

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

2022 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.В.07 Основы информационной безопасности

Направление подготовки 09.03.02 «Информационные системы и технологии»

Профиль/программа Системы информационной безопасности

Квалификация (степень) выпускника бакалавр

Форма обучения очная

Факультет Информационных технологий

Кафедра-разработчик рабочей программы информационных систем и технологий

Очное: курс - 3, семестр – 5

	Часы	Зачетные единицы
Лекции	18	0,5
Практические занятия	-	-
Лабораторные занятия	36	1
Контроль самостоятельной работы	54	1,5
Самостоятельная работа	36	1
Форма аттестации (часы на контроль)	Зачёт 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:

Ст. преподаватель

(должность)



(подпись)

Захарова И.Н.

(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.07 Основы информационной безопасности являются

- а) формирование знаний о методах, средствах защиты программ и данных от различных типов угроз;
- б) обучение технологии получения анализа состояния защищенности информации, выбора, построения и анализа показателей защищенности программно-аппаратных средств защиты информации;
- в) обучение применению программных и аппаратных средств защиты информации;
- г) раскрытие сущности теории защиты информации.

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

Дисциплина Б1.В.07 Основы информационной безопасности относится к обязательной 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 Б1.В.07 Основы информационной безопасности *бакалавр по* направлению подготовки 09.03.02 «Информационные системы и технологии» должен освоить материал предшествующих дисциплин:

- а) Б1.О.20 Основы информатики и кибернетики;
- б) Б1.О.23 Системы управления базами данных;
- в) Б1.О.25 Программирование на языке высокого уровня;
- г) Б1.В.05 Языки программирования общего назначения;
- д) Б1.В.04 Теория информации и кодирования;

Дисциплина является предшествующей и необходима для успешного усвоения последующих дисциплин:

- а) Б1.В.10 Криптографические методы защиты информации;
- б) Б1.В.16 Безопасность программного обеспечения;
- в) Б1.В.18 Управление информационным пространством;
- г) Б1.В.20 Проектирование и разработка защищённых автоматизированных систем;
- д) Б1.В.21 Киберфизические системы;
- е) Б1.В.23 Технологии проектирования программного обеспечения;
- ж) Б1.В.ДВ.01.01 Разработка приложений в среде 1С
- з) Б1.В.ДВ.03.01 Моделирование объектов, процессов и систем.

Знания, полученные при изучении дисциплины, Б1.В.07 Основы информационной безопасности могут быть использованы при прохождении практик и выполнении выпускной квалификационной работы.

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

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:

- а) принципы работы современных информационных технологий и программных средств, при решении задач защиты информации;*
- б) принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.*
- в) методики использования программных средств для решения практических задач защиты информации;*
- г) угрозы безопасности и способы предотвращения.*

2) Уметь:

- а) решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности*
- б) выявлять угрозы информационной безопасности.*

3) Владеть:

- а) навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;*
- б) навыками применения способов предотвращения угроз информационной безопасности;*
- в) навыками использования программных средств для решения практических задач защиты информации.*

4. Структура и содержание дисциплины Б1.В.07 Основы информационной безопасности

Общая трудоемкость дисциплины составляет 4_зачетных единиц, 144 часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практические занятия	Лабораторные работы	КСР	СРС	
1	Информационная безопасность в системе национальной безопасности РФ	7	8	-	12	26	12	Тестирование
2	Угрозы информационной безопасности	7	4	-	16	14	16	Тестирование
3	Обеспечение информационной безопасности компьютерных систем	7	6	-	4	14	10	Тестирование, подготовка реферата
ИТОГО			18		36	54	36	
Форма аттестации					Зачёт с оценкой(27)			

5. Содержание лекционных занятий по темам с указанием формируемых компетенций

№	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Индикаторы достижения компетенции
1	Информационная безопасность в системе национальной безопасности РФ	8	Национальная безопасность РФ	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Национальные интересы РФ и стратегические национальные приоритеты. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.	ПК – 2.1

			Угрозы безопасности РФ в информационной сфере.	Основные составляющие национальных Интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.	
			Основные понятия теории информационной безопасности.	Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности.	
			Понятие и виды защищаемой информации.	Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.	
2	Угрозы информационной безопасности	4	Понятие и виды угроз информационной безопасности	Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации	ПК – 2.1
			Обеспечение информационной безопасности	Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной противоборства. Компью-	

				терная система как объект информационного противоборства.	
3	Обеспечение информационной безопасности компьютерных систем	6	Методы и средства обеспечения информационной безопасности компьютерных систем	Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.	ПК – 2.1
			Модели политик безопасности	Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадуды. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности Ролевое управление доступом.	

