

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 «**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ**»

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	4; 7

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	54	1,5
Контроль самостоятельной работы	36	1
Самостоятельная работа	45	1,25
Форма аттестации: Экзамен (7 сем)	27	0,75
Всего	180	5

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 «Теоретические основы компьютерной безопасности» являются:

раскрыть содержание основных понятий и формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности)

Задачи дисциплины – дать основы:

- исходных понятий и формализации в сфере компьютерной безопасности;
- представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;
- методологии анализа архитектурных (схемно-технических) и программноалгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

## **2. Место дисциплины в структуре образовательной программы**

Дисциплина «Теоретические основы компьютерной безопасности» относится к формируемой участниками образовательных отношений части ООП и формирует у обучающихся по специализации «Технологии защиты информации в правоохранительной сфере» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Теоретические основы компьютерной безопасности» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Безопасность корпоративных информационных систем
2. Информатика

Дисциплина «Теоретические основы компьютерной безопасности» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Комплексная система защиты информации на предприятии
2. Подготовка к процедуре защиты и защита выпускной квалификационной работы
3. Производственная практика (преддипломная практика)

## **3. Компетенции обучающегося, формируемые в результате освоения дисциплины**

**ПК -2 Способен обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем**

ПК -2.1. Знает принципы построения компьютерных сетей, порядок реализации методов и средств межсетевого экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

ПК -2.2. Умеет оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях

ПК -2.3. Владеет навыками применения программно-аппаратных средств защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

**В результате освоения дисциплины обучающийся должен**

**Знать:**

методологические и технологические основы комплексного обеспечения безопасности АС.

- угрозы и методы нарушения безопасности АС,
- формальные модели, лежащие в основе систем защиты АС,
- стандарты по оценке защищенности АС и их теоретические основы,
- методы и средства реализации защищенных АС,
- методы и средства верификации и анализа надежности защищенных

основные модели данных;

физическую организацию баз данных;

средства обеспечения безопасности данных;

последовательность и содержание этапов проектирования баз данных;

#### **Уметь:**

проводить анализ АС с точки зрения обеспечения компьютерной безопасности,

разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы,

применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС,

реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС; данных;

создавать объекты базы данных;

выполнять запросы к базе данных;

разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;

применять средства обеспечения безопасности данных;

#### **Владеть:**

навыками работы с АС распределенных вычислений и обработки информации;

навыками работы с документацией АС,

навыками использования критериев оценки защищенности АС,

навыками построения формальных моделей систем защиты информации АС.

#### **4. Структура и содержание дисциплины**

Общая трудоёмкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ 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.	Модели безопасности компьютерных систем	7	9		20	14	15	Лабораторная работа
2.	Методы анализа и оценки	7	9		34	22	30	Лабораторная работа; Экзамен

№ 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
	защищенности компьютерных систем							
	<b>Итого по семестру</b>	<b>7</b>	<b>18</b>		<b>54</b>	<b>36</b>	<b>45</b>	<b>Экзамен</b>

### 5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Модели безопасности компьютерных систем	4	Модели безопасности на основе различных политик доступа	ПК -2.1
2.		5	Модели и технологии обеспечения целостности и доступности данных	ПК -2.1
3.	Методы анализа и оценки защищенности компьютерных систем	4	Теоретико-графовые модели комплексной оценки защищенности	ПК -2.1
4.		5	Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа	ПК -2.1
	<b>ВСЕГО</b>	<b>18</b>		

### 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.	Модели безопасности компьютерных систем	20	Модель безопасности компьютерных систем	ПК -2.2 ПК -2.3
2.	Методы анализа и оценки защищенности компьютерных систем	34	Применение методов анализа и оценки защищенности компьютерных систем	ПК -2.2 ПК -2.3
	<b>ВСЕГО</b>	<b>54</b>		

### 8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Модели безопасности компьютерных систем	15	подготовка к лабораторной работе	ПК -2.1 ПК -2.2 ПК -2.3
2.	Методы анализа и оценки защищенности компьютерных систем	30	подготовка к лабораторной работе, подготовка к экзамену	ПК -2.1 ПК -2.2 ПК -2.3

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
	<b>ВСЕГО</b>	<b>45</b>		

### 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 компьютерных систем	14	прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
2.	Методы анализа и оценки защищенности компьютерных систем	22	прием лабораторной работы, прием экзамена	ПК -2.1 ПК -2.2 ПК -2.3
	<b>ВСЕГО</b>	<b>36</b>		

### 9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Теоретические основы компьютерной 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
<b>7-й семестр</b>			
Лабораторная работа	2	36	60
Экзамен	1	24	40
<b>Итого</b>		<b>60</b>	<b>100</b>

### 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 «Теоретические основы компьютерной безопасности» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В. Г. Олифер,, Н. А. Олифер,, Основы сетей передачи данных [Прочее] : Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021	<a href="http://www.iprbookshop.ru/102041.html">http://www.iprbookshop.ru/102041.html</a> Режим доступа: по подписке КНИТУ
В. О. Сафонов,, Основы современных операционных систем [Прочее] учебное пособие: Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	<a href="http://www.iprbookshop.ru/94855.html">http://www.iprbookshop.ru/94855.html</a> Режим доступа: по подписке КНИТУ

## 11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
В. И. Петренко, Теоретические основы защиты информации [Прочее] учебное пособие: Ставрополь : СКФУ, 2015	<a href="http://biblioclub.ru/index.php?page=book&amp;id=458204">http://biblioclub.ru/index.php?page=book&amp;id=458204</a> Режим доступа: по подписке КНИТУ
Л.Х. Сафиуллина, А.Р. Касимова, Я.С. Рябов [и др.], Информационная безопасность. Практические аспекты [Прочее] учеб. пособие для студ. вузов спец. "Информ. безопасность": СПб. : ИЦ "Интермедия", 2021	5 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Э. Таненбаум, Д. Уэзеролл, Компьютерные сети [Прочее] : М. ; СПб. ; Н.Новгород ; Воронеж [и др.] : Питер, 2015	5 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Э. Таненбаум, Х. Бос, Современные операционные системы [Прочее] : М. [и др.] : Питер, 2015	10 экз. УНИЦ ФГБОУ ВО «КНИТУ»

## 11.3. Электронные источники информации

При изучении дисциплины «Теоретические основы компьютерной 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 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](http://www.scopus.com)

Web of Science Доступ свободный: [apps.webofknowledge.com](http://apps.webofknowledge.com)

Информационные справочные системы

Справочно-правовая система «ГАРАНТ» Доступ свободный: [www.garant.ru](http://www.garant.ru)

Справочно-правовая система «КонсультантПлюс» Доступ свободный: [www.consultant.ru](http://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 «Теоретические основы компьютерной 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  
Oracle VM VirtualBox  
СУБД Mysql 8.0 совместно с Workbench  
СУБД RDBMS Oracle 11 R2

Учебные аудитории для проведения учебных занятий оснащены оборудованием:

1. доска для записей,
2. мебель (стулья, столы, парты),

технические средства обучения:

1. ноутбук,
2. мультимедийный проектор,
3. экран.

Учебные аудитории и помещения для самостоятельной работы для проведения учебных занятий оснащены оборудованием:

Помещения оснащены компьютерной техникой, обеспечивающей доступ к сети Интернет и электронной информационно-образовательной среде КНИТУ.

### **13. Образовательные технологии**

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Теоретические основы компьютерной безопасности» составляет 18 ч.

В процессе освоения дисциплины «Теоретические основы компьютерной безопасности» используются следующие образовательные технологии:

- работа в малых группах;
- системы дистанционного обучения.