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 ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

Информационная безопасность телекоммуникационных систем
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

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 знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.
Задачи дисциплины:
– овладение методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
– формирование навыков анализа информационной инфраструктуры информационных систем и ее безопасности.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.2 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	*ОПК-4.2.1 Знает средства, методы и протоколы идентификации, аутентификации и авторизации*	*Знать: методики, обработку, принципы ААА, оценку достоверности результатов тестирования разных протоколов идентификазии/аутентификации.*
	ОПК-4.2.2 Умеет устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	*Уметь: проводить эксперименты и оценивать результаты тестирования. исследовать средства защиты информации, уметь оценивать по функциональным возможностям, надежности функционирования, эффективности обнаружения попыток НСД в телекоммуникационных системах*
	ОПК-4.2.3 Владеет навыками управления полномочиями пользователей	*Владеть: навыками проводить эксперименты по заданной методике; навыки работы с дискреционной и мандатной политиками доступа в телекоммуникационных системах.*
ПК-3 Способен управлять защитой информации в автоматизированных системах	*ПК-3.1 Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в*	*Знать: основные методы управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК РФ*

	автоматизированных системах	
	ПК-3.2 *Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах*	*Уметь: классифицировать угрозы, разрабатывать технические предложения по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с целью оценки рисков*
	ПК-3.3 *Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе*	*Владеть: навыками по разработке организационно-технических по защите информации, приемы и принципы в соответствие с ЕСКД, ЕСПД и другими нормативно-правовым документами*

1.3. Место дисциплины в структуре образовательной программы

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

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Аппаратные средства вычислительной техники», «Безопасность операционных систем», «Сети и системы передачи информации», «Информационные технологии. Администрирование подсистем защиты информации», «Программно-аппаратные средства защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Защита информации от вредоносного программного обеспечения», «Безопасность вычислительных сетей», «Преддипломная практика».

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., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Основные понятия, концепции и принципы информационной безопасности*	**8**	**2**					**4**	Опрос.
2	*Технологии аутентификации, авторизации и управления доступом*	**8**	**2**		**4**			**4**	Оценка выполнения практических заданий
3	*Технологии безопасности на основе фильтрации и мониторинга трафика*	**8**	**2**		**4**			**6**	Оценка выполнения практических заданий
4	*Атаки на транспортную инфраструктуру сети*	**8**	**4**		**4**			**6**	Оценка выполнения практических заданий
5	*Уязвимость программного кода.*	**8**	**2**		**4**			**6**	Оценка выполнения практических заданий
6	*Безопасность программного кода.*	**8**	**2**		**4**			**6**	Оценка выполнения практических заданий
7	*Безопасность сетевых служб*	**8**	**2**		**2**			**4**	Оценка выполнения практических заданий
	Зачет	**8**			**2**				*зачет по билетам*
	Итого:		**16**		**24**			**36**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Основные понятия, концепции и принципы информационной безопасности**	Идентификация, аутентификация и авторизация. Модели информационной безопасности. Триада «конфиденциальность, доступность, целостность». Гексада Паркера и модель STRIDE. Уязвимость, угроза, атака. Ущерб и риск. Управление рисками. Типы и примеры атак. Пассивные и активные атаки. Отказ в обслуживании. Внедрение вредоносных программ. Кража личности, фишинг. Иерархия средств защиты от информационных угроз. Средства безопасности законодательного уровня. Административный уровень. Политика безопасности. Средства безопасности процедурного уровня. Средства безопасности технического уровня. Принципы защиты информационной системы. Подход сверху вниз. Защита как процесс. Эшелонированная защита. Сбалансированная защита. Компромиссы системы безопасности. Шифрование — базовая технология безопасности. Основные понятия и определения. Симметричное шифрование. Проблема распределения ключей. Метод Диффи-Хелмана передачи секретного ключа по незащищенному каналу. Концепция асимметричного шифрования. Алгоритм асимметричного шифрования RSA. Хеш-функции. Односторонние функции шифрования. Проверка целостности.
2	**Технологии аутентификации, авторизации и управления доступом**	Технологии аутентификации. Факторы аутентификации человека. Аутентификация на основе паролей. Аутентификация на основе аппаратных аутентификаторов. Аутентификация информации. Электронная подпись. Аутентификация на основе цифровых сертификатов. Аутентификация программных кодов. Технологии управления доступом и авторизации. Формы представления ограничений доступа. Системы аутентификации и управления доступом операционных систем. Аутентификации пользователей ОС. Аутентификация в ОС семейства Unix. Протокол SSH. Управление доступом в операционных системах. Централизованные системы аутентификации и авторизации. Концепция единого логического входа. Система Kerberos.
3	**Технологии безопасности на основе фильтрации и мониторинга трафика**	Фильтрация. Виды фильтрации. Стандартные и дополнительные правила фильтрации маршрутизаторов Cisco. Файерволы. Функциональное назначение файервола. Типы файерволов. Прок-