6. Содержание практических занятий

Не предусмотрено

7. Содержание лабораторных занятий

Цель: получить навыки работы с компьютером по защите информации, овладеть методами информационных технологий по информационной безопасности информационных систем.

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1.	Информационная безопасность в системе национальной безопасности РФ	4	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	ПК – 2.1-2.3
2.	Угрозы информационной безопасности	4	Основные понятия и общеметодологические принципы теории информационной безопасности	ПК – 2.1-2.3
3.		4	Понятие и виды защищаемой информации	ПК – 2.1-2.3
4.		4	Понятие и виды угроз информационной безопасности	ПК – 2.1-2.3
5.		4	Обеспечение конфиденциальности	ПК – 2.1-2.3
6.		4	Обеспечение целостности	ПК – 2.1-2.3
7.		4	Обеспечение доступности	ПК – 2.1-2.3
8.	Обеспечение	4	Реализация политик информационной безопасности. Дискреционная модель безопасности	ПК – 2.1-2.3

9.	информацион- ной безопасно- сти компьютер- ных систем	4	Реализация политик информационной безопасности. Мандатная и ролевая модели безопасности	ПК – 2.1-2.3
----	--	---	--	--------------

8. Самостоятельная работа

№ п/п	Темы, выносимые на само- стоятельную работу	Часы	Форма СРС	Индика- торы дости- жения ком- петенции
1.	Национальная безопасность РФ	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
2.	Угрозы безопасности РФ в информационной сфере.	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
3.	Основные понятия теории информационной безопасно- сти.	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
4.	Понятие и виды защищае- мой информации.	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
5.	Понятие и виды угроз ин- формационной безопасности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
6.	Обеспечение информацион- ной безопасности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
7.	Методы и средства обеспе- чения информационной без- опасности компьютерных систем	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
8.	Модели политик безопасно- сти	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
9.	Основы государственной по- литики и угрозы безопасно- сти Российской Федерации в информационной сфере	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
10.	Основные понятия и обще- методологические принципы теории информационной без- опасности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
11.	Понятие и виды защищаемой информации	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
12.	Понятие и виды угроз инфор- мационной безопасности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
13.	Обеспечение конфиденци- альности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
14.	Обеспечение целостности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3

15.	Обеспечение доступности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
16.	Реализация политик информационной безопасности. Дискреционная модель безопасности	2	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3
17.	Реализация политик информационной безопасности. Мандатная и ролевая модели безопасности	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1.	Национальная безопасность РФ	5	консультирование	ПК – 2.1-2.3
2.	Угрозы безопасности РФ в информационной сфере.	7	консультирование	ПК – 2.1-2.3
3.	Основные понятия теории информационной безопасности.	7	консультирование	ПК – 2.1-2.3
4.	Понятие и виды защищаемой информации.	7	консультирование	ПК – 2.1-2.3
5.	Понятие и виды угроз информационной безопасности	7	консультирование	ПК – 2.1-2.3
6.	Обеспечение информационной безопасности	7	консультирование	ПК – 2.1-2.3
7.	Методы и средства обеспечения информационной безопасности компьютерных систем	7	консультирование	ПК – 2.1-2.3
8.	Модели политик безопасности	7	консультирование	ПК – 2.1-2.3

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины Б1.В.07 Основы информационной безопасности 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 реферат, тестирование. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

За экзамен студент может получить минимум 24 балла и максимум – 40 баллов.

