Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по УР
А.В. Бурмистров
«01» 07 2019 г.

Р А Б О Ч А Я П Р О Г Р А М М А

По дисциплине Б1.В.ДВ.9.2 «Теория информационной безопасности»
Направление подготовки 20.03.01 «Техносферная безопасность»
Профиль подготовки Безопасность жизнедеятельности в техносфере
Квалификация (степень) выпускника бакалавр
Форма обучения заочная
Институт, факультет: КМИЦ «Новые технологии»
Кафедра-разработчик рабочей программы КМИЦ «Новые технологии»
Курс, семестр курс –3, семестр – 5,6

	Часы	Зачетные единицы
Лекции	4	0,11
Практические занятия	-	-
Семинарские занятия	-	-
Лабораторные занятия	-	-
Самостоятельная работа	28	0,78
Форма аттестации	Зачет (4)	0,11
Всего	36	1,0

Казань, 2019 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования № 246 от 21.03.2016 по направлению 20.03.01 «Техносферная безопасность», профиль подготовки «Безопасность жизнедеятельности в техносфере», на основании учебного плана набора обучающихся 2019 года.

Примерная программа по дисциплине отсутствует.

Разработчик программы:

_____	_____	М.Р. Вахитов
(должность)	(подпись)	(И.О.Ф.)

Рабочая программа рассмотрена и одобрена на заседании КМИЦ «Новые технологии»,

протокол от «07» 06 2019 г. № 6

Директор, профессор	_____	А.Ф. Махоткин
(должность)	(подпись)	(И.О.Ф.)

УТВЕРЖДЕНО

Протокол заседания методической комиссии КМИЦ «Новые технологии»
от «07» 06 2019 г. № 6

Председатель комиссии, профессор	_____	А.Ф. Махоткин
(должность)	(подпись)	(И.О.Ф.)

Начальник УМЦ	_____	Л.А. Китаева
(должность)	(подпись)	(И.О.Ф.)

1. Цели освоения дисциплины

Цель освоения дисциплины «Теория информационной безопасности» - дать студентам теоретические знания об основных принципах, методах и средствах защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

2. Место дисциплины в структуре образовательной программы (ОП)

Дисциплина «Теория информационной безопасности» относится к дисциплинам по выбору вариативной части ООП и формирует у бакалавров по направлению подготовки 20.03.01 «Техносферная безопасность» набор знаний, умений, навыков и компетенций, необходимых для выполнения научно-исследовательской деятельности.

Дисциплина «Теория информационной безопасности» бакалавр по направлению подготовки 20.03.01 «Техносферная безопасность» является вводной в проблематику информационной безопасности, поэтому требований к входным знаниям, умениям и компетенциям студента, необходимым для ее изучения, не предъявляется.

Дисциплина «Теория информационной безопасности» является предшествующей и необходима для успешного усвоения последующих дисциплин:

а) Б1.В.ОД.11 «Системы промышленной безопасности».

Знания, полученные при изучении дисциплины «Теория информационной безопасности», могут быть использованы при прохождении преддипломной практики и при выполнении выпускной квалификационной работы по направлению подготовки 20.03.01 «Техносферная безопасность», профиль «Безопасность жизнедеятельности в техносфере».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

1) Общеобразовательные компетенции (ОК):

ОК-3 - владением компетенциями гражданственности (знание и соблюдение прав и обязанностей гражданина, свободы и ответственности).

2) Профессиональные компетенции:

ПК-21 - способностью решать задачи профессиональной деятельности в составе научно-исследовательского коллектива.

В результате освоения дисциплины обучающийся должен:

1) Знать:

а) цели, задачи, принципы и основные направления обеспечения информационной безопасности государства;

б) основные термины по проблематике информационной безопасности;

в) перспективные направления развития средств и методов защиты информации;

г) роль и место информационной безопасности в системе национальной безопасности страны;

д) угрозы информационной безопасности государства;

е) содержание информационной войны, методы и средства ее ведения;

ж) современные подходы к построению систем защиты информации.

2) Уметь:

а) выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;

б) пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;

в) применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований.

