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.В.4 «Организация и технология защиты информации»**

Код и наименование направления подготовки (специальности): **09.03.04 Программная инженерия**

Направленность (профиль, специализация): **Разработка программно-информационных систем**

Статус дисциплины: **часть, формируемая участниками образовательных отношений (вариативная)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	В.С. Троицкий
Согласовал	Зав. кафедрой «ПМ»	Е.Г. Боровцов
	руководитель направленности (профиля) программы	С.А. Кантор

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
ПК-1	готовностью применять основные методы и инструменты разработки программного обеспечения	Знать основные методы разработки программного обеспечения с использованием инструментальных средств, в том числе методы обеспечения защиты информации в разрабатываемых приложениях.	Уметь использовать основные методы и инструменты разработки программного обеспечения, в том числе, программные средства, реализующие основные криптографические функции.	Владеть простейшими методами и инструментами разработки программного обеспечения, в том числе, навыками в выборе, разработке и применении эффективных методов защиты информации в разрабатываемых приложениях.
ПК-4	владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	Знать концепции и атрибуты качества программного обеспечения, в том числе, критерии оценки защищенности систем, основные подходы к организации защиты, основные понятия информационной безопасности.	Эксплуатировать компьютерные системы и сети в соответствии с принятыми стандартами в области информационной безопасности. Использовать современные системные программные средства для защиты информации; Конфигурировать основные средства защиты информации.	Современной терминологией и методологией в области информационной безопасности; Навыками настройки систем безопасности в современных операционных системах. Первичными навыками в реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Архитектура вычислительных систем, Компьютерные сети и телекоммуникационные технологии, Операционные системы
Дисциплины (практики), для которых результаты освоения	Выпускная квалификационная работа, Информационная безопасность компьютерных систем

данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	и сетей, Научно-исследовательская работа, 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	17	17	0	74	45

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

Форма обучения: очная
Семестр: 6

Лекционные занятия (17ч.)

1. Введение и организационно-правовые механизмы обеспечения информационной безопасности {лекция с разбором конкретных ситуаций} (5ч.)[2,3] Основные понятия и определения. Информация в компьютерных сетях и ее свойства. Виды и источники угроз информационной безопасности. Основные направления обеспечения информационной безопасности. Комплексный подход к обеспечению информационной безопасности. Меры противодействия угрозам безопасности (Морально-этические меры, правовые меры, организационные меры, технологические меры, технические меры, физические меры и.др.). Концепция информационной безопасности. Формальная теории защиты информации. Концепции и атрибуты качества программного обеспечения, в том числе, критерии оценки защищенности систем.

Информация как товар. Экономические проблемы информационной защиты. Страхование как метод защиты информации. Экономическая эффективность защиты информации. Виды ущерба от несанкционированного доступа (НСД) к информации. Методы оценки ущерба от НСД. Основные методы определения

затрат на информационную безопасность. Оценка экономического эффекта защиты информации. Экономическая эффективность инвестиций в защиту информации.

Правовое обеспечение информационной безопасности. Информация как объект правового регулирования. Законодательство РФ в области информационной безопасности. Лицензирование и сертификация в области информационной безопасности. Компьютерные правонарушения. Основы организационного обеспечения информационной безопасности.

2. Криптографические методы защиты информации {лекция с разбором конкретных ситуаций} (6ч.)[2,3] Использование криптографических методов и соответствующих инструментальных средств защиты информации в существующих и разрабатываемых приложениях. Основные понятия и определения. История развития криптографии. Классификация криптографических систем. Стеганографические методы защиты конфиденциальности. Стойкость криптографических систем и алгоритмов (теоретическая, практическая, вычислительная). Элементы криптоанализа.

Современные симметричные и асимметричные криптосистемы. Симметричные криптосистемы. Основные свойства симметричных криптосистем. Блочные и поточные шифры. Шифры DES, AES, ГОСТ 28147-89, режимы работы блочных шифров. Поточные шифры.

Асимметричные криптосистемы. Основные свойства асимметричных криптосистем. Однонаправленные функции. Общая схема функционирования систем с открытыми ключами. Криптосистема RSA и криптография с использованием эллиптических кривых. Комбинированные криптосистемы. Надежность криптосистем.

Функции хэширования. Основные свойства хэш-функций. Функция хэширования SHA, MD5, ГОСТ Р 34.11-94. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Ключевые и бесключевые функции хэширования.

Управление ключами. Генерация и хранение ключей. Распределение ключей. Выбор ключа, время жизни ключа, разделение секрета. Схемы обмена секретными ключами. Управление ключами в системах с открытым ключом.

Методы обеспечения целостности. Электронно-цифровая подпись(ЭЦП). Схема ЭЦП. Электронные сертификаты. Назначение. Схемы управления: централизованная (стандарт X509), распределённая (стандарт OpenPGP). Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи. Примеры применения ЭЦП и электронных сертификатов (IPSec, VPN, Электронные деньги и пр.).