		си-серверы. Функции прокси-сервера. «Проксификация» приложений. Файерволы с функцией NAT. Традиционная технология NAT. Базовая трансляция сетевых адресов. Трансляция сетевых адресов и портов. Программные файерволы хоста. Типовые архитектуры сетей, защищаемых файерволами. Мониторинг трафика. Анализаторы протоколов. Анализаторы протоколов. Система мониторинга NetFlow. Системы обнаружения вторжений. Архитектура сети с защитой периметра и разделением внутренних зон. Аудит событий безопасности.
4	**Атаки на транспортную инфраструктуру сети**	TCP-атаки. ICMP-атаки. UDP-атаки. IP-атаки. Сетевая разведка. Задачи и разновидности сетевой разведки. Сканирование сети. Сканирование портов. Атаки на DNS. Технологии защищенного канала. Способы образования защищенного канала. Иерархия технологий защищенного канала. Распределение функций между протоколами IPSec. Безопасная ассоциация. Транспортный и туннельный режимы. VPN на основе шифрования.
5	**Уязвимость программного кода.**	Уязвимости программного кода и вредоносные программы. Уязвимости, связанные с нарушением защиты оперативной памяти. Уязвимости контроля вводимых данных.
6	**Безопасность программного кода.**	Внедрение в компьютеры вредоносных программ. Троянские программы. Сетевые черви. Вирусы. Программные закладки. Антивирусные программы. Ботнет.
7	**Безопасность сетевых служб**	Безопасность веб-сервиса. Безопасность веб-браузера. Приватность и куки. Протокол HTTPS. Безопасность средств создания динамических страниц. Безопасность электронной почты. Угрозы приватности почтового сервиса. Аутентификация отправителя. Шифрование содержимого письма. Защита метаданных пользователя. Спам. Атаки почтовых приложений. Облачные сервисы и их безопасность. Концепция облачных вычислений. Определение облачных вычислений. Модели сервисов облачных сервисов. Облачные вычисления как источник угрозы. Облачные сервисы как средство повышения сетевой безопасности.

4. Образовательные технологии

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1	*Основные понятия, концепции и принципы информационной безопасности*	*Лекция 1* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
2	*Технологии аутентификации, авторизации и управления доступом*	*Лекция 2* *Практическая работа 1* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*
3	*Технологии безопасности на основе фильтрации и мониторинга трафика*	*Лекция 3* *Практическая работа 2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*
4	*Атаки на транспортную инфраструктуру сети*	*Лекция 4.1* *Лекция 4.2* *Практическая работа 3* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*
5	*Уязвимость программного кода.*	*Лекция 5* *Практическая работа 4* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*
6	*Безопасность программного кода.*	*Лекция 6* *Практическая работа 5* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*
7	*Безопасность сетевых служб*	*Лекция 7* *Практическая работа 6* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- практическая работа №1* *- практическая работа №2* *- практическая работа №3* *- практическая работа №4* *- практическая работа №5* *- практическая работа №6*	 *15 баллов* *15 баллов* *15 баллов* *15 баллов* *20 баллов* *20 баллов*	 *15 баллов* *15 баллов* *15 баллов* *15 баллов* *20 баллов* *20 баллов*
Промежуточная аттестация *Зачет*		 *60 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-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1	Опрос
2.	Практические занятия 1 – 6	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1	План практических занятий

