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 **«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

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	2; 3

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	36	1
Контроль самостоятельной работы	18	0,5
Самостоятельная работа	81	2,25
Форма аттестации: Экзамен (3 сем)	27	0,75
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 «Основы информационной безопасности» являются:
а) развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
б) развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
в) привитие стремления к поиску оптимальных, простых и надежных решений;
г) расширение кругозора.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к обязательной 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 «Основы информационной безопасности» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:
1. Информатика
2. Информационные технологии в информационной безопасности

Дисциплина «Основы информационной безопасности» является предшествующей и необходима для успешного освоения последующих дисциплин:
1. Защита информационных процессов в телекоммуникациях

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-5.2 Способен применять технологии защиты информации при создании защищенных телекоммуникационных систем;

ОПК-5.2.1. Знает современные законы, стандарты, методы и технологии в области защиты информации

ОПК-5.2.2. Умеет использовать современные программно-аппаратные средства защиты информации при создании защищенных телекоммуникационных систем

ОПК-5.2.3. Владеет современными методами и технологиями обеспечения защиты информации при создании защищенных телекоммуникационных систем

В результате освоения дисциплины обучающийся должен

Знать:

современные законы, стандарты, методы и технологии в области защиты информации

технологии защиты телекоммуникационных систем

Уметь:

применять технологии защиты информации при создании защищенных телекоммуникационных систем

использовать современные программно-аппаратные средства защиты информации

Владеть:

методами и технологиями обеспечения защиты информации

способностью создания защищенных 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.	Теоретические основы информационной безопасности	3	8		12	8	38	Лабораторная работа; Реферат; Экзамен
2.	Методологические основы защиты информации	3	10		24	10	43	
	Итого по семестру	**3**	**18**		**36**	**18**	**81**	**Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Теоретические основы информационной безопасности	2	Составляющие национальных интересов Российской Федерации в информационной сфере	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.		2	Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.		2	Основные определения и задачи информационной безопасности. Риски и угрозы информационной безопасности	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
4.		2	Нормативно-правовое обеспечение информационной безопасности. Стандарты информационной безопасности	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
5.	Методологические основы защиты информации	2	Методы и технологии защиты информации. Классификация методов и средств защиты информации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
6.		2	Системы идентификации и аутентификации. Системы разграничения доступа	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
7.		2	Стеганографические и криптографические методы	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
8.		2	Методы обнаружения и блокирования угроз информационной безопасности	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
9.		2	Методы защиты в операционных системах. Сетевые технологии защиты	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

Проведение практических/семинарских занятий не предусмотрено учебным планом

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Теоретические основы информационной безопасности	6	Законодательство РФ в области информационной безопасности	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.		6	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.	Методологические основы защиты информации	6	Процедура аутентификации пользователя на основе пароля	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
4.		6	Программная реализация криптографических алгоритмов.	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
5.		6	Механизмы контроля целостности данных.	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
6.		6	Пакеты антивирусных программ.	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
	ВСЕГО	**36**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Составляющие национальных интересов Российской Федерации в информационной сфере	12	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.	Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации	10	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.	Основные определения и задачи информационной безопасности. Риски и угрозы информационной безопасности	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
4.	Нормативно-правовое обеспечение информационной безопасности. Стандарты информационной безопасности	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
5.	Методы и технологии защиты информации. Классификация методов и средств защиты информации	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
6.	Системы идентификации и аутентификации. Системы разграничения доступа	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
7.	Стеганографические и криптографические методы	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
8.	Методы обнаружения и блокирования угроз информационной безопасности	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
9.	Методы защиты в операционных системах. Сетевые технологии защиты	11	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
	ВСЕГО	**81**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Составляющие национальных интересов Российской Федерации в информационной сфере	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.	Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.	Основные определения и задачи информационной безопасности. Риски и угрозы информационной безопасности	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
4.	Нормативно-правовое обеспечение информационной безопасности. Стандарты информационной безопасности	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
5.	Методы и технологии защиты информации. Классификация методов и средств защиты информации	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
6.	Системы идентификации и аутентификации. Системы разграничения доступа	2	прием лабораторной работы, прием лабораторной работы, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
7.	Стеганографические и криптографические методы	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
8.	Методы обнаружения и блокирования угроз информационной безопасности	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
9.	Методы защиты в операционных системах. Сетевые технологии защиты	2	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
	ВСЕГО	**18**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Основы информационной безопасности» 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
3-й семестр			
Лабораторная работа	6	30	48
Реферат	1	6	12
Экзамен	1	24	40
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 «Основы информационной безопасности» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
А. Е. Фаронов, Основы информационной безопасности при работе на компьютере [Электронный ресурс] : Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52160.html Режим доступа: по подписке КНИТУ
Т. А. Гультяева, Основы информационной безопасности [Прочее] учебное пособие: Новосибирск : Новосибирский государственный технический университет, 2018	http://biblioclub.ru/index.php?page=book&id=574729 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
А. А. Внуков, Основы информационной безопасности: защита информации [Прочее] Учебное пособие Для СПО: Москва : Юрайт, 2020	https://urait.ru/bcode/467356 Режим доступа: по подписке КНИТУ
В. Ю. Рогозин, В. К. Новиков, И. Б. Галушкин [и др.], Основы информационной безопасности [Электронный ресурс] Учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»: Москва : ЮНИТИ-ДАНА, 2017	http://www.iprbookshop.ru/72444.html Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Основы информационной безопасности» 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/

УНИЦ
Согласовано

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 «Основы информационной безопасности»:

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

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
Аудитория 351-А;
1. Виртуальные машины VirtualBOX (GNU GENERAL PUBLIC LICENSE)
2. Симулятор сетей GNS3 (GNU GENERAL PUBLIC LICENSE)
3. Операционная система Linux (Fedora, Ubuntu). (GNU GENERAL PUBLIC LICENSE)
4. RADIUS сервер (GNU GENERAL PUBLIC LICENSE)
5. Sendmail - SMTP сервер (Sendmail License)
6. POP3 сервер (BSD License)
7. IMAP4 сервер (BSD License)
8. NTP сервер (BSD License)
9. Межсетевой экран iptables (GNU GENERAL PUBLIC LICENSE)
10. Межсетевой экран Firewalld (GNU GENERAL PUBLIC LICENSE)
11. Сканер сетевой безопасности nmap (GNU GENERAL PUBLIC LICENSE)
12. Система обнаружения атак snort (GNU GENERAL PUBLIC LICENSE)
13. Система синхронизации данных rsync
14. компьютер/ноутбук
техническими средствами обучения:
1. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» .
Помещения для самостоятельной работы оснащены компьютерной техникой:
Аудитория Г-407, компьютер/ноутбук с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Основы информационной безопасности» составляет 9 ч.

В процессе освоения дисциплины «Основы информационной безопасности» 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);