

Рубцовский индустриальный институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Алтайский государственный технический университет им. И.И. Ползунова»

## СОГЛАСОВАНО

И.о. декана ТФ  
Казанцева

Ю.В.

## Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.О.22 «Защита информации»**

Код и наименование направления подготовки (специальности): **09.03.01**

**Информатика и вычислительная техника**

Направленность (профиль, специализация): **Технологии разработки программного обеспечения**

Статус дисциплины: **обязательная часть**

Форма обучения: **очная**

| Статус     | Должность                                       | И.О. Фамилия |
|------------|---|--------------|
| Разработал | доцент  | Н.А. Ларина  |
| Согласовал | Зав. кафедрой «ПМ»                              | Л.А. Попова  |
|            | руководитель направленности (профиля) программы | Л.А. Попова  |

г. Рубцовск

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

| Компетенция | Содержание компетенции  | Индикатор | Содержание индикатора   |
|-------------|---|-----------|---|
| ОПК-2       | Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности                                 | ОПК-2.1   | Выбирает информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности               |
|             |   | ОПК-2.2   | Использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности |
| ОПК-3       | Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ОПК-3.1   | Использует основы информационной и библиографической культуры при работе с профессиональной информацией   |
|             |   | ОПК-3.2   | Применяет информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности   |
|             |   | ОПК-3.3   | Учитывает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности   |

## 2. Место дисциплины в структуре образовательной программы

|   |                        |
|---|------------------------|
| Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.                 | Базы данных            |
| Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения. | Преддипломная практика |

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 3 / 108

Форма промежуточной аттестации: Зачет

| Форма обучения | Виды занятий, их трудоемкость (час.) |                     |                      |                        | Объем контактной работы обучающегося с преподавателем (час) |
|----------------|--------------------------------------|---------------------|----------------------|------------------------|---|
|                | Лекции                               | Лабораторные работы | Практические занятия | Самостоятельная работа |   |
| очная          | 16                                   | 16                  | 16                   | 60                     | 57  |

**4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**Форма обучения: очная**

**Семестр: 7**

**Лекционные занятия (16ч.)**

**1. Информация и угрозы её безопасности(2ч.)[2,4]** Предмет защита информации. Понятие «информация». Свойства информации. Принципы работы современных информационных технологий и программных средств. История возникновения средств и способов защиты информации. Угрозы безопасности информации. Учет основных требований информационной безопасности при решении задач профессиональной деятельности Непреднамеренные угрозы. Угрозы безопасности информации. Преднамеренные угрозы Обеспечение достоверности информации в АС.

**2. Криптографическая защита данных.(6ч.)[1,2,3,5]** Криптография и криптоанализ. Симметричные криптосистемы: шифры перестановки, простой замены, сложной замены. Ассимметричные криптосистемы: криптосистемы с открытым ключом, RSA, система Эль Гамала. Построение и использование хеш-функций. Постановка и проверка электронной цифровой подписи.

**3. Организация и технологии защиты информации.(4ч.)[1,2]** Политика безопасности: дискреционная, мандатная, ролевая.

**4. Технологии межсетевых экранов защиты информации в сетях.(4ч.)[1,2]** Понятие "межсетевой экран". Классификация межсетевых экранов. Функции межсетевых экранов на уровне OSI. Основные и дополнительные возможности межсетевых экранов. Проблемы безопасности межсетевых экранов.

**Практические занятия (16ч.)**

**1. Шифрование методом перестановок. {беседа} (4ч.)[1]** Зеркальное отображение. Скитала.

**2. Решение задач шифрование методом замены. {мини-лекция} (4ч.)[2]** Знакомство с методиками шифрования: сдвигом, с помощью "Магического квадрата".

**3. Симметричные криптосистемы. {работа в малых группах} (4ч.)[2]** Американский стандарт шифрования данных DES. Блочные и поточные шифры.

**4. Асимметричные криптосистемы. {работа в малых группах} (4ч.)[4]**

Процедура шифрования и расшифрования в криптосистема RSA. Постановка и анализ электронной цифровой подписи.

### **Лабораторные работы (16ч.)**

- 1. Защита от вирусов. {имитация} (4ч.)[1,2]** Организация работы для поиска вирусов на рабочем месте программиста. Постановка и снятие паролей.
- 2. Шифры простой и сложной замены.(4ч.)[1,2]** Разработка программ шифрования и расшифрования методом простой замены: "Скитала", "Система шифрования Цезаря".
- 3. Защита информации методом симметричного шифрования. {деловая игра} (4ч.)[1,2]** Шифрование методами гаммирования, DES и раскрытие шифра.
- 4. Защита информации с использованием асимметричных алгоритмов. Системы с открытым ключом.(4ч.)[1,2,3,5]** Преобразование информации алгоритмом RSA. Нахождение хеш- функции сообщения. Постановка и проверка электронной цифровой функции.

### **Самостоятельная работа (60ч.)**

- 1. Разработка и реализация программы на тему "защита информации криптографическими методами. {творческое задание} (14ч.)[1,2,3,6]** Изучение метода, составление задания на программное обеспечение, написание, отладка и доказательство на контрольных примерах правильности работы его.
- 2. подготовка с лекционным, практическим занятиям и текущему контролю.(8ч.)[1,2,6]** Изучение лекционного материала, основной и дополнительной литературы.
- 3. Подготовка к защите творческой работы.(4ч.)[1]** Доклад с презентацией и комплект документации к программе.
- 4. подготовка к сдаче зачета.(18ч.)[1,2]** чтение литературы и лекций анализ алгоритмов защиты информации.
- 5. Зачет(16ч.)[1,2,3,4,5,6]**

### **5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине**

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронной информационно-образовательной среде АлтГТУ:

1. Ларина, Н.А. Защита информации. Криптология: метод. пособие для бакалавров направления подготовки "Информатика и вычислит. техника" дн. формы обучения/ Н.А. Ларина. - Рубцовск: РИО, 2014. - 56 с. URL: [https://edu.rubinst.ru/resources/books/Larina\\_N.A.\\_Zaschita\\_inphormatsii.\\_Kriptologiya\\_2014.pdf](https://edu.rubinst.ru/resources/books/Larina_N.A._Zaschita_inphormatsii._Kriptologiya_2014.pdf) (дата обращения 01.10.2021)

## **6. Перечень учебной литературы**

### **6.1. Основная литература**

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87995.html> (дата обращения: 28.02.2022). — Режим доступа: для авторизир. пользователей

### **6.2. Дополнительная литература**

3. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — Текст: электронный // Информационная сеть «Техэксперт»— Режим доступа: <http://docs.cntd.ru/document/gost-r-34-10-2012> , свободный.

4. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — Текст: электронный // Информационная сеть «Техэксперт»— Режим доступа: <http://docs.cntd.ru/document/1200101777> , свободный

5. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. — Текст: электронный // Информационная сеть «Техэксперт»— Режим доступа: <http://docs.cntd.ru/document/gost-r-34-11-2012> , свободный

## **7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

6. <https://intuit.ru/studies/courses/10/10/info>

## **8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации**

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

## **9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное

взаимодействие обучающегося с преподавателем через личный кабинет студента.

| <b>№пп</b> | <b>Используемое программное обеспечение</b> |
|------------|---|
| 1          | LibreOffice                                 |
| 2          | Windows                                     |
| 3          | Антивирус Kaspersky                         |

| <b>№пп</b> | <b>Используемые профессиональные базы данных и информационные справочные системы</b>   |
|------------|--|
| 1          | Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы ( <a href="http://Window.edu.ru">http://Window.edu.ru</a> )   |
| 2          | Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. ( <a href="http://нэб.рф/">http://нэб.рф/</a> ) |

#### **10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

| <b>Наименование специальных помещений и помещений для самостоятельной работы</b> |
|--|
| учебные аудитории для проведения учебных занятий                                 |
| помещения для самостоятельной работы   |

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».