

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.16 Безопасность программного обеспечения  
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 4, семестр 7

Очная форма	Часы	Зачетные единицы
	7 семестр	7 семестр
Лекции	9	0,25
Практические занятия	-	-
Семинарские занятия	-	-
Лабораторные занятия	27	0,75
Контроль самостоятельной работы	54	1,5
Самостоятельная работа	54	1,5
Форма аттестации	Зачет с оценкой	-
Всего	144	4

Нижекамск, 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.16 Безопасность программного обеспечения являются

а) изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

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.16 Безопасность программного обеспечения 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.04 Теория информации и кодирования,

Б1.В.07 Основы информационной безопасности

Б1.В.10 Криптографические методы защиты информации

Б1.В.15 Интеллектуальные информационные системы

Знания, полученные при изучении дисциплины, Б1.В.16 Безопасность программного обеспечения могут быть использованы при прохождении дисциплин:

Б1.В.20 Проектирование и разработка защищенных автоматических систем,

а также при прохождении практик и выполнении выпускной квалификационной работы.

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

ПК-1 Способен разрабатывать требования и проектировать программное обеспечение:

ПК-1.1 Знает методы и средства проектирования программного обеспечения, баз данных, программных интерфейсов;

ПК-1.2 Умеет применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов;

ПК-1.3 Владеет навыками применения методов и средств проектирования программного обеспечения, структур данных, базы данных, программных

интерфейсов;

ПК-2 Способен обеспечить информационную безопасность на уровне баз данных:

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:

средства и методы предотвращения и обнаружения вторжений;

технические каналы утечки информации;

возможности технических средств перехвата информации;

способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

организацию защиты информации от утечки по техническим каналам на объектах информатизации;

2) Уметь:

пользоваться нормативными документами по противодействию технической разведке;

оценивать качество готового программного обеспечения;

3) Владеть:

методами и средствами технической защиты информации;

методами расчета и инструментального контроля показателей технической защиты информации.

**4. Структура и содержание дисциплины** Б1.В.16 Безопасность программного обеспечения. 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	Введение в теорию обеспечения безопасности программного обеспечения	7	3	-	8	14	14	Лабораторная работа №1
2	Обеспечение технологической безопасности программного обеспечения	7	2	-	8	14	14	Лабораторная работа №2
3	Обеспечение эксплуатационной безопасности программного обеспечения.	7	2	-	6	13	13	Лабораторная работа №3



4	Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Человеческий фактор.	7	2	-	5	13	13	Лабораторная работа №4
<b>ИТОГО</b>		<b>144</b>	<b>9</b>	<b>-</b>	<b>27</b>	<b>54</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.	Введение в теорию обеспечения безопасности программного обеспечения	3	Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире.	Базовые научные дисциплины, принятая аксиоматика и терминология. Жизненный цикл программного обеспечения компьютерных систем. Технологическая и эксплуатационная безопасность программ. Модель угроз и принципы обеспечения безопасности программного обеспечения.	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
2.	Обеспечение технологической безопасности программного обеспечения	2	Формальные методы доказательства правильности программ и их спецификаций.	Методы и средства анализа безопасности программного обеспечения. Методы обеспечения надежности программ для контроля их технологической безопасности. Методы создания алгоритмически безопасных процедур. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок. Методы идентификации программ и их характеристик.	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
3.	Обеспечение эксплуатационной безопасности программного обеспечения.	2	Методы и средства защиты программ от компьютерных вирусов.	Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок. Методы и средства обеспечения целостности и достоверности используемого программного кода. Основные подходы к защите программ от несанкционированного копирования.	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
4.	Правовая и организационная поддержка	2	Стандарты и другие нормативные документы, регламентирующие защищен-	Сертификационные испытания программных средств. Безопасность программного обеспечения и человеческий фактор. Психоло-	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3

процессов разработки и применения программного обеспечения. Человеческий фактор.		ность программного обеспечения и обрабатываемой информации.	гия программирования.	
--	--	---	-----------------------	--

## **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.

<b>№ п/п</b>	<b>Раздел дисциплины</b>	<b>Часы</b>	<b>Наименование лабораторной работы</b>	<b>Индикаторы достижения компетенции</b>
1	Введение в теорию обеспечения безопасности программного обеспечения	8	Использование классических криптоалгоритмов подстановки	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
2	Обеспечение технологической безопасности программного обеспечения	8	Криптоанализ шифра простой замены	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
3	Обеспечение эксплуатационной безопасности программного обеспечения.	6	Шифрование данных методами подстановки	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
4	Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Человеческий фактор.	5	Шифры многобуквенной замены	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3

Место проведения: учебные лаборатории кафедры без использования специального оборудования.

