственных за обеспечение ИБ в подразделениях. Проблема человеческого фактора. Общие правила обеспечения безопасности. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности. Порядок работы с носителями ключевой информации.

Явная и неявная компрометация ключей. Признаки и действия при компрометации ключей. Регламентация правил парольной и антивирусной защиты. Регламентация порядка допуска к работе и изменения полномочий пользователей АС. Регламентация порядка изменения конфигурации аппаратно-программных средств АС.

Тема 4. Средства защиты информации от НСД

Основные механизмы защиты автоматизированных систем от НСД. Сущность и назначение идентификации и аутентификации пользователей. Виды и способы аутентификации. Разграничение доступа пользователей к ресурсам АС. Диспетчер доступа. Сущность избирательного и полномочного разграничения доступа. Замкнутая программная среда. Регистрация и оперативное оповещение о событиях безопасности. Криптографические методы защиты информации. Криптография с симметричными и открытыми ключами. Электронная цифровая подпись. Реализация ЭЦП. Принципы комбинированного шифрования. Доверие к открытому ключу и цифровые сертификаты. Система обнаружения атак. Защита периметра компьютерных сетей и управление механизмами защиты.
Аппаратно-программные средства защиты информации от НСД. Рекомендации по выбору СЗИ НСД. Виды биометрической идентификации, преимущества и недостатки.
Применение штатных и дополнительных СЗИ НСД. Стратегия безопасности компании Microsoft. Защита от вмешательства в процесс нормального функционирования АС. Встроенные механизмы разграничения доступа на примере ОС Windows. Уровни доверия механизм целостности. Оперативное оповещение о зарегистрированных попытках НСД. Службы ACS. Система защиты информации от НСД Secret Net 6. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования

Тема 5. Обеспечение безопасности компьютерных сетей

Проблемы обеспечения безопасности в компьютерных сетях.
Уровни информационной инфраструктуры корпоративной сети. Уязвимости и их классификация. Типы уязвимости с точки зрения технических особенностей. Классификация уязвимостей по степени риска. Получение информации по уязвимостям. «Стандартные» обозначения уязвимостей. Классификация атак.
Защита периметра корпоративной сети.
Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны их виды. Демилитаризованная зона. Анализ содержимого почтового и веб-трафика. Виртуальные частные сети.
Управление уязвимостями. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Средства анализа защищённости системного уровня. Мониторинг событий безопасности. Категории журналов событий. Инфраструктура управления журналами событий. Особенности защищённости электронного документооборота.

Тема 6. Основы технологии виртуальных защищённых сетей VPN

Концепция построения виртуальных частных сетей – VPN. Основные понятия и функции сети VPN. Защита информации в процессе её передачи по туннелю VPN. VPN-клиент, VPN-сервер и шлюз безопасности VPN. Реализация механизма VPN. Варианты построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN. Критерии безопасности данных применительно к задачам VPN. VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации. Основные варианты архитектуры VPN. Достоинства применения технологий VPN.

Тема 7. Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты веб-порталов

Протоколы формирования защищённых каналов на канальном уровне. Протокол PPTP. Структура пакета. Протокол L2TP, его преимущества. Формирование защищённого виртуального канала в протоколе L2TP. Протоколы формирования защищённых каналов на

сеансовом уровне. Процедура установления *SSL*-сессии. Недостатки протоколов *SSL* и *TLS.* Протокол *SOCKS,* его особенности. Схема установления соединения по протоколу *SOCKS* v5. Защита беспроводных сетей. Протоколы WEP, TKIP, WPA и WPA2.
Защита на канальном, сеансовом и сетевом уровнях. Архитектура средств безопасности IPSec. Компоненты реализаций протокола IPSec имеют следующие. Архитектура стека протоколов IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол аутентифицирующего заголовка. Применение протокола AH в транспортном и туннельном режимах. Протокол инкапсулирующей защиты, применение протокола ESP в транспортном и туннельном режимах. Алгоритмы аутентификации и шифрования в IPSec. Структура алгоритма HMAC. Протокол управления криптоключами IKE. Задачи, решаемые протоколами IKE. Установление безопасной ассоциации. Базы данных SAD и SPD. Основные схемы применения IPSec. Практические аспекты защиты веб-порталов от информационных атак. Типовая архитектура веб-портала. подсистемы антивирусной защиты, контроля целостности, разграничения доступа, обнаружения вторжений, анализа защищённости, криптографической защиты информации, подсистему управления защитой веб-порталов..

