

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Директор ИШИТР

Д.М. Сонькин

« 01 » сентября 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРИЕМ 2017 г.

ФОРМА ОБУЧЕНИЯ очная

Информационная безопасность и защита информации			
Направление подготовки/ специальность Образовательная программа (направленность (профиль)) Специализация Уровень образования Курс Трудоемкость в кредитах (зачетных единицах) Виды учебной деятельности	09.03.02 Информационные системы и технологии		
	Информационные системы и технологии		
	Геоинформационные системы		
	высшее образование - бакалавриат		
	4	семестр	8
	6		
Временной ресурс			
Контактная (аудиторная) работа, ч	Лекции		44
	Практические занятия		-
	Лабораторные занятия		33
	ВСЕГО		77
Самостоятельная работа, ч		139	
ИТОГО, ч		216	

Вид промежуточной аттестации

Экзамен

Обеспечивающее подразделение

ОИТ

Заведующий кафедрой -
руководитель отделения на
правах кафедры

Руководитель ООП

Преподаватель

Шерстнев В.С.

Цапко И.В.

Спицын В.Г.

2020 г.

1. Цели освоения дисциплины

Целями освоения дисциплины является формирование у обучающихся определенного ООП (п. 6. Общей характеристики ООП) состава компетенций для подготовки к профессиональной деятельности.

Код компетенции	Наименование компетенции	Результаты освоения ООП	Составляющие результатов освоения (дескрипторы компетенций)	
			Код	Наименование
ПК(У)-12	Способен разрабатывать средства реализации информационных технологий (методические, информационные, математические, алгоритмические, технические и программные)	Р9	ПК(У)-12.В14	Владеет опытом использования методов и средств обеспечения безопасности данных и компьютерных систем
			ПК(У)-12.У15	Умеет шифровать хранимые и передаваемые данные; определять оптимальные типы криптографических протоколов при передаче информации; применять компьютерные средства защиты информации от несанкционированного доступа
			ПК(У)-12.З14	Знает методы и средства обеспечения информационной безопасности компьютерных систем

2. Место дисциплины в структуре ООП

Дисциплина относится к вариативной части Блока 1 учебного плана образовательной программы

3. Планируемые результаты обучения по дисциплине

После успешного освоения дисциплины будут сформированы результаты обучения:

Планируемые результаты обучения по дисциплине		Компетенция
Код	Наименование	
РД1	Знать принципы построения систем защиты информации.	ПК(У)-12
РД 2	Уметь определять оптимальные типы криптографических протоколов при передаче информации. Владеть методами обеспечения безопасности данных и компьютерных систем	
РД 3	Уметь применять компьютерные средства защиты информации от несанкционированного доступа.	
РД 4	Уметь составлять научный отчет по выполненному заданию.	
РД 5	Выполнять аналитический обзор научной литературы и существующих методов, алгоритмов и систем.	

Оценочные мероприятия текущего контроля и промежуточной аттестации представлены в календарном рейтинг-плане дисциплины.

4. Структура и содержание дисциплины (модуля)

Разделы дисциплины	Формируемый результат обучения по дисциплине	Виды учебной деятельности	Объем времени, ч.

Раздел 1. Проблемы и методы защиты информации	РД 1	Лекции	11
	РД 2	Лабораторные занятия	8
		Самостоятельная работа	40
Раздел 2. Математические и методологические средства защиты информации	РД 1	Лекции	11
	РД 2	Лабораторные занятия	8
		Самостоятельная работа	40
Раздел 3. Криптографические алгоритмы обеспечения информационной безопасности	РД 3	Лекции	11
	РД 4	Лабораторные занятия	8
		Самостоятельная работа	30
Раздел 4. Компьютерные средства реализации защиты в информационных системах	РД 4	Лекции	11
	РД 5	Лабораторные занятия	9
		Самостоятельная работа	29

Раздел 1. Проблемы и методы защиты информации

Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста. Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности. Программа информационной безопасности России и пути ее реализации. Проблемы защиты информации в компьютерных системах. Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации. Организационное обеспечение информационной безопасности.

Лабораторная работа №1-3. Шифрование методом Полибия.

Раздел 2. Математические и методологические средства защиты информации

Криптографическая терминология. Сведения из теории информации и теории чисел. Алгоритмы и ключи. Симметричные алгоритмы. Алгоритмы с открытым ключом. Подстановочные и перестановочные шифры. Одноразовые блокноты. Однонаправленные хэш-функции. Передача информации с использованием криптографии с открытым ключом. Основные протоколы передачи информации.

Лабораторная работа № 2-6. Шифрование методом замены.

Лабораторная работа № 7-9. Шифрование методом умножения матриц.

