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.ДВ.9.2 «Информационная безопасность компьютерных систем и сетей»**

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

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

Статус дисциплины: **дисциплины (модули) по выбору**

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
ОПК-1	владением основными концепциями, принципами, теориями и фактами, связанными с информатикой	Знать основные концепции, принципы и факты, связанные с информатикой, в том числе, основные понятия, принципы и концепции информационной безопасности.	Уметь использовать основные концепции, принципы и факты, связанные с информатикой, в том числе, применять организационные и технические меры, направленные на обеспечение защиты информации.	Современной терминологией и методологией в области информационной безопасности; Первичными навыками в реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты информации;
ПК-2	владением навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных	Знать методы использования операционных систем, сетевых технологий, в том числе, основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах, СУБД и серверах приложений, современные возможности и направлениях развития аппаратных и программных средств защиты информации, основные подходы к организации защиты телекоммуникационн ых и вычислительных систем.	Уметь использовать операционные системы и сетевые технологии, в том числе, эксплуатировать компьютерные системы и сети в соответствии с принятыми стандартами в области информационной безопасности, использовать современные системные программные средства для защиты информации, эксплуатировать основные средства защиты информации, пользоваться программными средствами, реализующими основные криптографические функции.	Владеть навыками использования операционных систем, сетевых технологий, в том числе, навыками настройки систем безопасности в современных операционных системах, навыками в выборе, разработке и применении эффективных методов защиты компьютерных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Архитектура вычислительных систем, Операционные системы, Организация и технология защиты информации, Теоретические основы информатики
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Выпускная квалификационная 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: 2 / 72
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	13	26	0	33	44

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 (13ч.)

1. Обеспечение безопасности в компьютерных системах и сетях {лекция с разбором конкретных ситуаций} (2ч.)[2,3] методы использования операционных систем, сетевых технологий, в том числе, основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах. Основные концепции, принципы, и факты информатики, связанные с безопасностью ОС. Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.

Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Сетевые угрозы, уязвимости и атаки. Средства защиты сетей.

2. Назначение, возможности, и основные защитные механизмы межсетевых экранов (МЭ) {лекция с разбором конкретных ситуаций} (2ч.)[2,3] Методы использования сетевых технологий, в том числе, назначение и виды МЭ. Основные защитные механизмы, реализуемые МЭ. Основные возможности и варианты размещения МЭ. Достоинства и недостатки МЭ. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, script rejection, проверка почты, виртуальные частные сети, противодействие атакам, нацеленным на нарушение работоспособности сетевых служб, дополнительные функции. Общие рекомендации по применению. Политика безопасности при доступе к сети общего пользования. Демилитаризованная зона. Назначение, особенности и типовая схема "HoneyNet".

3. Анализ содержимого почтового и Web-трафика (Content Security) {лекция с разбором конкретных ситуаций} (1ч.)[2,3] Методы использования сетевых технологий, в том числе, использование систем анализа содержимого. Компоненты и функционирование систем контроля контента (электронная почта и HTTP-трафик). Политики безопасности, сценарии и варианты применения и реагирования.

4. Виртуальные частные сети (VPN) {лекция с разбором конкретных ситуаций} (1ч.)[2,3] Методы использования сетевых технологий, в том числе, назначение, основные возможности, принципы функционирования и варианты реализации VPN. Структура защищенной корпоративной сети. Варианты, достоинства и недостатки VPN-решений. Общие рекомендации по их применению. Решение на базе ОС Windows. VPN на основе аппаратно-программных комплексов шифрования. Угрозы, связанные с использованием VPN.

5. Антивирусные средства защиты {лекция с разбором конкретных ситуаций} (2ч.)[2,3] Методы использования операционных систем, в том числе, общие правила применение антивирусных средств. Технологии обнаружения вирусов. Возможные варианты размещение антивирусных средств. Антивирусная защита, как средство нейтрализации угроз.

6. Обнаружение и устранение уязвимостей {лекция с разбором конкретных ситуаций} (2ч.)[2,3] Основные концепции, принципы работы и классификация средств анализа защищенности. Место и роль в общей системе обеспечения безопасности. Сравнение возможностей с межсетевыми экранами. Средства обеспечения адаптивной сетевой безопасности. Варианты решений по обеспечению безопасности сети организации. Обзор средств анализа защищенности сетевого уровня и уровня узла. Специализированный анализ защищенности.

7. Мониторинг событий безопасности {лекция с разбором конкретных ситуаций} (1ч.)[2,3] Методы использования журналов событий в операционных системах и сетевых технологиях. Способы построения, дополнительные компоненты и реализация инфраструктуры управления журналами событий.

Технология обнаружения атак. Классификация систем обнаружения атак. Специализированные системы обнаружения атак.

