

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 «**ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ
ЗАЩИТЫ ИНФОРМАЦИИ**»

Специальность:	10.05.05 Безопасность информационных технологий в правоохранительной сфере
Специализация:	Технологии защиты информации в правоохранительной сфере
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	Очная
Институт:	Инженерный химико-технологический институт
Факультет:	Факультет экологической, технологической и информационной безопасности
Кафедра-разработчик:	Кафедра «Информационная безопасность»
Курс; семестр	2; 4

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Практическое занятие	27	0,75
Контроль самостоятельной работы	27	0,75
Самостоятельная работа	36	1
Форма аттестации: Экзамен (4 сем)	36	1
Всего	144	4

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1461 от 22.11.2020) по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере для специализации «Технологии защиты информации в правоохранительной сфере» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Старший преподаватель

А.Р. Касимова

СОГЛАСОВАНО

Рабочая программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность», протокол от 26.05.2021 г. № 10.

Заведующий кафедрой *Согласовано* В.А. Богомолов

УТВЕРЖДЕНО

Начальник центра УМЦ

Утверждаю

Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Теория информационной безопасности и методология защиты информации» являются:

- а) раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности,
- б) определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов;
- в) освоение данной дисциплины ориентировано на расширение и углубление знаний, умений, навыков и компетенций, определяемых содержанием базовых (обязательных) дисциплин, которые студенты будут изучать в дальнейшем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Теория информационной безопасности и методология защиты информации» относится к обязательной части ООП и формирует у обучающихся по специализации «Технологии защиты информации в правоохранительной сфере» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Теория информационной безопасности и методология защиты информации» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Аппаратные средства вычислительной техники
2. Информационные технологии в правоохранительной деятельности
3. Операционные среды, системы и оболочки
4. Средства и системы технического обеспечения обработки, хранения и передачи информации

Дисциплина «Теория информационной безопасности и методология защиты информации» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Защита персональных данных на предприятии
2. Комплексная система защиты информации на предприятии
3. Методы и средства криптографической защиты информации
4. Правовая защита информации
5. Уязвимость и безопасность вычислительных сетей

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-10 Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач

ОПК-10.1. Знает современные методы поиска профессиональной литературы

ОПК-10.2. Умеет составлять аналитические обзоры при выполнении профессиональных обязанностей

ОПК-10.3. Владеет навыками аналитического чтения профессиональных документов и специализированной литературы

В результате освоения дисциплины обучающийся должен

Знать:

базовый понятийный аппарат в области информационной безопасности (И- и защиты информации (ЗИ);

виды и составы угроз ИБ; принципы и общие методы обеспечения ИБ;

основные положения государственной политики обеспечения ИБ;

критерии, условия и принципы отнесения информации к защищаемой;
 виды носителей защищаемой информации;
 виды и подвиды тайн конфиденциальной информации;
 виды уязвимостей защищаемой информации и формы ее проявления;
 источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;
 каналы и методы НСД к защищаемой информации;
 состав объектов ЗИ; классификацию видов, методов и средств ЗИ;
 состав кадрового, ресурсного и технологического обеспечения ЗИ.

Уметь:

выявлять угрозы ИБ применительно к объектам защиты;
 выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;
 выявлять применительно к объекту защиты каналы и методы НСД к конфиденциальной информации

Владеть:

методами определения состава конфиденциальной информации применительно к видам тайны;
 навыками определения направлений и видов ЗИ с учетом характера информации и задач по ее защите.

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежуточной аттестации
			Лекция	Практические занятия	Лабораторные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Основные понятия и определения предмета защиты информации	4	2	4		6	6	Практические занятия; Реферат
2.	Угрозы информации, методология их выявления и оценки	4	4	8		10	12	Проект; Реферат
3.	Общая классификация защитных мер	4	2	6		4	10	Проект
4.	Система управления доступом	4	4	4		3	4	Практические занятия
5.	Контроль целостности информации. Обзор криптографических средств защиты.	4	6	5		4	4	Практические занятия; Экзамен
	Итого по семестру	4	18	27		27	36	Экзамен

