

Министерство науки и высшего образования Российской Федерации  
Нижекамский химико-технологический институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Казанский национальный исследовательский технологический университет»  
(НХТИ ФГБОУ ВО «КНИТУ»)



УТВЕРЖДАЮ

Заместитель директора по УР

Н.И. Никифорова

« 30 » мая 2022 г.

## РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.В.10 Криптографические методы защиты информации  
Направление подготовки 09.03.02 «Информационные системы и технологии»  
Профиль Системы информационной безопасности  
Квалификация выпускника бакалавр  
Форма обучения очная  
Факультет Информационных технологий  
Кафедра-разработчик рабочей программы Кафедра информационных систем и технологий  
Курс 3, семестр 6

Очная форма	Часы	Зачетные единицы
	6 семестр	6 семестр
Лекции	9	0,25
Практические занятия	-	-
Семинарские занятия	-	-
Лабораторные занятия	9	0,25
Контроль самостоятельной работы	72	2
Самостоятельная работа	54	1,5
Форма аттестации	Зачет с оценкой	
Всего	144	4

Нижнекамск, 2022 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования  
(№ 926 от 19.09.2017) по направлению 09.03.02

(номер, дата утверждения)

(шифр)

«Информационные системы и технологии»

(наименование направления)

на основании учебного плана набора обучающихся 2022 г.

Разработчик программы:

доцент

(должность)



(подпись)

Л.Р. Вотякова  
(Ф.И.О)

Рабочая программа рассмотрена и одобрена на заседании кафедры ИСТ,  
протокол от 20.04.2022 г. № 8

Зав. кафедрой



(подпись)

О.В. Матухина  
(Ф.И.О.)

### ***1. Цели освоения дисциплины***

Целями освоения дисциплины Б1.В.10 Криптографические методы защиты информации являются

- а) формирование знаний в области криптографии,
- б) обучение технологии использования криптографических методов для решения профессиональных задач,
- в) обучение способам применения криптографических методов защиты информации,
- г) раскрытие сущности процессов, происходящих в криптографических методах защиты информации.

### ***2. Место дисциплины (модуля) в структуре основной образовательной программы***

Дисциплина Б1.В.10 Криптографические методы защиты информации относится к формируемой участниками образовательных отношений части ООП и формирует у бакалавров по направлению подготовки 09.03.02 Информационные системы и технологии набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины бакалавр по направлению подготовки 09.03.02 Информационные системы и технологии должен освоить материал предшествующих дисциплин:

Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности,

Б1.В.07 Основы информационной безопасности.

Знания, полученные при изучении дисциплины, Б1.В.10 Криптографические методы защиты информации могут быть использованы при прохождении дисциплин:

Б1.В.16 Безопасность программного обеспечения,

Б1.В.17 Методы и средства защиты информационных систем критичных отраслей,

а также при прохождении практик и выполнении выпускной квалификационной работы.

### ***3. Компетенции и индикаторы достижения компетенции обучающегося, формируемые в результате освоения дисциплины***

ПК-2.1 Знает угрозы безопасности баз данных, способы предотвращения

ПК-2.2 Умеет выявлять угрозы безопасности на уровне баз данных

ПК-2.3 Владеет навыками применения способов предотвращения угроз безопасности на уровне баз данных

***В результате освоения дисциплины обучающийся должен:***

1) Знать:

основания криптографической защиты информации в организации;

основные понятия и требования криптографической защиты информации

2) Уметь:

выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации;

выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;

3) Владеть:

навыками определения криптографической стойкости шифрсистем;

навыками обоснования выбора криптографических средств для защиты информации

**4. Структура и содержание дисциплины Б1.В.10 Криптографические методы защиты информации.** Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

### Очная форма

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практ. занятия	Лаборатор. работы	КСР	СРС	
1	Математические основы криптографии.	6	2	-	1	16	14	Лабораторная работа №1 Вопросы к зачету
2	Классификация шифров по различным признакам	6	1	-	2	14	10	Лабораторная работа №2 Вопросы к зачету
3	Шифры перестановки	6	2	-	2	14	10	Лабораторная работа №3 Вопросы к зачету
4	Шифры замены	6	2	-	2	14	10	Лабораторная работа №4 Вопросы к зачету
5	Шифры гаммирования	6	2	-	2	14	10	Лабораторная работа №5 Вопросы к зачету
<b>ИТОГО</b>		<b>108</b>	<b>9</b>	<b>-</b>	<b>9</b>	<b>72</b>	<b>54</b>	
<b>Форма аттестации</b>								<b>Зачет с оценкой</b>

**5. Содержание лекционных занятий по темам с указанием формируемых компетенций**

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Индикаторы достижения компетенции
1.	Математические основы	2	1. Основные понятия криптографии	Операции над множествами. Бинарные отношения на множестве. Бинарные операции на множестве. Алгебраические структуры.	ПК-2.1, ПК-2.2, ПК-2.3