3) Владеть:

а) навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

4. Структура и содержание дисциплины «Теория информационной безопасности»

Общая трудоемкость дисциплины составляет одну зачетную единицу, 36 академических часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)				Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Семинар (практические занятия)	Лабораторные работы	СРС	
1	Общие понятия безопасности информации	5	2	-	-	7	Тестирование
2	Информационная безопасность в системе национальной безопасности Российской Федерации	6	-	-	-	4	Тестирование
3	Информационная война, методы и средства ее ведения	6	-	-	-	4	Тестирование
4	Государственная информационная политика	6	-	-	-	4	Тестирование
5	Основные понятия теории информационной безопасности	6	2		-	9	Тестирование, контрольная работа
Форма аттестации			4	-	-	28	Зачет (4)

5. Содержание лекционных занятий по темам с указанием формируемых компетенций

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Формируемые компетенции

1	Общие понятия безопасности информации	2	Тема №1. Роль и место информации в современном мире. Понятие безопасности информации.	Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности. Понятие безопасности и её составляющие. Безопасность информации.	ОК-3 ПК-21
2	Информационная безопасность в системе национальной безопасности Российской Федерации	-	Тема №2. Угрозы в информационной сфере и принципы обеспечения информационной безопасности.	Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере.	ОК-3 ПК-21
		-	Тема №3. Информационная безопасность в системе национальной безопасности Российской федерации.	Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.	ОК-3 ПК-21
3	Информационная война, методы и средства ее ведения.	-	Тема №4. Цели, объекты воздействия и основные проблемы информационной войны. Информационное оружие и его классификация.	Понятие информационной войны. Проблемы информационной войны. Информационное оружие и его классификация. Цели информационной войны, её составные части и средства её ведения.	ОК-3 ПК-21
		-	Тема №5. Возможные пути реализации информационной войны в современном мире. Уровни ведения информационной войны.	Отражение информационной войны в нормативно – законодательной базе Российской Федерации. Возможные пути реализации информационной войны в современном мире.	ОК-3 ПК-21
4	Государственная информационная политика.	-	Тема №6. Государственная информационная политика и первоочередные мероприятия по её реализации.	Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.	ОК-3 ПК-21
		-	Тема №7. Системы	Задача устойчивого развития в информационной сфере	ОК-3 ПК-21

			информационного обеспечения органов государственного и муниципального управления, предприятий и организаций.	государственного и муниципального управления. Виды защищаемой информации в сфере государственного и муниципального управления. Обеспечение информационной безопасности организации.	
5	Основные понятия теории информационной безопасности.	1	Тема №8. Основные понятия и общеметодологические принципы теории информационной безопасности.	Управление и защита информации в информационно-телекоммуникационных сетях. Организация и ответственность в области управления информацией.	ОК-3 ПК-21
		1	Тема №9. Общие методы обеспечения информационной безопасности.	Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.	ОК-3 ПК-21

6. Содержание семинарских, практических занятий (лабораторного практикума)

Учебным планом программы проведение практических (семинарских) занятий по дисциплине «Теория информационной безопасности» не предусмотрено.

7. Содержание лабораторных занятий

Учебным планом программы проведение лабораторных занятий по дисциплине «Теория информационной безопасности» не предусмотрено.

8. Самостоятельная работа бакалавра

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Формируемые компетенции
1	Тема №1. Роль и место информации в современном мире. Понятие безопасности информации.	7	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
2	Тема №2. Угрозы в информационной сфере и принципы обеспечения информационной безопасности.	2	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
3	Тема №3. Информационная безопасность в системе национальной безопасности Российской федерации.	2	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21

4	Тема №4. Цели, объекты воздействия и основные проблемы информационной войны. Информационное оружие и его классификация.	2	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
5	Тема №5. Возможные пути реализации информационной войны в современном мире. Уровни ведения информационной войны.	2	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
6	Тема №6. Государственная информационная политика и первоочередные мероприятия по её реализации.	2	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
7	Тема №7. Системы информационного обеспечения органов государственного и муниципального управления, предприятий и организаций.	2	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
8	Тема №8. Основные понятия и общеметодологические принципы теории информационной безопасности.	4	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к тестированию.	ОК-3 ПК-21
9	Тема №9. Общие методы обеспечения информационной безопасности.	5	Изучение рекомендуемой литературы и сайтов сети Интернет. Подготовка к контрольной работе	ОК-3 ПК-21

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности студентов в рамках дисциплины «Теория информационной безопасности» используется рейтинговая система оценки знаний студентов на основании Положения ФГБОУ ВО «КНИТУ» от 04.09.2017 "О балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса".

По дисциплине предусмотрено тестирование и контрольная работа. За все эти виды работ студент может набрать 100 баллов, которые входят в семестровую составляющую, которые распределяются по возможности равномерно по всему семестру. Минимальное количество баллов – 60.

