Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ А.С. Авдеев

Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.Б.19 «Криптографические методы защиты информации»**

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **обязательная часть (базовая)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	А.В. Санников
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	понятия, методы, модели разделов математики, необходимые для решения профессиональных задач, в том числе для защиты информации с применением методов криптографии	использовать математические методы для решения профессиональных задач, в том числе для реализации и применения алгоритмов шифрования, электронной подписи, криптографических протоколов	навыками применения математических расчетов для решения профессиональных задач, в том числе для защиты информации с применением методов криптографии
ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	значение информационно - коммуникационных технологий в развитии современного общества, в том числе значение криптографических методов для решения задач защиты информации	применять программные и аппаратные средства при решении профессиональных задач по обработке информации, в том числе применять криптографические методы для решения задач защиты информации	навыками применения программно-аппаратных средств для поиска или обработки информации, в том числе криптографического преобразования информации
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	виды, свойства и принципы работы средств криптографической защиты информации	выполнять работы по установке, настройке и обслуживанию программно-аппаратных (в том числе криптографических) и технических средств защиты информации, таких, как: КриптоАРМ, КриптоПро CSP, ViPNet CSP, ViPNet Client	навыками установки, настройки и обслуживания средств защиты информации, в том числе отечественных средств криптографической защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению	Дискретная математика, Информатика, Математика, Основы теории чисел, Теория вероятностей и

дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	математическая статистика
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Программно-аппаратные средства защиты информации, Сети и системы передачи информации, Системы электронного документооборота, Теория информации, Технологии защиты информации в глобальных сетях

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: Экзамен

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	17	34	0	57	56

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

Форма обучения: очная
Семестр: 5

Лекционные занятия (17ч.)

1. Введение. Традиционные криптосистемы. {лекция с разбором конкретных ситуаций} (2ч.)[2,6] Значение информации в развитии современного общества. Применение информационных технологий для поиска и обработки информации, а также для ее защиты. Основные понятия и определения. Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов. Шифры простой замены: полибианский квадрат, система шифрования Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом, шифрующие таблицы Трисемуса, биграммный шифр Плейфера,

криптосистема Хилла, система омофонов. Шифры сложной замены: шифр Гронсфельда, система шифрования Вижинера, шифр «двойной квадрат» Уитсона, одноразовая система шифрования, шифрование методом Вернама, роторные машины. Методы взлома классических шифров.

2. Современные симметричные шифры. {лекция с разбором конкретных ситуаций} (2ч.)[2,3,4] Применение информационных технологий для криптографического преобразования информации. Современные симметричные криптосистемы. Принцип итерирования. Конструкция Фейстеля. Американский стандарт шифрования данных DES. Область применения алгоритма DES. Основные режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования данных: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки. Атаки на блочные шифры. Дифференциальный криптоанализ. Линейный криптоанализ. Современный стандарт шифрования США.

3. Потоковые шифры. {лекция с разбором конкретных ситуаций} (2ч.)[2,3,6] Блочные и поточные шифры. Шифрование методом гаммирования: методы генерации псевдослучайных последовательностей чисел. Современные потоковые шифры. Регистры сдвига с линейной обратной связью. Генераторы истинно случайных последовательностей.

4. Асимметричное шифрование. {лекция с разбором конкретных ситуаций} (4ч.)[3,4,5] Концепция криптосистемы с открытым ключом. Однонаправленные функции. Применение математического аппарата для решения профессиональных задач защиты информации. Алгоритмы на основы задачи об укладке рюкзака. Криптосистема шифрования данных RSA: процедуры шифрования и расшифрования в криптосистеме RSA, безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига-Хеллмана. Схема шифрования Эль-Гамаля. Комбинированный метод шифрования. Генерация простых чисел. Построение больших простых чисел. Тесты проверки на простоту. Криптосистемы с открытым ключом на основе конечных автоматов.

5. Цифровая (электронная) подпись. {лекция с разбором конкретных ситуаций} (3ч.)[2,3,4] Идентификация и проверка подлинности. Основные понятия и концепции. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации с нулевой передачей знаний. Схема идентификации Гиллоу-Куискоутера. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи. Порядок выполнения работ по установке, настройке и обслуживанию современных криптографических средств защиты информации.

6. Криптографические протоколы. {лекция с разбором конкретных

ситуаций} (4ч.)[4,5,7] Введение в протоколы. Протоколы с посредником. Атаки на протоколы. Обмен ключами. Атака «человек посередине». Аутентификация. Разделение секрета. Групповые подписи. Подписи по доверенности. Подбрасывание монеты и игра в карты по телефону. Эзотерические протоколы. Применение криптографических протоколов.

Лабораторные работы (34ч.)

1. Взлом шифра простой замены. Метод частотного анализа.(2ч.)[1,2] Взлом шифра осуществляется без использования специализированного программного обеспечения.

2. Шифрование методом Вижинера. Взлом шифра Вижинера.(2ч.)[1,2] Программная реализация шифра Вижинера. Взлом шифра осуществляется с использованием специализированного программного обеспечения.

