

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.17 Методы и средства защиты информационных систем критичных отраслей

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 - 4, семестр – 7

	Часы	Зачетные единицы
Лекции	9	0,25
Практические занятия	-	-
Лабораторные занятия	27	0,75
Контроль самостоятельной работы	45	1,75
Самостоятельная работа	36	1
Форма аттестации (часы на контроль)	Экзамен (27)	0,75
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.17 Методы и средства защиты информационных систем критичных отраслей 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.17 Методы и средства защиты информационных систем критичных отраслей относится к вариативной 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.17 Методы и средства защиты информационных систем критичных отраслей 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;
- е) Б1.О.07 Основы информационной безопасности
- ж) Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности
- з) Б1.В.10 Криптографические методы защиты информации;

Дисциплина является предшествующей и необходима для успешного усвоения последующих дисциплин:

- а) Б1.В.20 Проектирование и разработка защищённых автоматизированных систем;
- б) Б1.В.21 Киберфизические системы;
- в) Б1.В.23 Технологии проектирования программного обеспечения.

Знания, полученные при изучении дисциплины, Б1.В.17 Методы и средства защиты информационных систем критичных отраслей 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

ПК-4 Способен обслуживать сетевые устройства информационно-коммуникационной системы

ПК-4.1 Знает общие принципы функционирования аппаратных, программных и программно-аппаратных средств информационно-коммуникационной системы

ПК-4.2 Умеет разрабатывать планы резервного копирования, архивирования и восстановления конфигураций сетевых устройств информационно-коммуникационных систем

ПК-4.3 Владеет навыками обновления программного обеспечения сетевых устройств информационно-коммуникационных систем

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) общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети*
- д) угрозы безопасности и способы предотвращения.*

2) Уметь:

- а) решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;*
- б) использовать современные средства администрирования баз данных*
- в) 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 администрирования сетевой системы и программного обеспечения инфокоммуникационной системы
- в) навыками применения способов предотвращения угроз информационной безопасности;
- г) навыками использования программных средств для решения практических задач защиты информации.

4. Структура и содержание дисциплины Б1.В.17 Методы и средства защиты информационных систем критичных отраслей

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 критических систем информационной инфраструктуры в системе национальной безопасности РФ	7	3	-	7	15	12	Тестирование
2	Модели систем защиты информации	7	3	-	8	15	12	Тестирование
3	Обеспечение информационной безопасности критичных отраслей	7	3	-	12	15	12	Тестирование, подготовка реферата
ИТОГО			9		27	45	36	
Форма аттестации					Экзамен (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 критических систем информационной инфраструктуры в системе национальной безопасности РФ	3	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, 4.1

			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.	
2	Модели систем защиты	3	СЗИ от угроз нарушения конфиденциальности	Модель системы защиты. Организационные меры информационной безопасности. Идентификация, авторизация, аутентификация. Методы аутентификации. Разграничение доступа (дискреционный, мандатный). Криптографические методы обеспечения конфиденциальности (симметричные, асимметричные криптосистемы). Методы защиты внешнего периметра (Межсетевое экранирование, системы обнаружения вторжений). Протоколирование и аудит.	ПК – 2.1, 4.1
			СЗИ от угроз нарушения целостности.	Принципы обеспечения целостности. Криптографические методы обеспечения целостности информации (цифровая подпись, криптографические хэш-функции, коды проверки подлинности).	
			СЗИ от угроз нарушения доступности	Построение систем защиты от угроз нарушения доступности информации	
3	Обеспечение информационной безопасности критичных отраслей	3	Безопасность периметра сети	Классификация удаленных атак. Методы защиты от них. Использование технологий криптографии для передачи конфиденциального трафика. Технологии VPN. Шифрование данных на сетевом уровне. Применение технологий шифрования данных совместно с межсетевыми экранами. Защищенные протоколы прикладных уровней. SSL, SHTTP. Пакет SSH. Методы защиты электронной почты. Пакет PGP.	ПК – 2.1, 4.1
			Защита рабочих станций	Угрозы безопасности операционной системе. Построение системы безопасности в системах с дискреционным доступом.	

				<p>Механизмы разграничения доступа в операционных системах. Идентификация, аутентификация и авторизация субъектов доступа. Аудит доступа. Реализация мандатного доступа в операционных системах. Алгоритмы аутентификации пользователей NTLM и Kerberos</p> <p>Подсистема защиты операционных систем семейства Windows, UNIX. Типовые сценарии атак на операционные системы.</p> <p>Перебор паролей. Атаки, основанные на переполнении буфера. Атаки на доверие. Использование разрушающих программных средств (РПС). Вирусы, сетевые черви, троянские кони. Анти-вирусная защита информации.</p>	
			<p>Мероприятия по защите ключевых систем информационной инфраструктуры</p>	<p>Последовательность мероприятий по защите КСИИ. Текущее состояние ИБ. Моделирование угроз. Разработка специальных технических требований. ФСТЭК РФ. Правовая защита информации, нормативные документы по безопасности критически важных объектов. Международные стандарты безопасности информационных технологий. Органы лицензирования и сертификации в области защиты информации в РФ. Процедуры лицензирования и сертификации Требования по защите информации.</p>	

