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.7 «Защита 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**

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 индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ПК-6	Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	ПК-6.1	Определяет атрибуты качества программного обеспечения
		ПК-6.2	Использует методы, инструменты и технологии обеспечения качества программного обеспечения

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Архитектура ЭВМ, Программирование
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Выполнение и защита выпускной квалификационной работы, 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: 5 / 180
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	24	24	0	132	62

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

Форма обучения: очная
Семестр: 8

Лекционные занятия (24ч.)

1. Основные понятия и определения {лекция с разбором конкретных ситуаций} (2ч.)[2] Информация (сигнал->данные->информация->знания). Носители информации, способы ее обработки и передачи (история). Информация в цифровом виде. Понятие "Защита информации". Краткий обзор правовых, организационных и технических мер. Экономические проблемы защиты информации.

2. Правовые методы защиты информации {лекция с разбором конкретных ситуаций} (1ч.)[2] Краткий обзор законодательных и нормативно правовых документов, регулирующих отношения в области защиты информации. Федеральный закон N 149-ФЗ. Виды информации для которых установлены конкретные требования по защите. Ответственность за нарушение таких требований. Регуляторы.

3. Организационные методы (мероприятия) защиты информации {лекция с разбором конкретных ситуаций} (1ч.)[2] Комплексный подход к обеспечению информационной безопасности. Что относится к организационным мероприятиям. Преимущества и недостатки организационных мер. Концепция информационной безопасности и механизм ее реализации. Алгоритм построения системы информационной безопасности. Формальные теории и стандарты в области защиты информации

4. Технические методы защиты информации и некоторые другие вопросы. {лекция с разбором конкретных ситуаций} (2ч.)[2] Технические средства защиты информации (программные, аппаратные, организационно-технические, инженерно-технические). Требования и рекомендации по технической защите данных. Криптография - основа большинства современных технологий в области защиты информации.

5. Криптографические методы защиты информации {лекция с разбором конкретных ситуаций} (6ч.)[2] Краткая история криптографии от древнего мира до появления электро-механических шифровальных устройств. Криптография Второй мировой войны. Математическая криптография с использованием цифровых электронных устройств (блочные шифры). "Новые направления в криптографии" - криптография с открытым ключом. Современная криптография. Квантовая физика и криптография - квантовая криптография.

6. Организационные вопросы защиты информации при создании приложений {лекция с разбором конкретных ситуаций} (4ч.)[2,3] Безопасность приложений сегодня. Необходимость защиты систем. Активный подход к безопасности
при разработке приложений (Совершенствование процессов, необходимость обучения, проектирование, разработка, тестирование, поставка и сопровождение). Основные принципы безопасности. Моделирование опасностей.

7. Методы безопасного кодирования {лекция с разбором конкретных ситуаций} (6ч.)[2,3,4] Проблема переполнения буфера. Как выбрать механизм

управления доступом. Принцип минимальных привилегий. Подводные камни криптографии. Защита секретных данных. Входные данные и обязательная проверка корректности. Недостатки канонического представления. Ввод в базу данных. Проблемы ввода в Web-среде. Проблемы поддержки других языков. Дополнительные методы создания защищенного кода (Противостояние атакам типа "Отказ в обслуживании", создание безопасного кода в .Net и пр.)

8. Другие вопросы создания защищенного кода {лекция с разбором конкретных ситуаций} (2ч.)[2,3,4] Атрибуты качества программного обеспечения. Методы, инструменты и технологии обеспечения качества программного обеспечения. Тестирование защиты. Анализ безопасности кода. Безопасная установка приложений. Обеспечение конфиденциальности. Общие методы обеспечения безопасности. Документация по безопасности и сообщения об ошибках. Подведение итогов и заключительные замечания.

Лабораторные работы (24ч.)

1. Обеспечение личной информационной безопасности в современном обществе {работа в малых группах} (2ч.)[2] 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 {разработка проекта} (4ч.)[2] 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 {разработка проекта} (4ч.)[2,3,4]
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 {разработка проекта} (4ч.)[2,3,4]
Реализовать приложение для шифрования и дешифрования файлов по заданному криптографическому алгоритму и 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 группы использовать алгоритм DES, а для чётных – ГОСТ.

5. Алгоритм шифрования RSA {творческое задание} (4ч.)[1,2,3,4] 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 . За выполнение первых 4-х - 10 баллов за каждое задание, за последние 3 - 20 баллов за каждое задание. Варианты заданий выбирать в соответствии с номером в списке группы.
6. Проблемы с переполнением буфера {творческое задание} (6ч.)[2,3,4] На примере своих C++ программ продемонстрировать:
1) как переполнение буфера в стеке можно использовать для выполнения произвольного кода (например: запуск на исполнение некоторой функции вашей программы).
2) как переполнение кучи можно использовать для выполнения произвольного кода.
3) как ошибки индексации массива можно использовать для выполнения произвольного кода

Самостоятельная работа (132ч.)
1. Подготовка к лекциям(48ч.)[1,2,3,4,5,6,7]
2. Оформление отчетов по лабораторным работам и подготовка к их защите(48ч.)[1,2,3,4,5,6,7]
3. Подготовка к сдаче экзамена(36ч.)[1,2,3,4,5,6,7]

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: АлтГТУ, 2015. - 8 с.,
Прямая ссылка: http://elib.altstu.ru/eum/download/pm/troickii_otzi.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 (дата обращения: 18.03.2021). — Режим доступа: для авториз. пользователей.

6.2. Дополнительная литература

3. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; под редакцией С. М. Молявко ; перевод с английского В. Д. Хорева. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 482 с. — ISBN 978-5-00101-700-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151552 (дата обращения: 18.03.2021). — Режим доступа: для авториз. пользователей.

4. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 с. — ISBN 978-5-97060-166-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/82817 (дата обращения: 18.03.2021). — Режим доступа: для авториз. пользователей.

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

5. https://www.securitylab.ru/ -Проект компании Positive Technologies. Помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.

6. https://habr.com/ru/hub/infosecurity/ -Популярный хаб сайта geektimes.ru про информационную безопасность.

7. http://cyberrus.com/ -Научный журнал «Вопросы кибербезопасности»

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	LibreOffice
2	Mozilla Firefox
3	Visual Studio
4	Windows
5	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/)
3	Программа Microsoft и интернет-ресурс, содержащий техническую информацию, новости и предстоящие события для профессионалов в сфере информационных технологий. На данный момент представляет собой сборник технической информации на русском языке для IT-специалистов (https://technet.microsoft.com/ru-ru/ https://docs.microsoft.com/ru-ru/welcome-to-docs)

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».