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

Вопросы к зачету - проверка сформированности компетенций ОПК-4.2, ПК-3

Контрольные вопросы	Реализуемые компетенции
1. Понятие идентификации, аутентификации и авторизации.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
2. Модели информационной безопасности.	ПК-3.3, ПК-3,2, ПК-3.1
3. Понятие уязвимости, угрозы, атаки.	ПК-3.3, ПК-3,2, ПК-3.1
4. Ущерб и риск. Управление рисками.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
5. Пассивные и активные атаки.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
6. Иерархия средств защиты от информационных угроз.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3
7. Понятие политики безопасности.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
8. Принципы защиты информационной системы.	; ПК-3.3, ПК-3,2, ПК-3.1
9. Основные понятия и определения криптографии.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
10. Симметричное шифрование.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
11. Асимметричное шифрование.	ОПК-4.2.1; ОПК-4.2.2;

	ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
12. Проблема распределения ключей.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
13. Хеш-функции.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
14. Проверка целостности.	; ПК-3.3, ПК-3,2, ПК-3.1
15. Технологии аутентификации.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
16. Аутентификация на основе паролей.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
17. Аутентификация на основе аппаратных аутентификаторов.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
18. Аутентификация информации.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
19. Электронная подпись.	ПК-3.3, ПК-3,2, ПК-3.1
20. Аутентификация на основе цифровых сертификатов.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3;
21. Аутентификация программных кодов.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
22. Технологии управления доступом и авторизации.	ПК-3.3, ПК-3,2, ПК-3.1
23. Системы аутентификации и управления доступом операционных систем.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
24. Аутентификации пользователей ОС.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
25. Аутентификация в ОС семейства Unix.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
26. Протокол SSH.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
27. Управление доступом в операционных системах.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
28. Централизованные системы аутентификации и авторизации. Концепция единого логического входа.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3;
29. Система Kerberos	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3
30. Фильтрация. Виды фильтрации.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
31. Файерволы. Функциональное назначение файервола.	ОПК-4.2.1; ОПК-4.2.2;

Типы файерволов.	ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
32. Прокси-серверы. Функции прокси-сервера. «Проксификация» приложений.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
33. Файерволы с функцией NAT. Традиционная технология NAT.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
34. Базовая трансляция сетевых адресов. Трансляция сетевых адресов и портов.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
35. Программные файерволы хоста.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
36. Типовые архитектуры сетей, защищаемых файерволами.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
37. Мониторинг трафика. Анализаторы протоколов. Анализаторы протоколов.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
38. Системы обнаружения вторжений.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1
39. Архитектура сети с защитой периметра и разделением внутренних зон.	ОПК-4.2.1; ОПК-4.2.2; ОПК-4.2.3; ПК-3.3, ПК-3,2, ПК-3.1

Примерные задания для тестирования- проверка сформированности компетенций ОПК-4.2, ПК-3

1. Криптомаршрутизатор - это:

а) аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов по протоколам IPsec AH и/или IPsec ESP при установлении соединения, соответствующий требованиям к средствам криптографической защиты информации ФСБ России и обеспечивающий базовую функциональность современного VPN-устройства..

б) мобильное средство связи.

в) дисковое устройство.

2. Шлюз безопасности VPN – это:

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

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

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

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники
Основные

1. *Руководящий докумен*т. 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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, 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-ot-30-marta-1992-g, 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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.
5. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Литература
Основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368
2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт,

2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063
4. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
5. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450234 (дата обращения: 09.09.2020).

6. *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
7. *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

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

1. Официальный сайт компании Криптопро [Электронный ресурс]: Режим доступа: http://www.cryptopro.com/, свободный. – Загл. с экрана.
2. Центр разработки Криптоком [Электронный ресурс]: Режим доступа: http://www.cryptocom.ru/products/index.html/, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлены 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 (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное

5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Secret Net Studio 8.4	Код безопасности	Свободное ПО, Режим доступа: https://securitycode.ru Демо-версия
8	Vmware Player 15.5	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия
9	XSpider 7.0	Positive Technologies	Свободное ПО, Режим доступа: https://www.ptsecurity.com/ru-ru/ Демо-версия
10	Nmap 7.8	Nmap	Свободное ПО, Режим доступа: https://nmap.org/ Демо-версия
11	Open VPN	OpenVPN	Свободное ПО, Режим доступа: https://openvpn.net/
12	SoftEther VPN	SoftEther	Свободное ПО, Режим доступа: https://www.softether.org/
13	Windscribe VPN	Windscribe	Свободное ПО, Режим доступа: https://windscribe.com/ Демо-версия
14	TinyFEC VPN	Wangyou	Открытое ПО, Режим доступа: https://github.com/wangyu-/tinyfecVPN

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

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

- для слепых и слабовидящих:

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

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

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

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

– письменные задания оформляются увеличенным шрифтом;

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

- для глухих и слабослышащих:

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

– письменные задания выполняются на компьютере в письменной форме;

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

- для лиц с нарушениями опорно-двигательного аппарата:

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

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

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

При необходимости предусматривается увеличение времени для подготовки ответа.

