

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки (специальности)
02.03.01 Математика и компьютерные науки

Направленность (профиль)
«Программирование, алгоритмы и анализ данных»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 12 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Изучение дисциплины «Информационная безопасность» способствует решению следующих задач профессиональной деятельности

- изучение концепции технической защиты информации;
- изучение теоретических основ технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ технической защиты информации;
- изучение методического обеспечения технической защиты информации.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. Знания и навыки, полученные в результате изучения дисциплины «Информационная безопасность», используются студентами в дальнейшем при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

| Формируемая компетенция (код и формулировка) | Индикатор достижения компетенции (код и формулировка) | Перечень планируемых результатов обучения |
|---|---|---|
| Общепрофессиональные компетенции | | |
| ПК-3 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники. | И-ПК-3.2 Знает основные методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов, их сопровождения, администрирования и развития (эволюции). И-ПК-3.3 Умеет использовать методы проектирования и | Знать: - основные методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов, их сопровождения, администрирования и развития (эволюции). - основные нормативные положения и концепции прикладного и системного программирования, архитектуры компьютеров и сетей (в том числе и глобальных), современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов. Уметь: использовать методы проектирования и производства программного продукта, |

| | | |
|--|--|--|
| | производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта. | принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта. |
|--|--|--|

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **2** зачетные единицы, **72** акад. часа.

| № п/п | Темы (разделы) дисциплины, их содержание | Семестр | Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах) | | | | | | Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам) |
|----------|--|---------|---|--------------|--------------|--------------|-----------------------------|---------------------------|--|
| | | | Контактная работа | | | | | | |
| | | | лекции | практические | лабораторные | консультации | аттестационные испытания | самостоятельная работа | |
| 1 | Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. | 8 | 2 | | | | | 2 | |
| 2 | Виды противников или «нарушителей». | 8 | 4 | 2 | | 2 | | | Опрос на практических занятиях |
| 3 | Вредоносное программное обеспечение. | 8 | 4 | 2 | | | | | Опрос на практических занятиях |
| 4 | Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства | 8 | 2 | | | 2 | | 2 | |
| 5 | Классификация нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. | 8 | 4 | 2 | | | | 2 | Опрос на практических занятиях |
| 6 | Анализ способов нарушений информационной безопасности. | 8 | 4 | 4 | | 2 | | 2 | Опрос на практических занятиях |

| | | | | | | | | | |
|---|---|---|----|----|--|---|-----|------|--------------------------------|
| 7 | Использование защищенных компьютерных систем. | 8 | 4 | 2 | | | | 3 | Опрос на практических занятиях |
| 8 | Методы криптографии | 8 | 4 | 2 | | | | 2 | Опрос на практических занятиях |
| 9 | Основные технологии построения защищенных систем. | 8 | 4 | 2 | | | | 2 | Опрос на практических занятиях |
| | | | | | | | 0,3 | 2,7 | Зачет |
| | Всего | | 32 | 16 | | 6 | 0,3 | 17,7 | |

Содержание разделов дисциплины:

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.

- 1.1. Стандарты в области информационной безопасности.
- 1.2. Международные стандарты информационного обмена.
- 1.3. Понятие угрозы, атаки.
- 1.4. Глобальные сети и информационная безопасность.

Тема 2. Виды противников или «нарушителей».

- 2.1. Понятие нарушителя информационной безопасности.
- 2.2. Хакеры. Виды хакеров. Примеры хакерских атак.

Тема 3. Вредоносное программное обеспечение.

- 3.1. Виды вредоносного программного обеспечения.
- 3.2. Вирусы как класс вредоносного программного обеспечения.
- 3.3. Виды вирусов и их классификация.

Тема 4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

- 4.1. Схема построения информационной безопасности на уровне государства.
- 4.2. Назначение и задачи в сфере обеспечения безопасности.
- 4.3. Регуляторы в сфере обеспечения информационной безопасности государства.

Тема 5. Классификация нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

- 5.1. Понятие и виды нарушений безопасности.
- 5.2. Причины нарушения информационной безопасности.
- 5.3. Аудит событий в рамках информационной системы.

Тема 6. Анализ способов нарушений информационной безопасности.

- 6.1. Анализ различных способов нарушений информационной безопасности.
- 6.2. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.

Тема 7. Использование защищенных компьютерных систем.

- 7.1. Защищенные компьютерные системы. Их виды и особенности.
- 7.2. Примеры защищенных систем. Их использование и применение на практике.

Тема 8. Методы криптографии.