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	*Введение в информационную безопасность автоматизированных систем*	*Лекция 1.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
2	*Организационно-правовые основы обеспечения информационной безопасности автоматизированных систем*	*Лекция 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
3	*Обеспечение безопасности автоматизированных систем*	*Лекция 3.* *Практическое занятие 1* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение задания* *Подготовка к занятиям с использованием ЭБС*
4	*Средства защиты информации от НСД*	*Лекция 4.* *Практическое занятие 2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение задания* *Подготовка к занятиям с использованием ЭБС*
5	*Обеспечение безопасности компьютерных сетей*	*Лекция 5.* *Практическое занятие 3*	*Традиционная лекция с использованием презентаций* *Выполнение задания*

		Самостоятельная работа	*Подготовка к занятиям с использованием ЭБС*
6	*Основы технологии виртуальных защищённых сетей VPN*	*Лекция 6.* *Практическое занятие 4* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение задания* *Подготовка к занятиям с использованием ЭБС*
7	*Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты веб-порталов*	*Лекция 7* *Практическое занятие 5* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение задания* *Подготовка к занятиям с использованием ЭБС*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-3)* *– опрос (темы 4-7)* *– практические занятия 1-5*	 *5 баллов* *5 баллов* *6 баллов*	 *15 баллов* *20 баллов* *30 баллов*
Промежуточная аттестация *зачет*		*35 баллов*
Итого за дисциплину *зачет*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 7	ОПК-2, ПК-13	Опрос
2.	Практические занятия 1 – 5	ОПК-2, ПК-13	План практического занятия

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 шкала	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/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	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»/ «зачтено (хорошо)»/ «зачтено»	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 выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		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 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	Реализуемая компетенция
1.	Критерии классификации и классификация нарушителей.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
2.	Основные понятия в ИБ АС.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
3.	Цель защиты АС и циркулирующей в ней информации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
4.	Классификация угроз по источнику возникновения.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
5.	Этапы анализа рисков и управления ими.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
6.	Виды мер противодействия угрозам безопасности, их взаимосвязь, достоинства и недостатки	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
7.	Виды информации по федеральному закону «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
8.	Понятие лицензии и лицензирования.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
9.	Виды деятельности в области защиты инфор-	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3;

	мации, подлежащих лицензированию.	ПК-13.1; ПК-13.2; ПК-13.3
10.	Классы защиты средств вычислительной техники, АС, межсетевых экранов.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
11.	Недекларированные возможности.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
12.	Классификация программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
13.	Организационная структура системы обеспечения безопасности АС.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
14.	Технология управления безопасностью (обеспечения безопасности) информации и ресурсов в АС.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
15.	Влияние на безопасность ИТ разных субъектов организации ИБ.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
16.	Порядок работы с носителями ключевой информации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
17.	Явная и неявная компрометация ключей.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
18.	Признаки и действия при компрометации ключей.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
19.	Регламентация правил парольной и антивирусной защиты.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
20.	Основные механизмы защиты автоматизированных систем от НСД.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
21.	Виды и способы аутентификации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
22.	Разграничение доступа пользователей к ресурсам АС. Диспетчер доступа.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
23.	Сущность избирательного и полномочного разграничения доступа.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
24.	Замкнутая программная среда.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
25.	Применение штатных и дополнительных СЗИ НСД.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
26.	Уязвимости и их классификация.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
27.	Классификация атак.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
28.	Защита периметра корпоративной сети.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
29.	Демилитаризованная зона.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
30.	Виртуальные частные сети.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
31.	Особенности сетевых агентов сканирования.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
32.	Мониторинг событий безопасности.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
33.	Категории журналов событий. Инфраструктура управления журналами событий.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3

34.	Особенности защищённости электронного документооборота	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
35.	VPN-клиент, VPN-сервер и шлюз безопасности VPN.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
36.	Классификация сетей VPN.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
37.	Основные варианты архитектуры VPN.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
38.	Протокол PPTP. Структура пакета.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
39.	Протокол L2TP, его преимущества.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
40.	Недостатки протоколов *SSL* и *TLS.*	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
41.	Протокол *SOCKS,* его особенности.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
42.	Защита беспроводных сетей. Протоколы WEP, TKIP, WPA и WPA2.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
43.	Архитектура стека протоколов IPSec.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3

Промежуточная аттестация (примерные вопросы к зачету) – проверка сформированности компетенций – ОПК-2.1, ПК-13

№	Вопрос	Реализуемая компетенция
1.	Актуальность проблемы защиты АС в современных условиях.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
2.	Защита АС как процесс управления рисками.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
3.	Методы оценки целесообразности затрат на обеспечение ИБ.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
4.	Информация и её свойства. Цель защиты АС и циркулирующей в ней информации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
5.	Основные структурно-функциональные элементы АС.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
6.	Типы угроз безопасности. Несанкционированный доступ и несанкционированное воздействие на информацию.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
7.	Основные источники угроз безопасности АС. Классификация угроз по источнику возникновения.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
8.	Критерии классификации и классификация каналов проникновения в АС и утечки информации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
9.	Неформальная модель нарушителя. Критерии классификации и классификация нарушителей.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
10.	Виды мер противодействия угрозам безопасности, их взаимосвязь, достоинства и недостатки.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
11.	Принципы построения системы обеспечения безопасности информации в АС.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
12.	Понятие лицензии и лицензирования. Виды деятельности в области защиты информации,	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3