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

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

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

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

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;
– в форме электронного документа;
– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;
– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;
– в форме электронного документа;
– в форме аудиофайла.

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

- для слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;
– дисплеем Брайля PAC Mate 20;
– принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - проверка сформированности компетенций ОПК-4.2, ПК-3

Практическое занятие 1 (4 ч.) «Технологии аутентификации, авторизации и управления доступом» - проверка сформированности компетенций ОПК-4.2, ПК-3
Задания:

1. Создание новых пользователей и исследование механизмов расширенной аутентификации на примере Secret Net Studio.
2. Управление доступом в операционных системах с помощью встроенных и наложенных средств защиты информации.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, средства защиты информации Secret Net Studio.

Практическое занятие 2 (4 ч.) «Технологии безопасности на основе фильтрации и мониторинга трафика» - проверка сформированности компетенций ОПК-4.2, ПК-3
Задания:

1. Установка и настройка VPN-клиента.
2. Осуществление мониторинга трафика.
3. Осуществление аудита событий безопасности.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer. VPN-клиент, выход в Интернет с возможностью доступа к сайтам https://ipleak.net , https://www.perfect-privacy.com/check-ip, https://ipx.ac/run, https://browserleaks.com/webrtc, https://www.perfect-privacy.com/dns-leaktest.

Практическое занятие 3 (4 ч.) «Исследования транспортной инфраструктуры сети» - проверка сформированности компетенций ОПК-4.2, ПК-3
Задания:

1. Изучить стек протокола TCP/IP.
2. Получить у преподавателя метрики зондируемых сетей.
3. Сканирование сети. Сканирование портов.
4. Подготовка отчета об уровне защищенности просканированных узлов.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer,Программное средство сканирования сети и портов (XSpider, Nmap), VPN-клиент, выход в Интернет с возможностью подключения к серверам VPN-услуг.

Практическое занятие 4 (4 ч.) «Уязвимости программного кода и вредоносные программы» - проверка сформированности компетенций ОПК-4.2, ПК-3
Задания:

1. Уязвимости программного кода.
2. Исследование механизмов контроля целостности, контроля приложений и т.д..
3. Настройка компонентов защиты.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, средства защиты информации Secret Net Studio.

Практическое занятие 5 (4 ч.) «Программные закладки. Работа с изолированной программной средой» - проверка сформированности компетенций ОПК-4.2, ПК-3
Задания:

1. Исследование методов внедрения программных закладок в виртуальной “песочнице”.
2. Настройка изолированной программной среды.
3. Конфигурирование компонента контроля съемных машинописных носителей информации.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, средства защиты информации Secret Net Studio.

Практическое занятие 6 (2 ч.) «Безопасность веб-сервиса» - проверка сформированности компетенций ОПК-4.2, ПК-3
Задания:
1. Изучить способы проведения тестов на проникновение.
2. Сбор сведений в сети нтернет по уязвимостям Web-серверов на примере apache и nginx.
3. Установить сканеры XSpider и Nmap.
4. Произвести сканирование на защищенность Web-сервисов на примере сайтов www.rsuh.ru, www.yandex.ru , www.ict.cn.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer.Сканеры Nmap и XSpider.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность телекоммуникационных 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 (профили подготовки – Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

Цель дисциплины – формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.
Задачи дисциплины:
– овладение методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
– формирование навыков анализа информационной инфраструктуры информационных систем и ее безопасности.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-4.2 -Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем
- ОПК-4.2.1 -Знает средства, методы и протоколы идентификации, аутентификации и авторизации
- ОПК-4.2.2 -Умеет устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации
- ОПК-4.2.3 -Владеет навыками управления полномочиями пользователей
- ПК-3 -Способен управлять защитой информации в автоматизированных системах
- ПК-3.1 -Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах
- ПК-3.2 -Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах
- ПК-3.3 -Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

В результате освоения дисциплины обучающийся должен:
Знать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
Владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.