3. Алгоритм шифрования ГОСТ 28147-89.(4ч.)[1,2] Программная имитация алгоритма ГОСТ. Изучение и программная имитация режимов использования блочных шифров.

4. Шифрование методом гаммирования.(4ч.)[1,2] Программная реализация схемы шифрования числовой последовательности с использованием регистров сдвига с линейной обратной связью (4-х разрядный LFSR) в режимах синхронного шифрования и самосинхронизирующегося шифрования.

5. Генераторы псевдослучайных кодов.(3ч.)[1,2] Изучение и программная реализация методов генерации псевдослучайных последовательностей чисел.

6. Построение больших простых чисел(3ч.)[1,3] Применение математического аппарата для решения профессиональных задач криптографической защиты информации. Изучение принципов получения и программная реализация методов построения больших простых чисел.

7. Криптография с открытым ключом(6ч.)[1,3] Программная реализация системы распределения ключей Диффи-Хеллмана, шифра Эль-Гамаля, алгоритма RSA.

8. Хеш-функции.(3ч.)[1,7] Программная имитация хеш-функции с использованием алгоритма ГОСТ 28147-89 в режиме выработки имитовставки. Ключевые и бесключевые функции хеширования.

9. Электронная подпись.(3ч.)[1,2,7] Выполнение работ по установке, настройке и обслуживанию криптографических средств защиты информации. Формирование и проверка электронной подписи с использованием ПО КриптоПро CSP, КриптоАРМ (пробные версии). Работа с сертификатами. Шифрование данных.

10. Криптографические протоколы.(4ч.)[5,7] Программная реализация криптографических протоколов (по заданию)

Самостоятельная работа (57ч.)

1. Оформление отчетов по лабораторным работам и подготовка к текущему

контролю(20ч.)[1]
2. Изучение профильной литературы по дисциплине(20ч.)[2,3,4,5,6,7]
3. Подготовка к экзамену(17ч.)[2,3,4]

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

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Ленюк С.В. Методические указания к выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации»/ С.В. Ленюк; АлтГТУ им. И.И. Ползунова. – Барнаул, АлтГТУ, 2014. – 241 с. [электронный ресурс]:-режим доступа: http://elib.altstu.ru/eum/download/ivtib/uploads/lenyuk-s-v-ivtib-546aee294c819.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Основы криптографии : учеб. пособие для вузов по группе специальностей в обл. информ. безопасности / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - Москва : Гелиос АРВ, 2005. - 480 с. : ил. - Библиогр.: с. 469-475. - 4000 экз. - ISBN 5-85438-137-0 : 185.50 р., 253.00 р., 39 экз.

3. Фороузан Б. А. Математика криптографии и теория шифрования [Электронный ресурс] / Б. А. Фороузан. - 2-е изд., испр. - Электрон. текстовые дан. - Москва : Национальный открытый Университет Интуит, 2016. - 511 с. : ил. - ISBN 978-5-9963-0242-0 : Б. ц. Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

4. Рябко Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : [монография] / Б. Я. Рябко, А. Н. Фионов. - 2-е изд. - Электрон. текстовые дан. - Москва : Горячая линия-Телеком, 2013. - 232 с. : ил., табл. - Библиогр.: с. 225-229. - ISBN 978-5-9912-0350-0 : Б. ц. Режим доступа: https://e.lanbook.com/book/63244

6.2. Дополнительная литература

5. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по специальностям 090102 — «Компьютерная безопасность», 090105 — «Комплексное обеспечение информационной безопасности автоматизированных систем»] / [А. А. Афанасьев и др.] ; под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. - [2-е изд.,

стер.]. - Электрон. текстовые дан. - Москва : Горячая линия - Телеком, 2012. - 552 с. - Библиогр. в конце частей. - ISBN 978-5-9912-0257-2 : Б. ц. Режим доступа: https://e.lanbook.com/book/5114

6. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов [Электронный ресурс] / М. В. Адаменко. - Электрон. текстовые дан. - Москва : ДМК Пресс, 2012. - 255 с. : ил. - ISBN 978-5-94074-456-6 : Б. ц. Режим доступа: https://e.lanbook.com/book/9123

7. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости : [учебное пособие для вузов по специальности "Компьютерная безопасность"] / А. В. Черемушкин. - Москва : Академия, 2009. - 271, [1] с. : ил. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 264-270. - 2000 экз. - ISBN 978-5-7695-5748-4 : 496.10 р., 10 экз.

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

8. Информационный портал по безопасности [электронный ресурс]:- режим доступа https://www.securitylab.ru

9. Сайт журнала "Information Security/ Информационная безопасность" [электронный ресурс]:- режим доступа: https://www.securitylab.ru

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.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

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.

№пп	Используемое программное обеспечение
1	Microsoft Office
2	Windows
3	Acrobat Reader
4	Chrome

№пп	Используемое программное обеспечение
5	Visual Studio
6	LibreOffice
7	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
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. (http://нэб.рф/)

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

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения занятий лекционного типа
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации
лаборатории в области программно-аппаратных средств обеспечения информационной безопасности
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».