8. Безопасность IP-телефонии {лекция с разбором конкретных ситуаций} (1ч.)[2,3] Методы использования сетевых технологий для передачи голоса и их защита. Основные понятия и определения VoIP. Основные протоколы VoIP. Уязвимости и атаки на VoIP. Инвентаризация VoIP сети. Перехват VoIP-трафика. Манипулирование в системах VoIP. Атаки на протокол передачи трафика реального времени RTP (Real-Time Protocol). Спам в VoIP-сетях. Механизмы обеспечения безопасности IP-телефонии. Планирование защищённой сетевой инфраструктуры IP-телефонии. Анализ защищенности VoIP. Криптографическая защита в VoIP сетях.

9. Безопасность беспроводных сетей {лекция с разбором конкретных ситуаций} (1ч.)[2,3] Методы использования беспроводных технологий и их защита. Общие сведения. Введение. Базовые механизмы защиты данных в беспроводных сетях. Защита беспроводных сетей на сетевом уровне. Стандарты WPA (Wi-Fi Protected Access) и 802.11i. Обнаружение атак в беспроводных сетях. Анализ защищённости беспроводных сетей. Сети WPAN. Безопасность Bluetooth. Организация гостевого доступа. Беспроводной доступ с использованием мобильных устройств.

Лабораторные работы (26ч.)

1. Обеспечение защиты ОС от атак {творческое задание} (2ч.)[1,2,3] Научиться использовать механизмы безопасности операционных систем. Произвести настройку Брандмауэра на своем ПК. Произвести настройку механизма «Удаленные сеансы» на своем ПК. Произвести настройку механизма «Удаленные пользователи» на своем ПК (Для ОС Windows).

2. Назначение, возможности, и основные защитные механизмы межсетевых экранов {творческое задание} (2ч.)[1,2,3] Используя литературу и сеть Internet, изучить основные концепции, принципы и факты относящиеся к современным межсетевым экранам и составить реферат с описанием одного из них.

3. Анализ содержимого трафика {работа в малых группах} (4ч.)[1,2,3] Научиться эксплуатировать современные средства защиты информации. А именно, установить, настроить и продемонстрировать преподавателю функционирование любой (на выбор студента) системы контроля контента.

4. Виртуальные частные сети (VPN) {работа в малых группах} (2ч.)[1,2,3] Научиться эксплуатировать современные средства защиты информации, а именно, установить и настроить VPN сервер и клиента на платформе Windows.

5. Средства защиты компьютера от вирусов. Работа с антивирусными пакетами {творческое задание} (4ч.)[1,2,3] Подготовить доклад на тему: «Общие сведения и особенности работы антивирусной программы [Название антивирусной программы]» (Название антивирусной программы выбрать согласно своему варианту из Вариантов заданий к работе). Исследовать вредоносную программу (архив с программой выдается). Составить отчет.

6. Обнаружение и устранение уязвимостей {творческое задание} (2ч.)[1,2,3] Используя литературу и сеть Internet, изучить современные средства анализа защищенности и составить реферат с описанием одного из них.
7. Мониторинг событий безопасности {творческое задание} (2ч.)[1,2,3] Используя литературу и сеть Internet, изучить современные средства обнаружения атак и составить реферат с описанием одного из них.
8. Безопасность IP-телефонии {работа в малых группах} (4ч.)[1,2,3] Продемонстрировать перехват и запись VoIP-трафика (программа для перехвата и записи на диск VoIP трафика выбирается студентом самостоятельно).
9. Безопасность беспроводных сетей {работа в малых группах} (4ч.)[1,2,3] Научиться эксплуатировать современные средства защиты информации, а именно, показать на практике применение одного (на выбор студента) свободно распространяемого инструмента аудита беспроводных сетей.

Самостоятельная работа (33ч.)
1. Изучение дополнительной литературы(10ч.)[2,3,4,5,6]
2. Подготовка к лабораторным работам(10ч.)[1,2,3,4,5,6]
3. Оформление комплексного отчета по лабораторным работам, подготовка к зачету(13ч.)[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. http://elib.altstu.ru/eum/download/pm/troickii_otzi.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем [Электронный ресурс] : методические указания / В.В. Бондарев. — Электрон. дан. — Москва : МГТУ им. Н.Э. Баумана, 2016. — 250 с. — Режим доступа: https://e.lanbook.com/book/103554. — 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. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А.С. Масалков. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 226 с. — Режим доступа: https://e.lanbook.com/book/105842. — Загл. с экрана.

5. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.

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

6. ИНТУИТ. Курс "Основы информационной безопасности" https://www.intuit.ru/studies/courses/10/10/info

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	NetBeans IDE
2	Windows
3	Mozilla Firefox
4	LibreOffice
5	Visual Studio
6	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
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».