Раздел 3. Криптографические алгоритмы обеспечения информационной безопасности

Алгоритм симметричного шифрования данных DES. Алгоритм криптографического преобразования ГОСТ 28147-89. Асимметричный алгоритм шифрования данных RSA. Комплекс криптографических алгоритмов PGP. Защита информации от несанкционированного доступа.

Лабораторная работа № 10-13. Разработка программы шифрования на основе асимметричного алгоритма шифрования данных RSA

Раздел 4. Компьютерные средства реализации защиты в информационных системах

Физический, сетевой, транспортный и прикладной уровни защиты информации. Обзор стандартов в области защиты информации. Методы и средства защиты локальной рабочей станции. Защита в локальных сетях. Защита информации при межсетевом взаимодействии. Брандмауэры. Типы вирусов и средства антивирусной защиты. Обеспечение информационной безопасности в корпоративных сетях.

Лабораторная работа № 13-16. Разработка программы шифрования на основе асимметричного алгоритма шифрования данных RSA

5. Организация самостоятельной работы студентов

Самостоятельная работа студентов при изучении дисциплины (модуля) предусмотрена в следующих видах и формах:

- Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса;
- Поиск, анализ, структурирование и презентация информации;
- Выполнение домашних индивидуальных заданий и домашних контрольных работ;
- Подготовка к лабораторным работам, к практическим и семинарским занятиям;
- Подготовка к оценивающим мероприятиям.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. М.: Горячая линия–Телеком, 2012. – 320 с.
2. Фороузан Б.А. Криптография и безопасность сетей. М.: Бином. Лаборатория знаний, 2010. – 784 с.
3. Спицын В.Г. Методы и средства защиты компьютерной информации: Учебное пособие. – Томск: Изд-во ТПУ, 2009. – 187 с.
4. Шаньгин, В. Ф.. Защита компьютерной информации. – Москва: Издательство "ДМК Пресс", 2010. - 544 с.

Дополнительная литература:

1. Спицын В.Г., Столярова Н.А. Защита информации и информационная безопасность. Учеб. пособие. - Томск: Изд. ТПУ, 2003. – 167 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.
3. Спицын В.Г. Информационная безопасность вычислительной техники : Учебное пособие. - Томск : Эль Контент, 2011 – 148 с.

6.2 Информационное обеспечение

Internet-ресурсы (в т.ч. в среде LMS MOODLE и др. образовательные и библиотечные ресурсы):

1. <http://www.ssl.stu.neva.ru/> - Санкт-Петербургский центр защиты информации.
2. <http://www.confident.ru/> - Журнал “Защита информации. Конфидент”..
3. http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm.
4. Электронно-библиотечная система «Лань» - <https://e.lanbook.com/>

Используемое для проведения практики лицензионное программное обеспечение (в соответствии с Перечнем лицензионного программного обеспечения ТПУ):

1. Visual Studio Pro2012.
2. Microsoft Office Standart 2016.
3. MATLAB Classroom From 10 to 24 Group All Platform Licenses (per License).

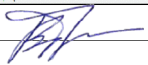
7. Особые требования к материально-техническому обеспечению дисциплины

В учебном процессе используется следующее лабораторное оборудование для практических и лабораторных занятий:

№	Наименование специальных помещений	Наименование оборудования
1.	Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации 634028, Томская область, г. Томск, Ленина проспект, д. 2, 410	Компьютер - 1 шт.; Проектор - 1 шт. Экран проекционный с электроприводом Lumien Master Control(LMC-100108) 153x203 см - 1 шт.; IP-камера купольная стационарная D-Link DCS-6210 - 1 шт.; Комплект громкоговорителей —APART SDQ5PIR-W и Врезная проводная панель удаленного управления APART ACPR - 1 шт.;
2.	Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) 634028, Томская область, г. Томск, Ленина проспект, д. 2 402	Компьютер - 12 шт. Доска аудиторная настенная - 1 шт.; Шкаф для документов - 1 шт.; Комплект учебной мебели на 12 посадочных мест;

Рабочая программа составлена на основе Общей характеристики образовательной программы по направлению 09.03.02 Информационные системы и технологии / Геоинформационные системы (приема 2017 г., очная форма обучения).

Разработчик(и):

Должность	Подпись	ФИО
Профессор ИШИТР		Спицын В.Г.

Программа одобрена на заседании кафедры Автоматики и компьютерных систем (протокол от «23» июня 2017г. № 9).

Заведующий кафедрой - руководитель отделения
на правах кафедры

 / В.С. Шерстнев

Лист изменений рабочей программы дисциплины:

Учебный год	Содержание /изменение	Обсуждено на заседании ШМП (протокол)