МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по учебной работе
Д.Ш. Султанова
«07» июня 2021 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1060
Подписал Проректор по учебной работе Д.Ш. Султанова
Дата 07.06.2021

РАБОЧАЯ ПРОГРАММА
по дисциплине **«ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В ТЕЛЕКОММУНИКАЦИЯХ»**

Направление подготовки:	10.03.01 Информационная безопасность
Профиль:	Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная
Институт:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Факультет:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Кафедра-разработчик:	Казанский межвузовский инженерный центр "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет"
Курс; семестр	3; 5

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	18	0,5
Практическое занятие	18	0,5
Контроль самостоятельной работы	18	0,5
Самостоятельная работа	108	3
Форма аттестации: Дифференцированный зачет (5 сем)		
Всего	180	5

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1427 от 17.11.2020) по направлению подготовки 10.03.01 Информационная безопасность для профиля «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент А.Ю. Сенцова

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании Казанского межвузовского инженерного центра "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет", протокол от 19.05.2021 г. № 6.

Директор ***Согласовано*** А.Ф. Махоткин

У Т В Е Р Ж Д Е Н О

Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита информационных процессов в телекоммуникациях» являются:

-ознакомить с основными понятиями, используемыми при защите информации в телекоммуникационных системах;

-дать представление об основных проблемах защиты информации в телекоммуникационных системах;

-обучить студентов методам защиты информации в телекоммуникационных системах для построения защищенных информационных технологий;

-получить навыки практической работы по использованию средств защиты информационных процессов в телекоммуникационных системах.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информационных процессов в телекоммуникациях» относится к формируемой участниками образовательных отношений части ООП и формирует у обучающихся по профилю «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Защита информационных процессов в телекоммуникациях» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Информационные технологии в информационной безопасности
2. Основы информационной безопасности
3. Теория информации

Дисциплина «Защита информационных процессов в телекоммуникациях» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Защита информации от утечки по техническим каналам
2. Комплексная система защиты информации
3. Методы и средства криптографической защиты информации
4. Программно-аппаратные средства защиты информации

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК-2 Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности

ПК-2.1. Знает критерии безопасности обработки информации в телекоммуникационных системах

ПК-2.2. Умеет выполнять мероприятия для реализации политики информационной безопасности

ПК-2.3. Владеет навыками определения состава и порядка настройки технических средств для управления телекоммуникационными системами и средствами их защиты от НСД

ПК-3 Способен выполнять работы по обеспечению информационной безопасности телекоммуникационных систем на всех этапах их жизненного цикла

ПК-3.1. Знает план мероприятий по внедрению решений и средств для обеспечения информационной безопасности в соответствии с требованиями реализуемой политики безопасности

ПК-3.2. Умеет восстанавливать работоспособность телекоммуникационных систем после инцидентов информационной безопасности

ПК-3.3. Владеет навыками проведения операции вывода защищённых телекоммуникационных систем из эксплуатации

В результате освоения дисциплины обучающийся должен

Знать:

-основные проектные решения современных сетей и систем передачи информации и средства их

защиты; основные источники информации, содержащие данные по параметрам антенн и фидеров; этапы проектирования телекоммуникационных систем;
-технологию построения защищенных телекоммуникационных систем; методы оценок защищенности телекоммуникационных систем; основные подходы к оценке защищенности телекоммуникационных систем.

Уметь:

-оценивать защищенность телекоммуникационных систем; анализировать риски в телекоммуникационных системах; осуществлять эксплуатацию средств защиты информационных процессов в телекоммуникационных системах;
-проводить анализ исходных данных для проектирования подсистем сетей передачи информации и средств обеспечения информационной безопасности;

Владеть:

-навыками анализа исходных данных для составления технического задания; базовыми навыками моделирования вычислительных операций; первичными навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
-навыками работы с нормативными документами по оценке защищенности телекоммуникационных систем; навыками сбора и анализа материалов, необходимых для оценки защищенности телекоммуникационных систем.

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Основы информационной безопасности в сфере телекоммуникаций	5	2		6	3	18	Лабораторная работа; Реферат
2.	Технология применения комплексной системы защиты информации	5	2		6	3	18	
3.	Сервисы, атаки, вирусы, криптозащита	5	4		6	3	18	
4.	Системы защиты	5	4	6		3	18	Практические занятия; Реферат
5.	Технологии криптозащиты и межсетевого обмена	5	4	6		3	18	
6.	НСД и технические средства защиты от него	5	2	6		3	18	
	Итого по семестру	**5**	**18**	**18**	**18**	**18**	**108**	**Дифференцированный зачет**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Основы информационной безопасности в сфере телекоммуникаций	2	Классификация и анализ угроз информационной безопасности в многоканальных телекоммуникационных системах. Виды уязвимости информации и формы ее проявления	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Технология применения комплексной системы защиты информации	2	Структурные схемы систем защиты информации в типовых информационных системах. Показатели защищенности телекоммуникационных систем.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Сервисы, атаки, вирусы, криптозащита	2	Сервисы, обеспечивающие информационную безопасность в телекоммуникационных системах и сетях электросвязи: ограничение физического доступа к автоматизированным системам; идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.		2	Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.	Системы защиты	2	Построение систем антивирусной защиты телекоммуникационных систем и сетей	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.		2	Технологии защиты данных	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
7.	Технологии криптозащиты и межсетевого обмена	2	Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография)	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
8.		2	Различные технологии аутентификации. Технологии защиты межсетевого обмена данных	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
9.	НСД и технические средства защиты от него	2	Требования по защите от несанкционированного	ПК-2.1 ПК-2.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
			доступа. Технические средства обеспечения безопасности телекоммуникационных систем	ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Системы защиты	6	Wireshark: анализ протоколов Ethernet и ARP.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Технологии криптозащиты и межсетевого обмена	6	Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	НСД и технические средства защиты от него	6	Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**18**		

