

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.О.30 «Методы и средства криптографической защиты информации»**

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

Направленность (профиль, специализация): **Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)**

Статус дисциплины: **обязательная часть**

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 индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2	Способен применять средства криптографической защиты при решении профессиональных задач

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Дискретная математика и теория чисел, Теория вероятностей и математическая статистика, Теория информации и кодирования
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Технологии защиты информации в вычислительных 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: 4 / 144

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	32	32	0	80	71

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 (32ч.)

- 1. Введение в криптографию {беседа} (2ч.)[2,3,4,5]** Традиционные криптосистемы. Основные понятия и определения. Цели и задачи криптографии. Классификация шифров и их характеристики. Классические шифры: шифры перестановки, шифры простой замены, шифры сложной замены. Шифрование телеграфных сообщений. Шифрование в аналоговой телефонии. Роторные машины. Методы взлома классических шифров и способы защиты от них. Особенности применения средств криптографической защиты при решении профессиональных задач защиты информации при ее хранении и передаче.
- 2. Современные симметричные шифры {лекция с разбором конкретных ситуаций} (4ч.)[2,3]** Современные симметричные криптосистемы. Требования к шифрам. Принципы построения современных шифров. Американский стандарт шифрования данных DES. Алгоритм шифрования данных IDEA. Алгоритм шифрования AES. Отечественные стандарты шифрования ГОСТ: описание и режимы работы. Атаки на блочные шифры и способы защиты от них. Понятие дифференциального и линейного криптоанализа. Отечественные средства криптографической защиты КриптоПРО и КриптоАРМ.
- 3. Поточные шифры {лекция с разбором конкретных ситуаций} (4ч.)[2,5]** Понятие поточных шифров и сфера их применения. Абсолютно стойкий шифр. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей. Требования к поточным шифрам. Современные поточные шифры. Регистры сдвига с линейной обратной связью. Криптографические алгоритмы защиты данных в сетях мобильной связи.
- 4. Асимметричная криптография {лекция с разбором конкретных ситуаций} (4ч.)[2,3,4]** Концепция криптосистем с открытым ключом и требования к алгоритмам. Решаемые задачи. Однонаправленные (односторонние) функции: понятие и примеры. Открытое распределение ключей Диффи-Хеллмана. Элементы теории чисел. Современные алгоритмы асимметричного шифрования, их безопасность и быстродействие. Гибридные криптосистемы. Атаки на алгоритмы и способы защиты.
- 5. Цифровая (электронная) подпись {лекция с разбором конкретных ситуаций} (4ч.)[2,3,5]** Основные понятия и концепции. Понятие и классификация хэш-функций. Современные отечественные и зарубежные хэш-функции. Обеспечение целостности данных. Задачи цифровой (электронной) подписи. Современные отечественные и зарубежные алгоритмы и средства электронной подписи.
- 6. Управление ключами {лекция с разбором конкретных ситуаций} (4ч.)[2,3,4]** Классификация ключей, используемых в алгоритмах. Понятие управления ключами. Методы генерации и распределения криптографических ключей. Сертификация открытых ключей. Инфраструктура открытых ключей. Центры сертификации. Протокол OCSP. Носители ключевой информации и особенности их хранения и использования.
- 7. Криптографические протоколы {лекция с разбором конкретных ситуаций} (4ч.)[3,5]** Понятие и классификация протоколов. Примитивные протоколы.

Прикладные протоколы. Идентификация и аутентификация. Протоколы аутентификации. Применение криптографических протоколов при защите информации в компьютерных системах и сетях. Программно-аппаратные средства криптографической защиты информации.

8. Практика применения средств криптографической защиты информации {с элементами электронного обучения и дистанционных образовательных технологий} (4ч.)[2,3,4] Законодательное регулирование использования средств криптографической защиты информации. Сертификация средств защиты. Лицензирование в области защиты информации. Особенности режима безопасности при использовании средств криптографической защиты информации.

9. Перспективы развития криптографических методов защиты информации {с элементами электронного обучения и дистанционных образовательных технологий} (2ч.)[2,3,4,5] Современное состояние криптографии и предстоящие вызовы. Стеганография. Цифровой водяной знак, защита авторских прав. Платежные системы. Технология блокчейн. Электронные деньги. Криптовалюты. Квантовая криптография.

Лабораторные работы (32ч.)

- 1. Классические шифры(4ч.)[1,2]** Взлом шифра простой замены. Шифрование методом Вижинера.
- 2. Симметричные шифры(4ч.)[1,2]** Программная реализация симметричного алгоритма ГОСТ 28147-89. Использование режимов шифрования.
- 3. Поточные шифры(4ч.)[1,2]** Программная реализация поточного шифра с применением регистра сдвига с обратной связью
- 4. Ассиметричная криптография(4ч.)[1,2,9]** Программная реализация алгоритма распределения ключей Диффи-Хеллмана и алгоритма шифрования RSA. Шифрование информации с использованием отечественного программного обеспечения: КриптоПРО, КриптоАРМ (пробные версии).
- 5. Электронная подпись(4ч.)[1,2,9]** Подписание электронных документов с использованием отечественного программного обеспечения: КриптоПРО, КриптоАРМ (пробные версии).
- 6. Защита электронной почты(4ч.)[1,4]** Шифрование электронных писем. Использование электронной подписи
- 7. Протокол IPSec(4ч.)[1,3]** Установление безопасного соединения в локальной вычислительной сети
- 8. Технологии ViPNet(4ч.)[1,7]** Работа с продуктами компании "Инфотекс"

Самостоятельная работа (80ч.)

- 1. Подготовка к текущим занятиям(44ч.)[1,2,3,4,5,7,8,9]**
- 2. Подготовка к экзамену(36ч.)[1,2,3,4,5,7,8,9]**

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. Прямая ссылка: <http://elib.altstu.ru/eum/download/ivtib/uploads/lenyuk-s-v-ivtib-546aee294c819.pdf>

6. Перечень учебной литературы

6.1. Основная литература

2. Лапони́на, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапони́на ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97571.html> (дата обращения: 24.04.2023). — Режим доступа: для авторизир. пользователей

3. Полянская, О. Ю. Инфраструктуры открытых ключей : учебное пособие / О. Ю. Полянская, В. С. Горбатов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 452 с. — ISBN 978-5-4497-0382-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89439.html> (дата обращения: 23.04.2023). — Режим доступа: для авторизир. пользователей

6.2. Дополнительная литература

4. Басалова, Г. В. Основы криптографии : курс лекций / Г. В. Басалова ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 253 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=233689> (дата обращения: 23.04.2023). – Текст : электронный.

5. Пилиди, В. С. Математические основы защиты информации : учебное пособие : [16+] / В. С. Пилиди ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 309 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=577894> (дата обращения: 09.06.2021). – Библиогр.: с. 301. – ISBN 978-5-9275-3363-3. – Текст : электронный.

6. 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.

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

7. Официальный сайт компании "Инфотекс" <https://infotecs.ru/>
8. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/fsb.htm>
9. Официальный сайт компании "КриптоПро" <https://www.cryptopro.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	Acrobat Reader
1	LibreOffice
2	Windows
2	FAR Manager
3	Антивирус Kaspersky
4	Microsoft Office
5	Mozilla Thunderbird
6	ViPNet client (демо-версия)
7	ViPNet Coordinator (демо-версия)
8	ViPNet CSP
10	WinRAR
12	КриптоАРМ Старт

№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 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».