	подлежащих лицензированию. Сертификация средств защиты информации и аттестация объектов информатизации.	
13.	Нормативно-правовые акты в области защиты информации от несанкционированного доступа. Классы защиты средств вычислительной техники, АС, межсетевых экранов.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
14.	Недекларированные возможности. Классификация программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
15.	Организационная структура системы обеспечения безопасности АС. Институт ответственных за обеспечение информационной безопасности. Влияние на безопасность ИТ разных субъектов организации ИБ.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
16.	Цели регламентации действий пользователей и обслуживающего персонала АС. Составляющие эффективного функционирования системы безопасности ИТ.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
17.	Политика безопасности организации в области ИТ, её цель, условия осуществления и проблемы. Уровни зрелости (в сфере обеспечения ИБ.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
18.	Обязанности пользователей и ответственных за обеспечение ИБ в подразделениях. Проблема человеческого фактора.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
19.	Порядок работы с носителями ключевой информации. Явная и неявная компрометация ключей.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
20.	Регламентация правил парольной и антивирусной защиты, порядка допуска к работе и изменения полномочий пользователей АС, порядка изменения конфигурации аппаратно-программных средств АС.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
21.	Основные механизмы защиты автоматизированных систем от НСД. аутентификации. Разграничение доступа.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
22.	Криптографические методы защиты информации. Электронная цифровая подпись. Реализация ЭЦП. Принципы комбинированного шифрования.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
23.	Доверие к открытому ключу и цифровые сертификаты. Система обнаружения атак.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
24.	Защита периметра компьютерных сетей и управление механизмами защиты.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
25.	Аппаратно-программные средства защиты информации от НСД. Виды биометрической идентификации, преимущества и недостатки.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
26.	Применение штатных и дополнительных СЗИ НСД.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
27.	Уровни информационной инфраструктуры корпоративной сети. Уязвимости и их классифика-	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3

	ция. Классификация атак.	
28.	Защита периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
29.	Управление уязвимостями. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
30.	Средства анализа защищённости системного уровня. Мониторинг событий безопасности.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
31.	Системы обнаружения атак. Классификация систем обнаружения атак.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
32.	Концепция построения виртуальных частных сетей – VPN.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
33.	Варианты построения виртуальных защищённых каналов.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
34.	Средства обеспечения безопасности VPN.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
35.	VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
36.	Основные варианты архитектуры VPN. Достоинства применения технологий VPN.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
37.	Протоколы формирования защищённых каналов на канальном уровне	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
38.	Протоколы формирования защищённых каналов на сеансовом уровне	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
39.	Защита беспроводных сетей	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
40.	Архитектура средств безопасности IPSec	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
41.	Защита передаваемых данных с помощью протоколов AH и ESP	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
42.	Протокол управления криптоключами IKE	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
43.	Особенности реализации средств IPSec	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
44.	Защита веб-порталов от информационных атак	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3

Промежуточная аттестация (примерные практические задания к экзамену) – проверка сформированности компетенций – ОПК-2.1; ПК-13

1.	Разработать для предложенной фирмы виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплекс-ной системы защиты.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
2.	Составить матрицу разделения доступа к ресурсам для предложенной фирмы.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
3.	Разработать систему защиты периметра сети	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3;

	организации.	ПК-13.1; ПК-13.2; ПК-13.3
4.	Разработать систему VPN для организации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3
5.	Сформировать в симуляторе Cisco Packet Tracer по заданной топологии сеть (задать адреса узлов шлюзов)	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ПК-13.1; ПК-13.2; ПК-13.3

Примерные тестовые задания проверка сформированности компетенций – ОПК-2.1, ПК-13

1. Выберите типы агентов сканирования, классифицированных по расположению относительно объекта сканирования:

а) сетевые

б) локальные

в) пассивные

г) активные

д) межсегментные

2. Диспетчер доступа – это:

а) средство, выступающее в роли посредника-контролёра при обращении субъектов доступа к объектам доступа

б) средство, осуществляющее мандатный доступ субъектов доступа к объектам доступа

в) средство, осуществляющее дискреционный доступ субъектов доступа к объектам доступа

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

1. *Руководящий документ.* Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс], Режим доступа: https://fstec.ru/component/attachments/download/296: свободный. – Загл. с экрана.
2. *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. свободный. – Загл. с экрана.
3. *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/component/attachments/download/297, свободный. – Загл. с экрана.