Оценочные средства	Кол-во	Min, баллов	Max, баллов
--------------------	--------	-------------	-------------

Реферат	1	20	40
Тестирование	1	40	60
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 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.07 Основы информационной безопасности в качестве основных источников информации рекомендуется использовать следующую литературу.

Основные источники информации	Кол-во экз.
1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3 . - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523). — Режим доступа: по подписке.	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711 . — Режим доступа: по подписке.	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
3 Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6 . - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 . — Режим доступа: по подписке., по паролю. — ЭБС «Znanium», УМО	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 . — Режим доступа: по подписке., по паролю. — ЭБС «Znanium» УМО	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)

5. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование: Бакалавриат). www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1784437 . — Режим доступа: по подписке. — ЭБС «Znanium» УМО	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
--	---

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Кол-во экз.
1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие. - М.-Берлин: Директ-Медиа, 2015. - 253 с. Режим доступа, по паролю. — ЭБС «Книгафонд»	1 (безлимитный доступ к ЭБС «Книгафонд» после регистрации с IP-адреса НХТИ)

11.3. Электронные источники информации

При изучении дисциплины Б1.В.07 Основы информационной безопасности использование электронных источников информации:

Федеральный портал «Российское образование» http://www.edu.ru/	Открытый Интернет-ресурс, свободный безлимитный доступ.
Федеральный центр информационно-образовательных ресурсов http://fcior.edu.ru/	Электронные образовательные ресурсы и сервисы для всех уровней и ступеней образования. Открытый Интернет-ресурс, свободный безлимитный доступ.
Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/	Российское образование: единое окно доступа к образовательным ресурсам, свободный безлимитный доступ.

11.4. Современные профессиональные базы данных и информационные справочные системы.

1. Журнал «Информационные технологии». Сайт журнала. — Доступ свободный: <http://novtex.ru/IT/>.

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

3. Базы данных правовой информации, информационно-справочные и поисковые системы - «Гарант» - www.garant.ru; - Информационно-справочная система «Консультант Плюс».

Согласовано:

Зав. отделом
по библиотечному
обслуживанию

Тарасова В.Я.

12. Материально-техническое обеспечение дисциплины (модуля).

«Компьютерный класс 115В»

Учебная аудитория для проведения учебных занятий оснащена оборудованием:

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

Техническими средствами обучения:

1. Интерактивная доска;
2. Проектор

Помещения для самостоятельной работы оснащены компьютерной техникой в количестве 15 шт. 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:

Microsoft Office

13. Образовательные технологии

Тема	Вид занятия	Интерактивная форма	часы
Национальная безопасность РФ	Лекция	Вводная лекция, лекция визуализация	1
Угрозы безопасности РФ в информационной сфере.	Лекция	лекция визуализация	1
Основные понятия теории информационной безопасности.	Лекция	лекция визуализация	1
Понятие и виды защищаемой информации.	Лекция	лекция визуализация	1
Понятие и виды угроз информационной безопасности	Лекция	лекция визуализация	1
Обеспечение информационной безопасности	Лекция	лекция визуализация	1
Методы и средства обеспечения информационной безопасности компьютерных систем	Лекция	лекция визуализация	1
Модели политик безопасности	Лекция	лекция визуализация	1
Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	Лаб.зан	Работа в малых группах, метод проектов	1
Основные понятия и общеметодологические принципы теории информационной безопасности	Лаб.зан	Работа в малых группах, метод проектов	1
Понятие и виды защищаемой информации	Лаб.зан	Работа в малых группах, метод проектов	1
Понятие и виды угроз информационной безопасности	Лаб.зан	Работа в малых группах, метод проектов	0.5

Обеспечение конфиденциальности	Лаб.зан	Работа в малых группах, метод проектов	0.5
Обеспечение целостности	Лаб.зан	Работа в малых группах, метод проектов	0.5
Обеспечение доступности	Лаб.зан	Работа в малых группах, метод проектов	0.5
Реализация политик информационной безопасности. Дискреционная модель безопасности	Лаб.зан	Работа в малых группах, метод проектов	0.5
Реализация политик информационной безопасности. Мандатная и ролевая модели безопасности	Лаб.зан	Работа в малых группах, метод проектов	0.5
Итого:			14