- 8.1. Криптография, Криптоанализ. Основные понятия криптологии.
- 8.2. История шифрования. Использование шифрования различными методами.
- 8.3. Программы для криптографии.
- 8.4. Электронная цифровая подпись.

Тема 9. Основные технологии построения защищенных систем.

- 9.1. Основные технологии построения защищенных систем.
- 9.2. Физические устройства. Их виды и использование.
- 9.3. Правовые особенности использования средств информационной защиты.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются: для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- Adobe Acrobat Reader;
- Интернет-версия справочной системы Гарант.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»

<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/370967>
2. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / Шаньгин В. Ф. - Москва : ДМК Пресс, 2012. - 592 с. - ISBN 978-5-94074-637-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785940746379.html>
3. Родичев Ю. А. Информационная безопасность: национальные стандарты Российской Федерации: учебное пособие для студентов. / Ю. А. Родичев; Редакционно-издат. совет Самарский нац. исслед. ун-т им. С. П. Королева - 2-е изд. - СПб.: Питер, 2019. - 304 с.: ил.

б) дополнительная литература

1. Белов, Е. В. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва : Горячая линия - Телеком, 2011. - 544 с. - ISBN 5-93517-292-5. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN5935172925.html>
2. Девянин П.Н. Модели безопасности компьютерных систем. - Москва: Академия, 2005.
3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для вузов. - М.: Академия, 2014.
4. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие для вузов / Под ред. профессора О. И. Шелухина. - Москва : Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785991203234.html>
5. Проскурин В.Г. Защита программ и данных - М., Издательский центр «Академия», 2012.
6. ГОСТ Р ИСО/МЭК ТО 19791-2008г., «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. <https://ohranatruda.ru/upload/iblock/f48/4293822466.pdf>
7. ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2014. <https://ohranatruda.ru/upload/iblock/b15/4293774833.pdf>
8. ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности», «Часть. 3. Компоненты доверия к безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2014.
Часть 1. <https://ohranatruda.ru/upload/iblock/857/4293781374.pdf>
Часть 2. <https://ohranatruda.ru/upload/iblock/c21/4293774728.pdf>
Часть 3. <http://gost.gtsever.ru/Data/554/55440.pdf>
9. ГОСТ Р ИСО/МЭК 53113.1-2008 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 1.

Общие положения», Фед. агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009.

<https://ohranatruda.ru/upload/iblock/47a/4293825688.pdf?ysclid=lirr3mjli7846150599>

10. ГОСТ Р ИСО/МЭК 53113-2-2009 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 2. Рекомендации по защите информации, информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов» Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2010.

<https://ohranatruda.ru/upload/iblock/f8a/4293824168.pdf>

11. Руководящие документы ФСТЭК России «Требования к системам обнаружения вторжений», введенных приказом ФСТЭК России от 6 декабря 2011 г. № 638 (зарегистрирован Минюстом России 1 февраля 2012 г., рег. №23088) для 4, 5 и 6 классов ИС. <https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-pismo-fstek-rossii?ysclid=lirs0sskd7386926451>

12. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год. <http://fstec.ru/component/attachments/download/289>

13. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=lirryc7hzh1975773957>

14. Банк данных угроз безопасности информации ФСТЭК России. <https://bdu.fstec.ru/threat>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

старший преподаватель
кафедры КБ и ММОИ

А.В. Саханда

**Приложение № 1 к рабочей программе дисциплины
«Информационная безопасность»**

**Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания или иные материалы,
используемые в процессе текущей аттестации**

Перечень вопросов для опросов на практических занятиях:

1. В чем суть отличий российской классификации угроз безопасности от принятой в западных стандартах?
2. В чем состоит суть защиты от нарушения конфиденциальности, целостности и доступности информации?
3. Как определить вероятные цели компьютерной атаки по признакам формы ее реализации?
4. Каковы составляющие российской системы обеспечения безопасности критических информационных систем от компьютерных атак?
5. Какие вы знаете модели взаимодействия программной закладки с атакуемой компьютерной системой?
6. Назовите предпосылки к внедрению и методы внедрения программных закладок.
7. В чем особенности компьютерных вирусов, выделяемых в отдельный класс вредоносных программ?
8. Охарактеризуйте жизненный цикл, особенности функционирования, особенности противодействия компьютерным вирусам того или иного класса.
9. В чем состоит отличие утечки информации по техническим каналам от других видов?
10. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними.
11. Современные средства защиты информации.
12. Современные криптографические системы.
13. Криптоанализ, современное состояние.
14. Правовые основы защиты информации.
15. Технические аспекты обеспечения защиты информации.
16. Современные пути решения проблемы информационной безопасности РФ.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету

1. Перечислите и охарактеризуйте угрозы информационной безопасности Российской Федерации, указанные в «Доктрине информационной безопасности» Российской Федерации.
2. Сформулируйте и обоснуйте общие принципы построения защиты информации в России.
3. В чем суть российской классификация угроз и ее отличие от принятой в западных стандартах.
4. Дайте обзор средств и методов информационной/компьютерной безопасности, принятых в России.
5. Дайте описание основных методов нарушения конфиденциальности, целостности и доступности информации.

6. Назовите и охарактеризуйте основные модели управления доступом к компьютерной информации.
7. На любом произвольном примере опишите Модель вероятного нарушителя, Модель действий вероятного нарушителя, соотнесите их с Моделью построения защиты на основе двух предыдущих.
8. Приведите и охарактеризуйте известные из учебной литературы классификации основных видов компьютерных атак.
9. Опишите и кратко охарактеризуйте методы и тактику проведения сетевой разведки.
10. Опишите элементы системы обеспечения безопасности критических информационных систем от компьютерных атак.
11. Опишите и кратко охарактеризуйте средства и методы нейтрализации компьютерных атак.
12. Приведите известные из учебной литературы классификации вредоносных программ.
13. Опишите и кратко охарактеризуйте признаки присутствия вредоносного ПО.
14. Назовите и охарактеризуйте способы внедрения вредоносного ПО.
15. Назовите и охарактеризуйте методы обнаружения вредоносного ПО.
16. Приведите и охарактеризуйте известные примеры сетевых атак.
17. Дайте определение и охарактеризуйте троянские программы, люки, эксплойты.
18. Назовите и охарактеризуйте методы защиты от вредоносного ПО, технологии самозащиты.
19. Опишите и кратко охарактеризуйте место и роль межсетевых экранов в обеспечении безопасности ресурсов автоматизированных систем.
20. Опишите и кратко охарактеризуйте возможности и ограничения антивирусных программ.
21. Назовите и охарактеризуйте специализированные средства и методы выявления вредоносных программ.
22. Приведите и охарактеризуйте известные из учебной литературы классификации средств защиты информации и нападения на элементы защиты.
23. Приведите и охарактеризуйте известные из учебной литературы классификации электронных устройств перехвата информации, внедряемых в средства вычислительной техники.
24. Чем обусловлена необходимость уничтожения документов. Охарактеризуйте особенности удаления информации с современных электронных носителей.
25. Следы в сети. Опишите и кратко охарактеризуйте уникальные идентификаторы интернет-пользователей и электронные «отпечатки», и относительность «конфиденциальности» в социальных сетях.
26. Назовите и охарактеризуйте средства и методы обнаружения технических каналов утечки информации.
27. Назовите и кратко охарактеризуйте системы защиты конфиденциальных данных от внутренних угроз.
28. В чем заключаются задачи криптографии?
29. Какая схема шифрования называется многоалфавитной подстановкой?
30. Какие системы шифрования вы знаете?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Какие требования предъявляются к современным криптографическим системам защиты информации?
34. Как классифицируются криптографические алгоритмы по стойкости?
35. Что является основными характеристиками технических средств защиты информации?

36. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
37. Какие требования предъявляются к межсетевым экранам?
38. В чем заключается организация работ по защите от несанкционированного доступа информационной системы управления предприятием.
39. Какие задачи решает система компьютерной безопасности?
40. Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
41. Что понимают под политикой информационной безопасности?

3. Правила приема зачета.

Оценка знаний по итогу прохождения курса проводится в форме принятия зачета.

На зачете проверяется сформированность всех указанных в учебной программе компетенций.

В билет для зачета включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

Также есть возможность ответить на контрольные вопросы в электронном курсе «Информационная безопасность» в LMS Электронный университет Moodle ЯрГУ.

По итогам ответов студенту выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «зачтено» выставляется студенту, если: он знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины, владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется студенту, если: он не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине, не в полной мере владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

**Приложение №2 к рабочей программе дисциплины
«Информационная безопасность»**

Методические указания для студентов по освоению дисциплины

Изучение дисциплины предполагает уверенное владение компьютером, умение осуществлять поиск и оценку достоверности необходимой информации в сети Интернет, но студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Основы информационной безопасности». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым в силу обучения на них учащихся сравнительным оценкам знаний из различных источников, критической их оценки. Также без упорных и регулярных самостоятельных занятий в течение семестра, желательно с «упреждающим знакомством» с содержанием предстоящего занятия, крайне сложно усвоить логику и аргументацию упомянутых сравнительных оценок и критического анализа знаний из различных источников, что не позволит студентам развить продвинутого и высокого уровня компетенций.