	крипто- графии.			Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.	
2.	Классификация шифров по различным признакам	1	2. Классификация шифров замены	Математическая модель шифра простой замены.	ПК-2.1, ПК-2.2, ПК-2.3
3.	Шифры перестановки	2	3. Маршрутные перестановки.	Элементы криптоанализа шифров перестановки.	ПК-2.1, ПК-2.2, ПК-2.3
4.	Шифры замены	2	4. Поточные шифры простой замены.	Элементы криптоанализа поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Многоалфавитные шифры замены.	ПК-2.1, ПК-2.2, ПК-2.3
5.	Шифры гаммирования	2	5. Табличное гаммирование.	О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Элементы криптоанализа шифра Виженера. Ошибки шифровальщика.	ПК-2.1, ПК-2.2, ПК-2.3

## 6. Содержание практических занятий

Не предусмотрено учебным планом

## 7. Содержание лабораторных занятий

Целью проведения лабораторных занятий является закрепление теоретического материала по дисциплине и развитие навыков самостоятельной работы.

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1	Математические основы криптографии.	1	1. Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации	ПК-2.1, ПК-2.2, ПК-2.3
2	Классификация шифров по различным признакам	2	2. Криптоанализ шифра простой замены	ПК-2.1, ПК-2.2, ПК-2.3
3	Шифры перестановки	2	3. Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами	ПК-2.1, ПК-2.2, ПК-2.3
4	Шифры замены	2	4. Шифры многобуквенной замены на примере шифра Хилла	ПК-2.1, ПК-2.2, ПК-2.3

5	Шифры гаммирования	2	5. Шифр гаммирования	ПК-2.1, ПК-2.2, ПК-2.3
---	--------------------	---	----------------------	------------------------

Место проведения: учебные лаборатории кафедры без использования специального оборудования.

### **8. Самостоятельная работа**

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1.	Математические основы криптографии.	14	текущая работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, выполнение лабораторной работы №1, подготовка к зачету	ПК-2.1, ПК-2.2, ПК-2.3
2.	Классификация шифров по различным признакам	10	текущая работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, выполнение лабораторной работы №2, подготовка к зачету	ПК-2.1, ПК-2.2, ПК-2.3
3.	Шифры перестановки	10	текущая работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, выполнение лабораторной работы №3, подготовка к зачету	ПК-2.1, ПК-2.2, ПК-2.3
4.	Шифры замены	10	текущая работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, выполнение лабораторной работы №4, подготовка к зачету	ПК-2.1, ПК-2.2, ПК-2.3
5.	Шифры гаммирования	10	текущая работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, выполнение лабораторной работы №5, подготовка к зачету	ПК-2.1, ПК-2.2, ПК-2.3

### **8.1 Контроль самостоятельной работы**

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	Математические основы криптографии.	16	Проверка лабораторных работ, консультирование	ПК-2.1, ПК-2.2, ПК-2.3
2	Классификация шифров по различным признакам	14	Проверка лабораторных работ, консультирование	ПК-2.1, ПК-2.2, ПК-2.3
3	Шифры перестановки	14	Проверка лабораторных работ, консультирование	ПК-2.1, ПК-2.2, ПК-2.3
4	Шифры замены	14	Проверка лабораторных работ, консультирование	ПК-2.1, ПК-2.2, ПК-2.3

5	Шифры гаммирования	14	Проверка лабораторных работ, консультирование	ПК-2.1, ПК-2.2, ПК-2.3
---	--------------------	----	---	------------------------

### **9. Использование рейтинговой системы оценки знаний**

При оценке результатов деятельности обучающихся в рамках дисциплины «Б1.В.10 Криптографические методы защиты информации» используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. 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».

При изучении дисциплины предусматривается зачет, выполнение лабораторных работ. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

#### **Очная форма**

№	Оценочные средства	Min, баллов (базовый уровень)	Max, баллов (повышенный уровень)
1	Лабораторная работа №1	7	12
2	Лабораторная работа №2	7	12
3	Лабораторная работа №3	7	12
4	Лабораторная работа №4	7	12
5	Лабораторная работа №5	8	12
	<b>Текущий рейтинг</b>	<b>36</b>	<b>60</b>
	<b>Сдача зачета</b>	<b>24</b>	<b>40</b>
	<b>Рейтинг по дисциплине</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 обучающихся и итоговой (государственной 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 «Б1.В.10 Криптографические методы защиты информации» в качестве основных источников информации рекомендуется использовать следующую литературу.