Оценочные средства	***Кол-во***	***Min, баллов***	***Max, баллов***
Тестирование	3	15*3=45	25*3=75
Контрольная работа	1	15	25
Итого:		60	100

Пересчет итоговой суммы баллов за семестр, где предусмотрен зачет, в традиционную и международную оценку

Оценка	***Итоговая сумма баллов***	***Оценка (ECTS)***
5 (отлично)	***87-100***	***A (отлично)***
4 (хорошо)	***83-86***	***B (очень хорошо)***
	78-82	***C (хорошо)***
	74-77	***D (удовлетворительно)***
3 (удовлетворительно)	***68-73***	
	60-67	***E (посредственно)***
2 (неудовлетвори-тельно),	***Ниже 60 баллов***	***F (неудовлетвори-тельно)***

После окончания семестра студент, набравший менее 60 баллов, считается неуспевающим, не получившим зачет. Возможна дополнительная сдача (пересдача) контрольных точек в дополнительные сроки, согласованные с деканатом.

10 Информационно-методическое обеспечение дисциплины

10.1 Основная литература

При изучении дисциплины «Теория информационной безопасности» в качестве основных источников информации, рекомендуется использовать следующую литературу:

Основные источники информации	Кол-во экз.
1. Мельников В.П. Информационная безопасность: учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. - Москва: Русайнс, 2016. - 354 с.	ЭБС «BOOK.ru» https://www.book.ru/book/920736 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
2. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — ISBN 978-5-94774-821-5.	ЭБС «IPR BOOKS» http://www.iprbookshop.ru/52209.html Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
3. Нестеров, С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва: Издательство Юрайт, 2019. — 321 с.	ЭБС «Юрайт» https://www.biblio-online.ru/bcode/434171 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
4. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=420047 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ

10.2 Дополнительная литература

В качестве дополнительных источников информации, рекомендуется использовать следующую литературу:

Дополнительные источники информации	Кол-во экз.
1. Москвитин Г.И. Комплексная защита информации в организации: монография / Г.И. Москвитин. - Москва: Русайнс, 2016. - 352 с.	ЭБС «BOOK.ru» https://www.book.ru/book/920774 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
2. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=495249 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=491597 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ

4. Бачило И.Л. Актуальные проблемы информационного права: учебник / И.Л. Бачило под. ред., М.А. Лапина под ред. - Москва: Юстиция, 2016. - 532 с.	ЭБС «BOOK.ru» https://www.book.ru/book/918541 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ

10.3 Электронные источники информации

При изучении дисциплины «Теория информационной безопасности» в качестве электронных источников информации, рекомендуется использовать следующие источники:

1. Электронный каталог УНИЦ КНИТУ – Режим доступа: https://ruslan.kstu.ru/
2. ЭБС «Znanium.com» – Режим доступа: http://znanium.com/
3. ЭБС «IPR BOOKS» - Режим доступа: http://www.iprbookshop.ru
4. ЭБС «BOOK.ru» - Режим доступа: https://www.book.ru/
5. ЭБС «Юрайт» - Режим доступа: https://www.biblio-online.ru/

10.4 Профессиональные базы данных и информационные справочные системы

1. Официальный сайт Президента РФ, http://www.kremlin.ru/acts
2. Официальный сайт Совет Безопасности Российской Федерации, http://www.scrf.gov.ru/
3. Официальный сайт ФСБ, http://www.fsb.ru/
4. Справочная правовая система «Гарант», http://www.garant.ru/iv/
5. Правовая справочно-поисковая система «Консультант Плюс», http://www.consultant.ru/about/software/cons/.

Согласовано:

Зав. сектором ОКУФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ» Учебно-научный информационный центр

Усольцева И.И.

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

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

12. Материально-техническое обеспечение дисциплины

По всем видам учебной деятельности в рамках дисциплины «Теория информационной безопасности» используются учебные аудитории для проведения занятий (лекционного типа, занятий лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной консультаций, текущего контроля и промежуточной аттестации), укомплектованные специализированной мебелью, оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Лицензированное, свободно распространяемое программное обеспечение, используемое в учебном процессе при освоении дисциплины «Теория информационной безопасности»:

-MS Office 2010-2016 Standard от 08.11.2016 No 16/2189/Б;

- Linux GNU General Public License.

13. Образовательные технологии

Удельный вес занятий по дисциплине «Теория информационной безопасности», проводимых в интерактивных формах, составляет 0 часов.