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 критических систем информационной инфраструктуры в си-	7	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	ПК – 2.1-2.3, 4.1 – 4.3

	стеме национальной безопасности РФ			
2.	Модели систем защиты информации	4	Обеспечение конфиденциальности	ПК – 2.1-2.3, 4.1 – 4.3
3.		4	Обеспечение целостности	ПК – 2.1-2.3, 4.1 – 4.3
4.		2	Обеспечение доступности	ПК – 2.1-2.3, 4.1 – 4.3
5.	Обеспечение информационной безопасности критичных отраслей	4	Межсетевой экран	ПК – 2.1-2.3, 4.1 – 4.3
6.		4	Оценка уязвимости ПО Рабочих станций	ПК – 2.1-2.3, 4.1 – 4.3
7.		4	Анализ степени защищенности объекта информатизации	ПК – 2.1-2.3, 4.1 – 4.3

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1.	Национальная безопасность РФ	6	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
2.	Угрозы безопасности РФ в информационной сфере.	6	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
3.	СЗИ от угроз нарушения конфиденциальности	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
4.	СЗИ от угроз нарушения целостности.	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
5.	СЗИ от угроз нарушения доступности	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
6.	Безопасность периметра сети	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
7.	Защита рабочих станций	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3
8.	Мероприятия по защите ключевых систем информационной инфраструктуры	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3, 4.1 – 4.3

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1.	Национальная безопасность РФ	8	консультирование	ПК – 2.1-2.3, 4.1 – 4.3
2.	Угрозы безопасности РФ в информационной сфере.	7	консультирование	ПК – 2.1-2.3, 4.1 – 4.3

3.	СЗИ от угроз нарушения конфиденциальности	5	консультирование	ПК – 2.1-2.3, 4.1 – 4.3
4.	СЗИ от угроз нарушения целостности.	5	консультирование	ПК – 2.1-2.3, 4.1 – 4.3
5.	СЗИ от угроз нарушения доступности	5	консультирование	ПК – 2.1-2.3, 4.1 – 4.3
6.	Безопасность периметра сети	5	консультирование	ПК – 2.1-2.3, 4.1 – 4.3
7.	Защита рабочих станций	5	консультирование	ПК – 2.1-2.3, 4.1 – 4.3
8.	Мероприятия по защите ключевых систем информационной инфраструктуры	5	консультирование	ПК – 2.1-2.3, 4.1 – 4.3

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины Б1.В.17 Методы и средства защиты информационных систем критичных отраслей 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.17 Методы и средства защиты информационных систем критичных отраслей 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.	ЭБС «Znanium» https://znanium.com/catalog/product/1210523 . Доступ с любой точки интернет 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.	ЭБС «Znanium» https://znanium.com/catalog/product/1013711 . Доступ с любой точки интернет 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	ЭБС «Znanium» https://znanium.com/catalog/product/1189326 . Доступ с любой точки интернет 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	ЭБС «Znanium» https://znanium.com/catalog/product/1093695 . Доступ с любой точки интернет 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.
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	ЭБС «Znanium» https://znanium.com/catalog/product/1784437 . Доступ с любой точки интернет после регистрации с IP-адреса НХТИ

11.3. Электронные источники информации

При изучении дисциплины Б1.В.17 Методы и средства защиты информационных систем критичных отраслей использование электронных источников информации:

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

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
СЗИ от угроз нарушения конфиденциальности	Лекция	лекция визуализация	1
СЗИ от угроз нарушения целостности.	Лекция	лекция визуализация	1
СЗИ от угроз нарушения доступности	Лекция	лекция визуализация	1

Безопасность периметра сети	Лекция	лекция визуализация	1
Защита рабочих станций	Лекция	лекция визуализация	1
Мероприятия по защите ключевых систем информационной инфраструктуры	Лекция	лекция визуализация	1
Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	Лаб.зан	Работа в малых группах, метод проектов	1
Обеспечение конфиденциальности	Лаб.зан	Работа в малых группах, метод проектов	1
Обеспечение целостности	Лаб.зан	Работа в малых группах, метод проектов	1
Обеспечение доступности	Лаб.зан	Работа в малых группах, метод проектов	1
Межсетевой экран	Лаб.зан	Работа в малых группах, метод проектов	1
Оценка уязвимости ПО Рабочих станций	Лаб.зан	Работа в малых группах, метод проектов	1
Анализ степени защищенности объекта информатизации	Лаб.зан	Работа в малых группах, метод проектов	1
Итого:			14