Дополнительная

1. *Уголовный кодекс Российской Федерации* от 13.06.1996 № 63-ФЗ (ред. от 03.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_10699/, свободный. – Загл. с экрана.

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

1. ОХРАНА.ru. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : https://oxpaha.ru/, свободный. – Загл. с экрана.
2. 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

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

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

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. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR 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.
– 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 – проверка сформированности компетенций – ОПК-2.1, ПК-13

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля за подготовкой 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 лабораторных работ, 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 (4 ч.) – проверка сформированности компетенций – ПК-13, ОПК – 2.1
Задания:
1. Разработать для предложенной фирмы виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты.

Указания по выполнению заданий:
1. Изучить теоретические материалы.
2. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Список литературы:
1. *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.znanium.com/catalog/product/996789 (дата обращения: 11.08.2019)

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой ОС Microsoft Office 2010, Windows 10 Pro

Практическое занятие 2 (4 ч.) – проверка сформированности компетенций – ПК-13, ОПК-2.1
Задания:
1. Составить матрицу разделения доступа к ресурсам для предложенной фирмы.
2. Выполнить мандатное разграничение доступа к ресурсам.

3. Выбрать модель разграничения доступа.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Список литературы:

1. *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.znanium.com/catalog/product/996789 (дата обращения: 11.08.2019)
2. *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.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Microsoft Office 2010, Windows 10 Pro.

Практическое занятие 3 (4 ч.) – проверка сформированности компетенций – ПК-13, ОПК – 2.1

Задания:

1. Разработать систему защиты периметра сети организации.
2. Спроектировать демилитаризованную зону с указанием оборудования вынесенного в ДМЗ.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Список литературы:

1. *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.znanium.com/catalog/product/996789 (дата обращения: 11.08.2019)

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Microsoft Office 2010, Windows 10 Pro..

Практическое занятие 4 (6 ч.) – проверка сформированности компетенций – ПК-13, ОПК – 2.1

Задания:

1. Разработать систему VPN для организации.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Список литературы:

1. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
2. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

Материально-техническое обеспечение занятия:

1. Компьютеры с выходом в интернет с ОС Microsoft Office 2010, Windows 10 Pro.

Практическое занятие 5 (6 ч.) – проверка сформированности компетенций – ПК-13, ОПК – 2.1

Задания:

1. Сформировать в симуляторе *Cisco Packet Tracer* по заданной топологии сеть (задать адреса узлов шлюзов)
2. Создать безопасный удалённый доступ (SSH) к указанному узлу.
3. Изучить прохождение пакетов, оформить отчёт.
4. Ответить на контрольные вопросы

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Преподаватель выдаёт каждому студенту адресное пространство сети класса С.

Список литературы:

1. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
2. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

Материально-техническое обеспечение занятия:

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

Результаты практических заданий обучающиеся оформляют в виде отчётов. Отчёт оформляется с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённого способа связи.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность автоматизированных систем» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки Организация и технология защиты информации) кафедрой комплексной защиты информации.

Цель дисциплины: формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.
Задачи: рассмотрение понятийного базиса в области обеспечения информационной безопасности автоматизированных систем, классов и типовых моделей автоматизированных систем; причин нарушения безопасности систем, существо проблемы обеспечения информационной безопасности, концептуальную модель безопасности, формирование требований к безопасности, основные механизмы обеспечения информационной безопасности систем; безопасный доступ к информационным ресурсам, формирование доверенных сред.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-2.1 - Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью вы-явления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба
    - ОПК-2.1.1 - Знает принципы построения систем защиты информации; критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя
    - ОПК-2.1.2 - Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей
    - ОПК-2.1.3 - Владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации
- ПК-13 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации;
    - ПК-13.1 – Знает процедуру организации установки и настройки технических, программных (программ-но-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации;
    - ПК-13.2 - Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации;
    - ПК-13.3 - Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

В результате освоения дисциплины обучающийся должен:

Знать методологические и технологические основы комплексного обеспечения безопасности АС; угрозы и методы нарушения безопасности АС; формальные модели, лежащие в основе систем защиты АС; стандарты по оценке защищённости АС и их теоретические основы; методы и средства реализации, защищённых АС; методы и средства верификации и анализа надёжности, защищённых АС.

Уметь проводить анализ АС с точки зрения обеспечения компьютерной безопасности; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы; применять стандарты по оценке защищённости АС при анализе систем защиты информации в АС; реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищённости АС.

Владеть навыками работы с АС распределённых вычислений и обработки информации; навыками работы с документацией АС; приёмами использования критериев оценки защищённости АС; приёмами построения формальных моделей систем защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 2 зачётных единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Информационная безопасность автоматизированных систем

по направлению подготовки 10.03.01 Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата