

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Клочков Юрий Сергеевич  
Должность: и.о. ректора  
Дата подписания: 09.04.2024 16:20:31  
Уникальный программный ключ:  
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
**«ТОМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»**

**УТВЕРЖДАЮ**

\_\_\_\_\_ г.  
«\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

**РАБОЧАЯ ПРОГРАММА**

дисциплины:	Методы и средства криптографической защиты информации
направление подготовки:	38.03.05 «Бизнес - информатика»
направленность:	Информационные системы предприятия
форма обучения:	очная

Рабочая программа рассмотрена  
на заседании кафедры бизнес-информатики и математики

Заведующий кафедрой

\_\_\_\_\_ О.М. Барбаков

Рабочую программу разработал:

А.Н. Величко, старший преподаватель

\_\_\_\_\_

## 1. Цели и задачи освоения дисциплины

Цель освоения дисциплины: овладение теоретическими знаниями и умениями, развитие навыков практических действий по использованию методов и средств криптографической защиты информации.

Задачи освоения дисциплины:

- изучение нормативных правовых и организационных основ обеспечения информационной безопасности;
- изучение основных методов и средств криптографической защиты информации;
- практическая отработка способов и порядка проведения работ по защите информации с использованием средств криптографической защиты информации;
- развитие исследовательских и аналитических навыков, интеллектуального потенциала.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

- знание теоретических основ информационных и сетевых технологий и информационной безопасности;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины является логическим продолжением содержания дисциплины «Информационная безопасность и защита информации» и может служить основой для прохождения учебной и производственной практик, подготовки к выполнению выпускной квалификационной работы и профессиональной деятельности.

## 3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
УК – 1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК – 1.2. Систематизирует и критически анализирует информацию, полученную из разных источников, в соответствии с требованиями и условиями задачи	Знать (З1) теоретические основы криптографии, методов и средств криптографической защиты информации
		Уметь (У1) определять требования к криптографической защите информации в ИС
		Владеть (В1) практическими навыками разработки проектов по внедрению средств криптографической защиты информации
ПКС – 3. Способен выявлять и анализировать требования к ИС, разрабатывать архитектуру, осуществлять прототипирование, проектирование и дизайн ИС, писать технические задания на разработку ИС, создавать	ПКС – 3.3 Использует современные стандарты и регламенты деятельности при разработке и управлении ИТ-архитектуры предприятия	Знать (З2) основные методы криптографической защиты информации и основные характеристики средств криптографической защиты информации
		Уметь (У2) планировать и организовывать мероприятия по криптографической защите информации на предприятии

пользовательскую документацию к ИС		Владеть (В2) практическими навыками внедрения и настройки средств криптографической защиты информации
------------------------------------	--	---

#### 4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единиц, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	4/8	12	-	24	72	-	Зачет

#### 5. Структура и содержание дисциплины

##### 5.1. Структура дисциплины.

##### очная форма обучения (ОФО)

Таблица 5.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Правовые и организационные основы информационной безопасности	3	-	6	18	27	УК-1.2 ПКС-3.3	Задание на лабораторную работу
2	2	Методы и средства криптографической защиты информации	3	-	6	18	27		Задание на лабораторную работу
3	3	Применение СКЗИ	3	-	6	18	27		Задание на лабораторную работу
4	4	Проектирование средств криптографической защиты информации	3	-	6	18	27		Задание на лабораторную работу
5	Зачет		-	-	-	-	-	УК-1.2 ПКС-3.3	Вопросы к зачету
Итого:			12		24	72	108	X	X

##### заочная форма обучения (ЗФО)

не реализуется

##### очно-заочная форма обучения (ОЗФО)

не реализуется

##### 5.2. Содержание дисциплины.

### 5.2.1. Содержание разделов дисциплины (дидактические единицы).

**Раздел 1. Правовые и организационные основы информационной безопасности.** Основные понятия в области информационной безопасности. Нормативно-правовые акты, специальные нормативные документы и документы национальной (международной) системы стандартизации в области информационной безопасности. Система органов обеспечения информационной безопасности в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Нормативные документы в области применения средств криптографической защиты информации. Требования Положения ПКЗ-2005. Требования к средствам электронной подписи. Использование криптографических средств для обеспечения безопасности персональных данных. Требования по организации и обеспечению функционирования шифровальных (криптографических) средств. Рекомендации по применению криптосредств при обработке персональных данных.

**Раздел 2. Методы и средства криптографической защиты информации.** Общая характеристика программно-аппаратных средств криптографической защиты информации. Криптосредства. Электронная цифровая подпись. Контроль целостности. Уничтожение остаточной информации. Организация виртуальных частных сетей.

**Раздел 3. Применение СКЗИ.** Система защиты конфиденциальной информации StrongDisk. Система защиты корпоративной информации Secret Disk. Система криптографической защиты информации «Верба-OW». Организация VPN средствами СКЗИ VipNet. Организация VPN средствами СКЗИ StrongNet.. Организация VPN сетевого уровня средствами программного комплекса «Игла-П». Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ «КриптоПро CSP»

**Раздел 4. Проектирование средств криптографической защиты информации.** Применение библиотек CryptoAPI для работы с СКЗИ «КриптоПро CSP» в среде программирования Borland Delphi. Применение библиотек CryptoPro.Sharpei для работы с СКЗИ «КриптоПро CSP» на базе платформы программирования Microsoft .Net Framework. Проектирование средств криптографической защиты информации на базе библиотек СКЗИ «Верба-OW». Применение библиотек CryptoAPI для создания VPN-системы на основе СКЗИ «КриптоПро CSP» с применением ключей eToken.

### 5.2.2. Содержание дисциплины по видам учебных занятий.

#### Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	3	-	-	Правовые и организационные основы информационной безопасности
2	2	3	-	-	Методы и средства криптографической защиты информации
3	3	3	-	-	Применение СКЗИ
4	4	3	-	-	Проектирование средств криптографической защиты информации
Итого:		12	-	-	-

#### Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема занятия
		ОФО	ЗФО	ОЗФО	
1	1	6	-	-	Правовые и организационные основы информационной

					безопасности
2	2	6	-	-	Методы и средства криптографической защиты информации
3	3	6	-	-	Применение СКЗИ
4	4	6	-	-	Проектирование средств криптографической защиты информации
Итого:		24	-	-	-

### Практические занятия

Практические занятия учебным планом не предусмотрены.

### Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	18	-	-	Правовые и организационные основы информационной безопасности	Подготовка к лабораторным работам, оформление отчетов
2	2	18	-	-	Методы и средства криптографической защиты информации	Подготовка к лабораторным работам, оформление отчетов
3	3	18	-	-	Применение СКЗИ	Подготовка к лабораторным работам, оформление отчетов
4	4	18	-	-	Проектирование средств криптографической защиты информации	Подготовка к лабораторным работам, оформление отчетов
5	1-4	-	-	-	Зачет	Подготовка к зачету
Итого:		72	-	-		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- ИКТ – технологии (визуализация учебного материала в PowerPoint в диалоговом режиме);
- обучение в сотрудничестве (коллективная, групповая работа);
- технология проблемного обучения.

### 6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

### 7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

### 8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Лабораторная работа № 1	0-15
2	Лабораторная работа № 2	0-15
	ИТОГО за первую текущую аттестацию	<b>0-30</b>
2 текущая аттестация		
3	Лабораторная работа № 3	0-30
	ИТОГО за вторую текущую аттестацию	<b>0-30</b>
3 текущая аттестация		
4	Лабораторная работа № 4	0-40
	ИТОГО за третью текущую аттестацию	<b>0-40</b>
	<b>ВСЕГО</b>	<b>0-100</b>

## 9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ <http://webirbis.tsogu.ru/>;
- Цифровой образовательный ресурс – библиотечная система IPR SMART — <https://www.iprbookshop.ru/>;
- Электронно-библиотечная система «Консультант студента» [www.studentlibrary.ru](http://www.studentlibrary.ru/);
- Электронно-библиотечная система «ЛАНЬ» [https://e.lanbook.com](https://e.lanbook.com/);
- Образовательная платформа ЮРАЙТ [www.urait.ru](http://www.urait.ru/);
- Научная электронная библиотека ELIBRARY.RU [http://www.elibrary.ru](http://www.elibrary.ru/);
- Библиотеки нефтяных вузов России:
  - Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина <http://elib.gubkin.ru/>;
  - Электронная библиотека Уфимского государственного нефтяного технического университета <http://bibl.rusoil.net/>;
  - Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ <http://lib.ugtu.net/books>;
- Электронная справочная система нормативно-технической документации «Технорматив»;
- ЭКБСОН – информационная система доступа к электронным каталогам библиотек сферы образования и науки.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- StrongDisk;
- Secret Disk;
- Верба-OW;
- VipNet;
- Игла-П;
- КриптоПро CSP.

## 10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

**Обеспеченность материально-технических условий реализации ОПОП ВО**

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
	2	3	4
	Методы и средства криптографической защиты информации	<p>Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.</p>	625039, г. Тюмень, ул. Мельникайте, д. 70.
<p>Лабораторные занятия: Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.</p>		625039, г. Тюмень, ул. Мельникайте, д. 70	

**11. Методические указания по организации СРС**

**11.1. Методические указания по подготовке к лабораторным занятиям.**

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом занятии.