## **8. Самостоятельная работа**

<b>№ п/п</b>	<b>Темы, выно- симые на самостоя- тельную работу</b>	<b>Часы</b>	<b>Форма СРС</b>	<b>Индикаторы достижения компетенции</b>
1.	Введение в теорию обеспечения безопасности программного обеспечения	5	текущая работа с лекционным матери- алом, предусматривающая проработку конспекта лекций и учебной литерату- ры, выполнение лабораторной работы №1, подготовка к зачету	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
2.	Обеспечение тех- нологической без- опасности про- граммного обеспечения	5	текущая работа с лекционным матери- алом, предусматривающая проработку конспекта лекций и учебной литерату- ры, выполнение лабораторной работы №2, подготовка к зачету	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
3.	Обеспечение экс- плуатационной безопасности про- граммного обеспе- чения.	4	текущая работа с лекционным матери- алом, предусматривающая проработку конспекта лекций и учебной литерату- ры, выполнение лабораторной работы №3, подготовка к зачету	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
4.	Правовая и орга- низационная под- держка процессов разработки и при- менения про- граммного обеспе- чения. Человеческий фак- тор.	4	текущая работа с лекционным матери- алом, предусматривающая проработку конспекта лекций и учебной литерату- ры, выполнение лабораторной работы №4, подготовка к зачету	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3

### ***8.1 Контроль самостоятельной работы***

<b>№ п/п</b>	<b>Темы, выносимые на самостоятель- ную работу</b>	<b>Часы</b>	<b>Форма КСР</b>	<b>Индикаторы достижения компетенции</b>
1	Введение в теорию обеспечения безопасности программного обеспечения	5	Проверка лабораторных работ, кон- сультирование	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
2	Обеспечение техно- логической безопас- ности программного обеспечения	5	Проверка лабораторных работ, кон- сультирование	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
3	Обеспечение экс- плуатационной без- опасности про- граммного обеспечения.	4	Проверка лабораторных работ, кон- сультирование	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
4	Правовая и органи- зационная поддерж- ка процессов разра- ботки и применения программного обес-	4	Проверка лабораторных работ, кон- сультирование	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3

	печения. Человеческий фактор.		
--	-------------------------------	--	--

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

При оценке результатов деятельности обучающихся в рамках дисциплины «Б1.В.16 Безопасность программного обеспечения» 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**

<b>№</b>	<b>Оценочные средства</b>	<b>Min, баллов (базовый уровень)</b>	<b>Max, баллов (повышенный уровень)</b>
1	Лабораторная работа №1	9	15
2	Лабораторная работа №2	9	15
3	Лабораторная работа №3	9	15
4	Лабораторная работа №4	9	15
	<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.16 Безопасность программного обеспечения» в качестве основных источников информации рекомендуется использовать следующую литературу.

<b>Основные источники информации</b>	<b>Кол-во экз.</b>
1. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-	ЭБС «Znanium» <a href="https://znanium.com/catalog/document?id=3">https://znanium.com/catalog/document?id=3</a>



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="#">58668</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/186450">https://znanium.com/catalog/product/186450</a> 1. 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/118933">https://znanium.com/catalog/product/118933</a> 7. 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> 73 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. — Москва : ИНФРА-М, 2021. — 462 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011776-8. - Текст : электрон-	ЭБС «Znanium» : <a href="https://znanium.com/catalog/product/1215864">https://znanium.com/catalog/product/1215864</a> Доступ с любой точки Интернет после регистра-

ный. - URL: <a href="https://znanium.com/catalog/product/1215864">https://znanium.com/catalog/product/1215864</a> – Режим доступа: по подписке.	ции IP-адреса НХТИ
--	--------------------

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

При изучении дисциплины «Б1.В.10 Криптографические методы защиты информации» в качестве электронных источников информации, рекомендует-ся 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***

Количество занятий, проводимых в интерактивных формах, для очной формы обучения – 20 ак.час.

Применяются системы дистанционного обучения, онлайн-формы консультаций, обсуждений, презентаций, докладов и защит результатов работ.