3. Безопасность компьютерных систем и сетей {лекция с разбором конкретных ситуаций} (6ч.)[2,3] Использование инструментальных средств защиты информации в сетевых приложениях. Общие вопросы безопасности в ЛВС. Классификация сетевых атак. Средства защиты. Аутентификация и

управление идентификациями. Аутентификация на основе одноразовых и многоразовых паролей. Биометрическая идентификация и аутентификация пользователя. Аутентификация, основанная на симметричных и асимметричных алгоритмах. Протоколы аутентификации и идентификации. Взаимная проверка подлинности. Протоколы обмена и распределения ключей. Хранение учетных записей.

Основные схемы сетевой защиты. Сегментирование сетей на канальном уровне. Межсетевые экраны. Системы обнаружения и предотвращения проникновений. Приоритезация трафика и создание альтернативных маршрутов. Технологии туннелирования.

Принципы и средства защиты электронной почты, Web-технологий, VoIP, Wifi.

Вредоносное программное обеспечение. Классификация вредоносного ПО, механизмы его воздействия на телекоммуникационные и вычислительные системы. Методы и средства борьбы с вредоносным ПО.

Резервное копирование. Подсистема хранения данных. Уровни резервного копирования. Виды резервного копирования. Резервное копирование на физическом уровне, технология RAID. Надёжное удаление информации с носителей. Методы и инструменты разработки программного обеспечения для защиты информации. Концепции и атрибуты качества создаваемого программного обеспечения

Лабораторные работы (17ч.)

1. Обеспечение личной информационной безопасности в современном обществе {работа в малых группах} (1ч.)[1] Понять роль людей, процессов, методов, инструментов и технологий в обеспечении личной информационной безопасности.

Перед студентами ставится задача собрать и систематизировать как можно больше информации друг о друге с использованием общедоступных Интернет-ресурсов, оценить угрозу злоумышленного применения информации и выработать рекомендации по обеспечению необходимого уровня безопасности частной жизни в мире цифровых зависимостей.

- Для выполнения лабораторной работы студенты разбиваются на пары.
- Первая задача: найти как можно больше личной информации о коллеге, используя общедоступные сетевые ресурсы:
- Систематизировать собранную информацию
- Оценить возможность использования найденной информации злоумышленниками
- Передать собранные материалы "коллеге" и получить досье с информацией о себе
- Оценить уровень конфиденциальности, актуальности и достоверности собранной информации
- Проанализировать выводы коллеги о возможности использования найденной

информации злоумышленниками

•Оценить уровень влияния цифровых технологий на свою частную жизнь и продумать шаги по обеспечению желаемого уровня безопасности

2. Разработка ПО (утилита или вебсервис) для автоматизации поиска некоторой информации о человеке в сети Интернет {творческое задание} (2ч.)[1] В предыдущей лабораторной работе вы, используя общедоступные Интернет-ресурсы собирали и систематизировали информацию о вашем друге. Это делалось либо в ручном режиме, либо с использованием специальных утилит и сервисов.

В данной лабораторной работе вам предлагается разработать ПО (утилита или вебсервис) для автоматизации поиска некоторой информации о человеке в сети Интернет. Объем исходных данных, степень автоматизации поиска, анализа и систематизации можете выбрать самостоятельно.

Например:

- ПО для формирования досье по ФИО основываясь на данных сайта АлтГТУ;
- ПО для построения графа дружеских/родственных связей заданного человека по данным социальной сети ОДНОКЛАССНИКИ;
- Геолокация по геотегам фотографий для заданой учетной записи социальной сети.

Для выполнения лабораторной работы вам необходимо:

1) Определить какую именно информацию будете искать, как и где будет вестись поиск;
2) Разработать ПО для поиска, анализа и систематизации;
3) Продемонстрировать ПО преподавателю и ответить на возникшие вопросы;
4) Оформить отчет по проделанной работе.

3. Криптоанализ классических шифров {творческое задание} (2ч.)[1] Научиться разрабатывать программные средства, реализующие основные криптографические функции, а именно:

1) Разработать программу для распознавания открытого текста (уметь отличать открытый текст от случайной последовательности знаков). Критерии распознавания выбираются студентом самостоятельно.
2) Криптоанализ шифра столбцовой перестановки (переставлены столбцы) и двойной перестановки (сначала были переставлены столбцы, затем строки). Текст содержит 25 символов и записан в квадратную матрицу 5x5. Написать программу для криптоанализа этого шифра.
3) Криптоанализ шифра простой замены. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка известна. Написать программу для криптоанализа этого шифра.
4) Криптоанализ шифра Виженера. Программа должна определить ключевое слово и восстановить открытый текст (пробел является частью алфавита).

4. Стандарты симметричного шифрования {творческое задание} (4ч.)[1] Научиться разрабатывать программные средства, реализующие основные криптографические функции, а именно:

Реализовать приложение для шифрования, позволяющее выполнять следующие действия:

•Шифровать данные по заданному в варианте алгоритму: шифруемый текст должен храниться в одном файле, ключ шифрования – в другом, зашифрованный текст - в третьем; предусмотреть возможность просмотра и изменения ключа, шифруемого и зашифрованного текстов в шестнадцатеричном, двоичном и символьном виде; программа должна показывать время шифрования.

•Исследовать лавинный эффект (исследования проводить на одном блоке текста): для бита, который будет изменяться, приложение должно позволять задавать его позицию (номер) в открытом тексте или в ключе; приложение должно уметь после каждого раунда шифрования подсчитывать число бит, изменившихся в зашифрованном тексте при изменении одного бита в открытом тексте либо в ключе; приложение может строить графики зависимости числа бит, изменившихся в зашифрованном тексте, от раунда шифрования, либо графики можно строить в стороннем ПО, но тогда приложение для шифрования должно сохранять в файл необходимую для построения графиков информацию.

Реализовать приложение для дешифрования, позволяющее выполнять следующие действия:

•Дешифровать данные по заданному в варианте алгоритму: зашифрованный текст должен храниться в одном файле, ключ – в другом, расшифрованный текст в третьем; в процессе дешифрования предусмотреть возможность просмотра и изменения ключа, зашифрованного и расшифрованного текстов в шестнадцатеричном, двоичном и символьном виде.

С помощью реализованных приложений выполнить следующие задания:

•Протестировать правильность работы разработанных приложений.

•Исследовать лавинный эффект при изменении одного бита в открытом тексте и в ключе: построить графики зависимостей числа бит, изменившихся в зашифрованном сообщении, от раунда шифрования (всего должно быть построено 2 графика).

Варианты

Для нечётных номеров в списке алгоритм DES, а для чётных – ГОСТ.

5. Алгоритм шифрования RSA {творческое задание} (4ч.)[1] Научиться разрабатывать программные средства, реализующие основные криптографические функции, а именно:

Ознакомиться с методическими указаниями http://window.edu.ru/resource/762/66762/files/Algoritm_RSA.pdf

где приведено описание алгоритма RSA и популярные атаки на алгоритм, а также практическая часть состоящая из 7 заданий (лабораторных работ). За выполнение первых 4-х получите по 10 баллов за каждое задание, за последние 3 по 20 баллов за каждое задание. Варианты заданий выбирать в соответствии с номером в

списке группы.

6. Анализ уязвимостей информационной системы методом "тестирование на проникновение" {творческое задание} (4ч.)[1] Научиться эксплуатировать компьютерные системы и сети в соответствии с принятыми стандартами в области информационной безопасности и применять эффективные методы защиты в разрабатываемых приложениях. Для этого используйте следующий метод оценки защищенности:

Тестирование на проникновение – это метод оценки защищенности компьютерной системы или сети, основанный на имитации действий внешнего злоумышленника не обладающего правами на доступ к системе. Лабораторная работа состоит из нескольких частей и предполагает создание ПО для компрометации некоторой информационной системы (на выбор обучающегося), его применение с целью получения несанкционированного доступа к ресурсам этой информационной системы и разработку рекомендаций по улучшению механизмов обеспечения информационной безопасности в выбранной информационной системе.

Самостоятельная работа (74ч.)

1. Изучение дополнительной литературы(10ч.)[2,3,4,5,6]

2. Подготовка к лабораторным работам(55ч.)[1,2,3,4,5,6]

3. Подготовка к зачету(9ч.)[1,2,3,4,5,6]

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. Троицкий В.С. Организация и технология защиты информации [Электронный ресурс]: Методические указания к выполнению лабораторных работ / В.С.Троицкий. –Барнаул 2015: АлтГТУ, 8 с. Прямая ссылка: http://elib.altstu.ru/eum/download/pm/troickii_otzi.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк [и др.] ; под ред. Горбатова В.С.. — Электрон. дан. — Москва : Горячая линия-Телеком, 2018. — 288 с. — Режим доступа: https://e.lanbook.com/book/111075. — Загл. с экрана.

3. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014.

— 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

6.2. Дополнительная литература

4. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032. — Загл. с экрана.

5. Бирюков, Андрей Александрович. Информационная безопасность: защита и нападение [Электронный ресурс] / А. А. Бирюков. - Электрон. текстовые дан. - Москва : ДМК Пресс, 2012. - 474 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990. - ISBN 978-5-94074-647-8 : Б. ц.

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

6. Видео лекции по изучаемой теме на www.youtube.com, например https://www.youtube.com/watch?v=_B1jt1VPEz8

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	Android Studio
2	Eclipse IDE
3	Visual Studio
4	Qt Creator Open Source
5	Linux
6	Windows

№пп	Используемое программное обеспечение
7	LibreOffice
8	Антивирус Kaspersky
9	Chrome

№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
лаборатории
помещения для самостоятельной работы
учебные аудитории для проведения текущего контроля и промежуточной аттестации

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».