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Основные понятия и определения предмета защиты информации	2	Сущность и понятие информационной безопасности. Основные понятия и определения предмета защиты информации	ОПК-10.1 ОПК-10.3
2.	Угрозы информации, методология их выявления и оценки	2	Понятие, классификация и оценка угроз безопасности информации	ОПК-10.1 ОПК-10.3
3.		2	Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа.	ОПК-10.1 ОПК-10.3
4.	Общая классификация защитных мер	2	Классификация видов, способов, методов и средств защиты информации.	ОПК-10.1 ОПК-10.3
5.	Система управления доступом	4	Разграничение доступа к информации в компьютерных системах	ОПК-10.1 ОПК-10.3
6.	Контроль целостности информации. Обзор криптографических средств защиты.	4	Симметричные и ассимметричные криптосистемы	ОПК-10.1 ОПК-10.3
7.		2	Хеширование, электронная подпись	ОПК-10.1 ОПК-10.3
	ВСЕГО	18		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Основные понятия и определения предмета защиты информации	2	Актуальность угроз ИБ. Анализ НПА.	ОПК-10.2 ОПК-10.3
2.		2	Теоретические основы ИБ РФ	ОПК-10.1 ОПК-10.3
3.	Угрозы информации, методология их выявления и оценки	6	Разработка рекомендаций по совершенствованию системы защиты информации в информационной системы предприятия (по отраслям). Часть 1	ОПК-10.1 ОПК-10.3
4.		2	Способы реализации угроз безопасности информации. Уязвимости систем обработки информации	ОПК-10.1 ОПК-10.2 ОПК-10.3
5.	Общая классификация защитных мер	6	Разработка рекомендаций по совершенствованию системы защиты информации в информационной системы предприятия (по отраслям). Часть 2	ОПК-10.1 ОПК-10.3
6.	Система управления доступом	4	Идентификация и аутентификация пользователя с использованием различных моделей управления.	ОПК-10.1 ОПК-10.3
7.	Контроль целостности информации. Обзор криптографических средств защиты.	4	Симметричные криптосистемы. Алгоритм RSA.	ОПК-10.1 ОПК-10.3
8.		1	Аутентификация на основе сертификатов	ОПК-10.1 ОПК-10.3
	ВСЕГО	27		

7. Содержание лабораторных занятий

Проведение лабораторных занятий не предусмотрено учебным планом

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Модели безопасности информационных технологий организации	6	написание реферата, подготовка к практическому занятию	ОПК-10.1 ОПК-10.3
2.	Объекты защиты. Взаимосвязь угрозы с уязвимостью и рисками	12	написание реферата, подготовка к проекту	ОПК-10.1 ОПК-10.3
3.	Неформальная модель нарушителя безопасности автоматизированной системы	10	подготовка к проекту	ОПК-10.1 ОПК-10.3
4.	Безопасность системы контроля и управления доступом	4	подготовка к практическому занятию	ОПК-10.1 ОПК-10.3
5.	Контроль конфиденциальности	4	подготовка к практическому занятию, подготовка к экзамену	ОПК-10.1 ОПК-10.3
ВСЕГО		36		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Модели безопасности информационных технологий организации	6	проверка знаний на практическом занятии, проверка реферата	ОПК-10.1 ОПК-10.3
2.	Объекты защиты. Взаимосвязь угрозы с уязвимостью и рисками	10	проверка проекта, проверка реферата	ОПК-10.1 ОПК-10.3
3.	Неформальная модель нарушителя безопасности автоматизированной системы	4	проверка проекта	ОПК-10.1 ОПК-10.3
4.	Безопасность системы контроля и управления доступом	3	проверка знаний на практическом занятии	ОПК-10.1 ОПК-10.3
5.	Контроль конфиденциальности	4	прием экзамена, проверка знаний на практическом занятии	ОПК-10.1 ОПК-10.3
ВСЕГО		27		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Теория информационной безопасности и методология защиты информации» 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
4-й семестр			
Проект	1	16	24
Реферат	2	8	16
Практические занятия	4	12	20
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 «Теория информационной безопасности и методология защиты информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
А.Р. Касимова, Л.Х. Сафиуллина, А.М. Садыков [и др.], Информационная безопасность. Практические аспекты [Электронный ресурс] учебник: СПб : ИЦ "Интермедия", 2021	http://ft.kstu.ru/ft/Safiullina- Inform_bezop_prakt_aspekty.pdf Доступ с IP адресов КНИТУ
Медведев В.А., Информационная безопасность. Введение в специальность + еПриложение: Тесты [Прочее] Учебник: Москва : КноРус, 2021	https://www.book.ru/book/936335 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
В.Ф. Шаньгин, Информационная безопасность компьютерных систем и сетей [Прочее] Учебное пособие: Москва : Издательский Дом "ФОРУМ", 2021	http://znanium.com/catalog/document?id=364622 Режим доступа: по подписке КНИТУ
И.С. Клименко, Информационная безопасность и защита информации: модели и методы управления [Прочее] Монография: Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	http://znanium.com/go.php?id=1137902 Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Теория информационной безопасности и методология защиты информации» 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 IPRbooks: 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

Scopus Доступ свободный: www.scopus.com

Web of Science Доступ свободный: apps.webofknowledge.com

Информационные справочные системы

Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru

Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

Банк данных угроз ФСТЭК

<https://bdu.fstec.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 «Теория информационной безопасности и методология защиты информации»:

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:

Комплект учебной мебели, переносные (стационарные) проектор и экран, АРМ преподавателя и студентов.

Помещения для самостоятельной работы оснащены компьютеризированные рабочие места, с доступом к электронным библиотечным ресурсам, с выходом в Интернет и необходимым комплектом лицензионного программного обеспечения 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 «Теория информационной безопасности и методология защиты информации» составляет 18 ч.

В процессе освоения дисциплины «Теория информационной безопасности и методология защиты информации» используются следующие образовательные технологии:

- работа в малых группах;
- разработка проекта (метод проектов);
- системы дистанционного обучения.