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Основы информационной безопасности в сфере телекоммуникаций	6	Программная аутентификация и идентификация в сетевых операционных системах.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Технология применения комплексной системы защиты информации	6	Методы разграничения доступа в сетевых операционных системах.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Сервисы, атаки, вирусы, криптозащита	6	Методы защиты информации. Шифр простой перестановки. Шифр Цезаря.	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**18**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Программная аутентификация и идентификация в сетевых операционных системах.	18	написание реферата, подготовка к лабораторной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Методы разграничения доступа в сетевых операционных системах.	18	написание реферата, подготовка к лабораторной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Методы защиты информации. Шифр простой перестановки. Шифр Цезаря.	18	написание реферата, подготовка к лабораторной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.	Wireshark: анализ протоколов Ethernet и ARP.	18	написание реферата, подготовка к практическому занятию	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.	Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH.	18	написание реферата, подготовка к практическому занятию	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.	Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей	18	написание реферата, подготовка к практическому занятию	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**108**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Программная аутентификация и идентификация в сетевых операционных системах.	3	прием лабораторной работы, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Методы разграничения доступа в сетевых операционных системах.	3	прием лабораторной работы, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Методы защиты информации. Шифр простой перестановки. Шифр Цезаря.	3	прием лабораторной работы, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
				ПК-3.3
4.	Wireshark: анализ протоколов Ethernet и ARP.	3	проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
5.	Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH.	3	проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
6.	Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей	3	проверка знаний на практическом занятии, проверка реферата	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**18**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита информационных процессов в телекоммуникациях» используется рейтинговая система. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО КНИТУ.

Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Мин.баллов	Макс.баллов
5-й семестр			
Лабораторная работа	3	24	42
Практические занятия	3	24	42
Реферат	1	12	16
Итого		**60**	**100**

10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

11. Информационно-методическое обеспечение дисциплины

11.1. Основная литература

При изучении дисциплины «Защита информационных процессов в телекоммуникациях» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В. Ф. Шаньгин, Информационная безопасность [Электронный ресурс] : Москва : ДМК Пресс, 2014	http://e.lanbook.com/books/element.php?pl1_id=50578 Режим доступа: по подписке КНИТУ
А. М. Голиков, Кодирование в телекоммуникационных системах [Электронный ресурс] Учебное пособие для	http://www.iprbookshop.ru/72111.html Режим доступа: по подписке КНИТУ

специалитета: 090302.65 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, задание на самостоятельную работу: Томск : Томский государственный университет систем управления и радиоэлектроники, 2016	

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников, Информационная безопасность [Лабораторные работы] лабор. практикум : учеб. пособие: М. : Кнорус, 2013	1 экз. УНИЦ ФГБОУ ВО «КНИТУ»
В. В. Лисяк, Разработка информационных систем [Прочее] учебное пособие: Ростов-на-Дону|Таганрог : Южный федеральный университет, 2019	http://biblioclub.ru/index.php?page=book&id=577875 Режим доступа: по подписке КНИТУ
А. В. Артемов, Информационная безопасность [Прочее] курс лекций: Орел : МАБИВ, 2014	http://biblioclub.ru/index.php?page=book&id=428605 Режим доступа: по подписке КНИТУ
Е.А. Бельтюкова, О.М. Любимова, Информационная безопасность телекоммуникационных систем предприятия (объединения [Прочее] : М. ; Брюссель : , 2001	1 экз. УНИЦ ФГБОУ ВО «КНИТУ»

11.3. Электронные источники информации

При изучении дисциплины «Защита информационных процессов в телекоммуникациях» предусмотрено использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/
6. ЭБС IPR SMART: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

11.4. Профессиональные базы данных и информационные справочные системы

Базы данных
Wiley Online Library: https://onlinelibrary.wiley.com/
Springer Nature: https://link.springer.com/
zbMath : https://zbmath.org/

Информационные справочные системы
Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru
Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

12. Материально-техническое обеспечение дисциплины

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое в учебном процессе при освоении дисциплины «Защита информационных процессов в телекоммуникациях»:

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard
Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

Офисные и деловые программы: 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях
Офисные и деловые программы: Константа: Управление процессами.

Дополнительное ПО доступное по бесплатной подписке от Microsoft

Офисные и деловые программы: Microsoft Office 365 Версия для студентов
Офисные и деловые программы: Microsoft Office 365 Версия для преподавателей
ПО для коллективной работы Microsoft Teams

Moodle 3.10

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
1. Ноутбук на базе процессора AMD Dual-Core E-350
2. Проектор мультимедийный EB-W10, экран для проектора.
3. Экран проекционный настенный.

Помещения для самостоятельной работы оснащены компьютерной техникой:
компьютер преподавателя
11 компьютеров студента тип AMD A4-6300
кондиционер SystemAir Sysplit Wall Smart
Проектор Acer H5360BD с доской интерактивной, экран
с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ..Допускается замена оборудования его виртуальными аналогами.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Защита информационных процессов в телекоммуникациях» составляет 9 ч.

В процессе освоения дисциплины «Защита информационных процессов в телекоммуникациях» используются следующие образовательные технологии:
• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция).