

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.О.08 Безопасность и защита информации в информационных системах

Направление подготовки 09.04.01 Информатика и вычислительная техника

Профиль/программа Автоматизированные системы обработки информации и управления

Квалификация (степень) выпускника магистр

Форма обучения очная, очно-заочная

Факультет Информационных технологий

Кафедра-разработчик рабочей программы Информационных систем и технологий

Очная форма: курс - 1, семестр – 2, очно-заочная форма - курс - 1, семестр – 2

| | Очная форма | | Очно-заочная форма | |
|-------------------------------------|--------------|------------------|--------------------|------------------|
| | Часы | Зачетные единицы | Часы | Зачетные единицы |
| Лекции | 18 | 0,5 | 18 | 0,5 |
| Практические занятия | - | - | | |
| Лабораторные занятия | 36 | 1 | 27 | 0,75 |
| Контроль самостоятельной работы | 18 | 0,5 | 18 | 0,5 |
| Самостоятельная работа | 117 | 3,25 | 126 | 3,5 |
| Форма аттестации (часы на контроль) | Экзамен (27) | 0,75 | Экзамен (27) | 0,75 |
| Всего | 216 | 6 | 216 | 6 |

Нижнекамск, 2022 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (№ 918 от 19.09.2017) по направлению 09.04.01

(номер, дата утверждения)

(шифр)

«Информатика и вычислительная техника»

(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 Безопасность и защита информации в информационных системах являются

- а) формирование знаний о современном программном и аппаратном обеспечении информационных и автоматизированных систем,
- 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 информационных систем

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

Дисциплина Безопасность и защита информации в информационных системах относится к обязательной части ООП и формирует у магистров по направлению подготовки 09.04.01 «Информатика и вычислительная техника» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины Безопасность и защита информации в информационных системах магистр по направлению подготовки 09.04.01 «Информатика и вычислительная техника» должен освоить основы Защиты информации и материалы предшествующих дисциплин:

- а) Б1.О.04 Управление проектированием информационных систем цифрового предприятия;
- б) Б1.О.06 Технологии разработки программного обеспечения.

Дисциплина Безопасность и защита информации в информационных системах является предшествующей и необходима для успешного усвоения последующих дисциплин:

- а) Б1.О.15 Базы данных;
- б) Б1.О.14 ERP-системы.

Знания, полученные при изучении дисциплины, Безопасность и защита информации в информационных системах могут быть использованы при прохождении практик и выполнении выпускной квалификационной работы.

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

ОПК – 5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем

ОПК – 5.1 Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем

ОПК – 5.2 Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач

ОПК – 5.3 Владеет навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения

профессиональных задач

ОПК – 6 Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования;

ОПК – 6.1 Знает аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности

ОПК – 6.2 Умеет анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования

ОПК – 6.3 Владеет навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса

В результате освоения дисциплины обучающийся должен:

1) Знать:

- а) современное программное и аппаратное обеспечение информационных и автоматизированных систем;
- б) аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности.

2) Уметь:

- а) модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач
- б) анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования.

3) Владеть:

- а) навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач
- б) навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса

4. Структура и содержание дисциплины Безопасность и защита информации в информационных системах

Общая трудоемкость дисциплины составляет 64 учебных единиц, 216 часов.

Очная форма

| № п/ п | Раздел дисциплины | Семестр | Виды учебной работы(в часах) | | | | | Оценочные средства для проведения про- межуточной ат- тестации по раз- делам |
|------------------|--|---------|---------------------------------|---------------------------|-----------------------------|-----------|------------|---|
| | | | Лек- ции | Практ. заня- тия | Лабора- торные работы | КСР | СРС | |
| 1 | Основные понятия и определения в области информационной безопасности автоматизированных систем | 2 | 2 | - | 4 | 2 | 13 | Экзамен |
| 2 | Угрозы безопасности | 2 | 2 | - | 4 | 2 | 13 | Реферат |
| 3 | Модели защиты | 2 | 2 | - | 4 | 2 | 13 | Экзамен |
| 4 | Аудит информационной безопасности и оценка рисков | 2 | 2 | - | 4 | 2 | 13 | Экзамен |
| 5 | Средства защиты информации | 2 | 2 | - | 4 | 2 | 13 | Экзамен, РГР |
| 6 | Аутентификация пользователей | 2 | 2 | - | 4 | 2 | 13 | Экзамен |
| 7 | Криптографические средства защиты | 2 | 2 | - | 4 | 2 | 13 | Экзамен, РГР |
| 8 | Системы обнаружения атак | 2 | 2 | - | 4 | 2 | 13 | Экзамен, групповое творческое задание |
| 9 | Защита от внутренних угроз информационной безопасности | 2 | 2 | - | 4 | 2 | 13 | Экзамен |
| ИТОГО | | | 18 | | 36 | 18 | 117 | |
| Форма аттестации | | | | Очная форма: экзамен (27) | | | | |

Очно-заочная форма

| № п/ п | Раздел дисциплины | Семестр | Виды учебной работы(в часах) | | | | | Оценочные средства для проведения про- межуточной ат- тестации по раз- делам |
|------------------|--|---------|---------------------------------|---------------------------|----------------------------------|-----------|------------|---|
| | | | Лек- ции | Практ. заня- тия | Лабора- тор- ные работы | КСР | СРС | |
| 1 | Основные понятия и определения в области информационной безопасности автоматизированных систем | 2 | 2 | - | 3 | 2 | 14 | Экзамен |
| 2 | Угрозы безопасности | 2 | 2 | - | 3 | 2 | 14 | Реферат |
| 3 | Модели защиты | 2 | 2 | - | 3 | 2 | 14 | Экзамен |
| 4 | Аудит информационной безопасности и оценка рисков | 2 | 2 | - | 3 | 2 | 14 | Экзамен |
| 5 | Средства защиты информации | 2 | 2 | - | 3 | 2 | 14 | Экзамен, РГР |
| 6 | Аутентификация пользователей | 2 | 2 | - | 3 | 2 | 14 | Экзамен |
| 7 | Криптографические средства защиты | 2 | 2 | - | 3 | 2 | 14 | Экзамен, РГР |
| 8 | Системы обнаружения атак | 2 | 2 | - | 3 | 2 | 14 | Экзамен, групповое творческое задание |
| 9 | Защита от внутренних угроз информационной безопасности | 2 | 2 | - | 3 | 2 | 14 | Экзамен |
| ИТОГО | | | 18 | | 27 | 18 | 126 | |
| Форма аттестации | | | | Очная форма: экзамен (27) | | | | |

5. Содержание лекционных занятий по темам с указанием формируемых компетенций

| № | Раздел дисциплины | Часы | Тема лекционного занятия | Краткое содержание | Индикаторы достижения компетенции |
|----|--|------|---|---|-----------------------------------|
| 1. | Основные понятия и определения в области информационной безопасности автоматизированных систем | 2 | Основные понятия и определения в области информационной безопасности автоматизированных | Объект защиты; Автоматизированная система как среда для обработки, хранения и передачи информации; Уязвимости АС; Информационные атаки, виды, последствия | ОПК – 5.1, ОПК – 6.1 |

| | | | | | |
|----|---|---|---|--|-------------------------|
| | | | систем | | |
| 2. | Угрозы безопасности | 2 | Угрозы безопасности | Классификация угроз безопасности; Интерпретация угроз атаки. Надежность, параметры, характеристики безопасности; Классификация угроз уязвимостей и уровней защиты | ОПК – 5.1, ОПК – 6.1 |
| 3. | Модели защиты | 2 | Модели защиты | Методы и абстрактные модели защиты информации; Модели защиты автоматизированных систем от информационных атак; Математическое моделирование угроз безопасности | ОПК – 5.1, ОПК – 6.1 |
| 4. | Аудит информационной безопасности и оценка рисков | 2 | Аудит информационной безопасности и оценка рисков | Аудит информационной безопасности и оценка рисков | ОПК – 5.1, ОПК – 6.1 |
| 5. | Средства защиты информации | 2 | Средства защиты информации | Средства криптографической защиты информации; Средства разграничения доступа пользователей к информационным ресурсам АС; Средства межсетевого экранирования; Средства анализа защищенности автоматизированных систем; Средства антивирусной защиты Средства защиты от спама; Средства контентного анализа; Системы обнаружения атак и история их развития; Средства , системы и комплексы защиты ПО | ОПК – 5.1, ОПК – 6.1 |
| 6. | Аутентификация пользователей | 2 | Аутентификация пользователей | Аутентификация пользователей на основе инфраструктуры открытых ключей | ОПК – 5.1, ОПК – 6.1 |
| 7. | Криптографические средства защиты | 2 | Криптографические средства защиты | Симметричное шифрование; Криптография с открытым ключом; Обзор интерфейса программирования | ОПК – 5.1, ОПК – 6.1 |
| 8. | Системы обнаружения атак | 2 | Системы обнаружения атак | Сбор исходной информации системами обнаружения атак; Методы обнаружения информационных атак; Противодействие выявленным информационным атакам | ОПК – 5.1, ОПК – 6.1 |
| 9. | Защита от внут- | 2 | Защита от | Каналы утечки конфиденциаль- | ОПК – 5.1, |

| | | | | | |
|--|--|--|--|---|-----------|
| | ренных угроз информационной безопасности | | внутренних угроз информационной безопасности | ной информации; Изолированная автоматизированная система для работы с конфиденциальной информацией; Системы активного мониторинга рабочих станций пользователей; Выделенный сегмент терминального доступа к конфиденциальной информации ; Средства контентного анализа исходящих пакетов данных; Средства криптографической защиты конфиденциальной информации ; Примеры систем защиты от внутренних угроз безопасности ; Система «InfoWatchNetMonitor»; Система «Insider»; Система «Урядник»; Система «DeviceLock» | ОПК – 6.1 |
|--|--|--|--|---|-----------|