В начале лабораторного занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать знания, подготовиться к научно-исследовательской деятельности. В процессе работы на лабораторных занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

#### 11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, изучение мультимедиалекций, расположенных в свободном доступе, решение ситуационных (профессиональных) задач, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

**Планируемые результаты обучения для формирования компетенции и критерии их оценивания**

**Дисциплина:** Методы и средства криптографической защиты информации

**Код, направление подготовки:** 38.03.05 Бизнес - информатика

**Направленность (профиль):** Информационные системы предприятия

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
УК – 1. Способен осуществлять поиск, критически анализ и синтез информации, применять системный подход для решения поставленных задач	УК – 1.2. Систематизирует и критически анализирует информацию, полученную из разных источников, в соответствии с требованиями и условиями задачи	Знать (З1) теоретические основы криптографии, методов и средств криптографической защиты информации	Не знает теоретические основы криптографии, методов и средств криптографической защиты информации	Знает на низком уровне теоретические основы криптографии, методов и средств криптографической защиты информации	Знает на среднем уровне теоретические основы криптографии, методов и средств криптографической защиты информации	Знает в совершенстве теоретические основы криптографии, методов и средств криптографической защиты информации
		Уметь (У1) определять требования к криптографической защите информации в ИС	Не умеет определять требования к криптографической защите информации в ИС	Умеет на низком уровне определять требования к криптографической защите информации в ИС	Умеет на среднем уровне определять требования к криптографической защите информации в ИС	Умеет в совершенстве определять требования к криптографической защите информации в ИС
		Владеть (В1) практически навыками разработки проектов по внедрению средств криптографической защиты информации	Не владеет практическим и навыками разработки проектов по внедрению средств криптографической защиты информации	Владеет на низком уровне практическим и навыками разработки проектов по внедрению средств криптографической защиты информации	Владеет на среднем уровне практическим и навыками разработки проектов по внедрению средств криптографической защиты информации	Владеет в совершенстве практическим и навыками разработки проектов по внедрению средств криптографической защиты информации

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
<p>ПКС – 3. Способен выявлять и анализировать требования к ИС, разрабатывать архитектуру, осуществляя прототипирование, проектирование и дизайн ИС, писать технические задания на разработку ИС, создавать пользовательскую документацию к ИС</p>	<p>ПКС – 3.3 Использует современные стандарты и регламенты деятельности и при разработке и управлении ИТ-архитектуры предприятия</p>	<p>Знать (32) основные методы криптографической защиты информации и основные характеристики средств криптографической защиты информации</p>	<p>Не знает основные методы криптографической защиты информации и основные характеристики средств криптографической защиты информации</p>	<p>Знает на низком уровне основные методы криптографической защиты информации и основные характеристики средств криптографической защиты информации</p>	<p>Знает на среднем уровне основные методы криптографической защиты информации и основные характеристики средств криптографической защиты информации</p>	<p>Знает в совершенстве основные методы криптографической защиты информации и основные характеристики средств криптографической защиты информации</p>
		<p>Уметь (У2) планировать и организовывать мероприятия по криптографической защите информации на предприятии</p>	<p>Не умеет планировать и организовывать мероприятия по криптографической защите информации на предприятии</p>	<p>Умеет на низком уровне планировать и организовывать мероприятия по криптографической защите информации на предприятии</p>	<p>Умеет на среднем уровне планировать и организовывать мероприятия по криптографической защите информации на предприятии</p>	<p>Умеет в совершенстве планировать и организовывать мероприятия по криптографической защите информации на предприятии</p>
		<p>Владеть (В2) практически навыками внедрения и настройки средств криптографической защиты информации</p>	<p>Не владеет практическим и навыками внедрения и настройки средств криптографической защиты информации</p>	<p>Владеет на низком уровне практическим и навыками внедрения и настройки средств криптографической защиты информации</p>	<p>Владеет на среднем уровне практическим и навыками внедрения и настройки средств криптографической защиты информации</p>	<p>Владеет в совершенстве практическим и навыками внедрения и настройки средств криптографической защиты информации</p>

**КАРТА**  
**обеспеченности дисциплины учебной и учебно-методической литературой**

**Дисциплина:** «Методы и средства криптографической защиты информации»

**Код, направление подготовки:** 38.03.05 Бизнес - информатика

**Направленность (профиль):** Информационные системы предприятия

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	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). - ЭБС "Юрайт". - ISBN 978-5-534-04732-5 <a href="https://urait.ru/bcode/449285">https://urait.ru/bcode/449285</a>	ЭР*	30	100	+
2	Криптографические методы защиты информации : учебник для вузов : в 2 ч. Ч. 2. Системные и прикладные аспекты / В. М. Фомичёв, Д. А. Мельников. - М. : Издательство Юрайт, 2023. - 245 с. - (Высшее образование). - URL: <a href="https://urait.ru/bcode/512423">https://urait.ru/bcode/512423</a> . - Режим доступа: для автор. пользователей. - ЭБС "Юрайт".	ЭР*	30	100	+
3	<b>Васильева, Ирина Николаевна.</b> <b>Криптографические методы защиты информации</b> : учебник и практикум для вузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2023. - 349 с. - (Высшее образование). - URL: <a href="https://urait.ru/bcode/511890">https://urait.ru/bcode/511890</a> . - Режим доступа: для автор. пользователей. - ЭБС "Юрайт"	ЭР*	30	100	+
4	Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Лань, 2019. - 344 с. - ЭБС Лань. - ISBN 978-5-8114-3940-9 <a href="https://e.lanbook.com/book/125739">https://e.lanbook.com/book/125739</a>	ЭР*	30	100	+

\*ЭР – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ <http://webirbis.tsogu.ru/>