Основные источники информации	Кол-во экз.
1. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский	ЭБС «Znanium» <a href="https://znanium.com/c">https://znanium.com/c</a>

юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1094244">https://znanium.com/catalog/product/1094244</a> . - Режим доступа: по подписке.	<a href="https://znanium.com/catalog/product/1094244">ata-log/document?id=358668</a> . Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
2. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст: электронный.-URL: <a href="https://znanium.com/catalog/product/1864501">https://znanium.com/catalog/product/1864501</a> . - Режим доступа: по подписке.	ЭБС «Znanium» <a href="https://znanium.com/catalog/product/1864501">https://znanium.com/catalog/product/1864501</a> . Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
3. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мещатунян. — Москва : ФОРУМ : ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/">https://znanium.com/catalog/product/</a> . - Режим доступа: по подписке.	ЭБС «Znanium» <a href="https://znanium.com/catalog/product/1189337">https://znanium.com/catalog/product/1189337</a> . Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
4. Полуэктова, Н. Р. Разработка веб-приложений : учебное пособие для вузов / Н. Р. Полуэктова. — Москва : Издательство Юрайт, 2021. — 204 с. — (Высшее образование). — ISBN 978-5-534-13715-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/466449">https://urait.ru/bcode/466449</a> / Гриф УМО ВО	ЭБС «Юрайт» <a href="https://urait.ru/bcode/466449">https://urait.ru/bcode/466449</a> Доступ с любой точки Интернет после регистрации IP-адреса НХТИ

## 11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Кол-во экз.
1. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/468473">https://urait.ru/bcode/468473</a> / Гриф УМО ВО	ЭБС «Юрайт» <a href="https://urait.ru/bcode/468473">https://urait.ru/bcode/468473</a> Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
2. Алексеев, А. П. Курсовое проектирование для криптографов : учебное пособие / А. П. Алексеев. - Москва : СОЛОН-Пресс, 2020. - 100 с. - ISBN 978-5-91359-314-6. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1858779">https://znanium.com/catalog/product/1858779</a> . - Режим доступа: по подписке.	ЭБС «Znanium» : <a href="https://znanium.com/catalog/product/1858779">https://znanium.com/catalog/product/1858779</a> Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
3. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1819309">https://znanium.com/catalog/product/1819309</a> . - Режим доступа: по подписке.	ЭБС «Znanium» : <a href="https://znanium.com/catalog/product/1819309">https://znanium.com/catalog/product/1819309</a> Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
4. Шишов, О. В. Современные технологии и технические средства информатизации : учебник / О.В. Шишов. —	ЭБС «Znanium» : <a href="https://znanium.com/catalog/product/">https://znanium.com/catalog/product/</a>



Москва : ИНФРА-М, 2021. — 462 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011776-8. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1215864">https://znanium.com/catalog/product/1215864</a> – Режим доступа: по подписке.	<a href="https://znanium.com/catalog/product/1215864">og/product/1215864</a> Доступ с любой точки Интернет после регистрации IP-адреса НХТИ
--	---

### ***11.3. Электронные источники информации***

При изучении дисциплины «Б1.В.10 Криптографические методы защиты информации» в качестве электронных источников информации, рекомендуется использовать следующие источники:

1. ЭБС «Юрайт» – Режим доступа: <https://urait.ru>
2. ЭБС «Znanium» – Режим доступа: <https://znanium.com>

### ***11.4. Современные профессиональные базы данных и информационные справочные системы.***

1. Журнал «Математические вопросы криптографии». Сайт журнала. – Доступ свободный: [http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option\\_lang=rus](http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option_lang=rus).

2. Журнал «Информационные технологии и системы». Сайт журнала. – Доступ свободный: <https://itsys.tb.ru>.

#### **Согласовано:**

Зав. отделом  
по библиотечному  
обслуживанию



В.Я.Тарасова

### ***12. Материально-техническое обеспечение дисциплины (модуля)***

Учебные аудитории (228В ауд., 230В ауд.) для проведения учебных (лекционных и лабораторных) занятий оснащена оборудованием:

1. Доступ к электронной информационно-образовательной среде вуза
2. Схемы и стенды для проведения лабораторных практикумов

Техническими средствами обучения: интерактивная доска; проектор, столы, стулья.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду НХТИ. Допускается замена оборудования его виртуальными аналогами.

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, используемое в учебном процессе при освоении дисциплины: NotePad, MicrosoftOffice.

Электронный читальный зал (кабинет для самостоятельной работы студентов, групповых и индивидуальных консультаций). Оснащение помещения: столы, стулья, персональные компьютеры с выходом в Интернет, принтер, сканер, ксерокс.

### ***13. Образовательные технологии***

### Очная форма

Тема	Вид занятия	Интерактивная форма	Часы
Операции над множествами. Бинарные отношения на множестве. Бинарные операции на множестве. Алгебраические структуры. Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.	Лекция	Лекция-визуализация	2
Элементы криптоанализа шифров перестановки.	Лекция	Лекция-визуализация	2
Элементы криптоанализа поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Многоалфавитные шифры замены.	Лабораторное занятие	Работа в малых группах	5
Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Элементы криптоанализа шифра Виженера. Ошибки шифровальщика.	Лабораторное занятие	Работа в малых группах	5
<b>ИТОГО</b>			<b>14</b>