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. | Основные понятия и определения в области информационной безопасности автоматизированных систем | 4/3 | Моделирование информационной безопасности | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 2. | Угрозы безопасности | 4/3 | Модель угроз | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 3. | Модели защиты | 4/3 | Модель защиты автоматизированной системы от информационных атак | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 4. | Аудит информационной безопасности и оценка рисков | 4/3 | Аудит информационной безопасности и оценка рисков | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 5. | Средства защиты информации | 4/3 | Средства защиты информации по категории значимости объекта управления | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |

| | | | | |
|----|--|-----|---|--|
| 6. | Аутентификация пользователей | 4/3 | Элементы теории информации | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 7. | Криптографические средства защиты | 4/3 | Избыточное кодирование данных в информационных системах | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 8. | Системы обнаружения атак | 4/3 | Системы обнаружения атак | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 9. | Защита от внутренних угроз информационной безопасности | 4/3 | Сжатие или распаковка данных | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |

8. Самостоятельная работа

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма СРС | Индикаторы достижения компетенции |
|--------------|--|-------------|------------------|--|
| 1. | Основные понятия и определения в области информационной безопасности автоматизированных систем | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 2. | Угрозы безопасности | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 3. | Модели защиты | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 4. | Аудит информационной безопасности и оценка рисков | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 5. | Средства защиты информации | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 6. | Аутентификация пользователей | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 7. | Криптографические средства защиты | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 8. | Системы обнаружения атак | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 9. | Защита от внутренних угроз информационной безопасности | 13/14 | Выполнение РГР | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |

8.1 Контроль самостоятельной работы

| № п/п | Темы, выносимые на самостоятельную работу | Часы | Форма КРС | Индикаторы достижения компетенции |
|--------------|--|-------------|------------------|--|
| 10. | Основные понятия и определения в области информационной безопасности автоматизированных систем | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 11. | Угрозы безопасности | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 12. | Модели защиты | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 13. | Аудит информационной безопасности и оценка рисков | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 14. | Средства защиты информации | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 15. | Аутентификация пользователей | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 16. | Криптографические средства защиты | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 17. | Системы обнаружения атак | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |
| 18. | Защита от внутренних угроз информационной безопасности | 2 | консультирование | ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-6.1, ОПК-6.2, ОПК-6.3 |

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Безопасность и защита информации в информационных системах» 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 экзамен, реферат, выполнение двух расчётно-графических работ. 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 |
|-----------------------------|---------------|--------------------|--------------------|
| Расчётно-графических работа | 2 | 26 | 40 |
| Реферат | 1 | 10 | 20 |
| Экзамен | 1 | 24 | 40 |
| 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 «Безопасность и защита информации в информационных системах» 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. - Режим доступа: https://znanium.com/catalog/product/1210523 | ЭБС «Znanium» https://znanium.com/catalog/product/1210523 Доступ из любой точки Интернет после регистрации с IP-адресов НХТИ |
| 2. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт. — Режим доступа: https://urait.ru/bcode/449285 | ЭБС Юрайт https://urait.ru/bcode/449285 Доступ из любой точки Интернет после регистрации с IP-адресов НХТИ |

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

| Дополнительные источники информации | Кол-во экз. |
|---|---|
| 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. - Режим доступа: https://znanium.com/catalog/product/1189326 . | ЭБС «Znanium» https://znanium.com/catalog/product/1189326 . Доступ из любой точки Интернет после регистрации с IP-адресов НХТИ |

11.3. Электронные источники информации

При изучении дисциплины Б1.О.06 «Безопасность и защита информации в информационных системах» в качестве электронных источников информации, рекомендуется использовать следующие источники:

1. Электронная библиотека УНИЦ НХТИ – режим доступа: <https://www.nchti.ru/studentam/электронная-библиотека>.
2. ЭБС «Znanium.com» – Режим доступа: <http://znanium.com>
3. ЭБС «Юрайт» – Режим доступа: <http://www.urait.ru>

11.4. Современные профессиональные Программирование и информационные справочные системы

1. Научная электронная библиотека (РУНЭБ). – <http://elibrary.ru>
2. ЭБС ZNANIUM.COM. – <http://znanium.com>
3. ЭБС «РУКОНТ» – <http://rucont.ru>

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

Количество занятий, проводимых в интерактивных формах, для очной формы обучения – 12 ак. час., очно-заочной – 8 ак. час.

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