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.15 «Безопасность и защита информации в информационных системах»**

Код и наименование направления подготовки (специальности): **09.04.01 Информатика и вычислительная техника**

Направленность (профиль, специализация): **Программно-техническое обеспечение автоматизированных систем**

Статус дисциплины: **обязательная часть**

Форма обучения: **очная**

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

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ОПК-5	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.1	Выбирает средства автоматизации разработки и модернизации программного и аппаратного обеспечения
ОПК-6	Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ОПК-6.1	Разрабатывает компоненты программно-аппаратных комплексов обработки информации

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Архитектура параллельных вычислительных систем
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	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: 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	16	32	0	96	57

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

Форма обучения: очная
Семестр: 2

Лекционные занятия (16ч.)

1. Обеспечение безопасности межсетевого взаимодействия. Разработка и модернизация программного и аппаратного обеспечения информационных и автоматизированных систем в области обеспечения их безопасности. {беседа} (6ч.)[5,6] Тема 1. Межсетевое взаимодействие. Основы сетевого и межсетевого взаимодействия. Классификация сетевых атак. Информационная безопасность. Тема 2. Политика безопасности. Шаблоны политики безопасности. Сетевая политика безопасности. Эшелонированная оборона. Тема 3. Определение информационных ресурсов, подлежащих защите. Средства автоматизации разработки и модернизации программного и аппаратного обеспечения

2. Межсетевые экраны. {беседа} (4ч.)[5,6] Тема 1. Классификация межсетевых экранов. Пакетные фильтры. Пример набора правил пакетного фильтра. Пакетный фильтр с учетом контекста (Stateful Packet Inspection). Межсетевые экраны host-based. Прокси-сервер прикладного уровня. Тема 2. Различные типы окружений межсетевых экранов. Основные принципы построения окружения межсетевого экрана. Конфигурация с одной DMZ-сетью. Конфигурация Service Leg. Конфигурация с двумя DMZ-сетями.

3. Виртуальные частные сети. {беседа} (4ч.)[5,6,7] Тема 1. Виртуализация. Гипервизоры (Microsoft Hyper-V, VMware ESX, VirtualBOX). Технологии распределённых вычислений. Облачные вычисления. Кластеры. Диагностика сетей (программные, аппаратные и программно-аппаратные комплексы для тестирования и сопровождения сетей). Тема 2. Виртуальные частные сети (VPN). Туннелирование. Протоколы VPN канального уровня. Протокол PPTP. Протокол L2TP. Протокол IPSec. Ассоциация обеспечения безопасности. Тема 3. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Совместное использование протоколов ESP и AH. Основные типы защищенных связей. Протоколы VPN транспортного уровня. Протокол SSL. Протокол SOCKS.

4. Системы обнаружения вторжений (Intrusion Detection Systems). {беседа} (2ч.)[5,6,7] Типы IDS. Архитектура IDS. Способы управления. Информационные источники. Анализ, выполняемый IDS. Возможные ответные действия IDS. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. Цели и задачи использования IDS. Существующая политика безопасности. Развертывание IDS. Сильные стороны и ограниченность IDS.

Лабораторные работы (32ч.)

1. Защита сети и сокрытие ее топологии. FireWall & Proxy-сервис. Разработка компонент программно-аппаратных комплексов обработки информации. {работа в малых группах} (4ч.)[1,2,3,4,12] Обеспечить защиту

локальной сети со стороны сети общего доступа путем установки и настройки межсетевого экрана Iptables и proxy-сервера squid. Задачи лабораторной работы: -закрепление, углубление и расширение знаний в процессе выполнения конкретных практических задач; -развитие профессиональных навыков, практическое овладение методами экспериментальных исследований в области администрирования компьютерных сетей; -обработки и представления результатов проведенных исследований и формирования выводов; -приобретение умений и навыков в настройке прокси сервера; -приобретение умений и навыков в настройке межсетевого экрана – фаэрвола Iptables.

2. Настройка системы обнаружения сетевых атак Snort {работа в малых группах} (4ч.)[2,3,5,7] Изучение и практическое применение системы обнаружения сетевых атак Snort. Задание к выполнению работы: Установить на сервер необходимую оснастку; В соответствие с вариантом настроить на сервере правила; Проверить работоспособность созданного сервера.

3. Организация VPN средствами СЗИ Vipnet. {работа в малых группах} (4ч.)[2,3,5,7] Изучение принципов построения виртуальных частных сетей средствами СЗИ Vipnet. Указания для выполнения работы: -установить на сервер необходимую оснастку; -в соответствии с вариантом работы настроить на сервере требуемые правила; проверить работоспособность созданного сервера.

4. Защита сети средствами DLP {работа в малых группах} (4ч.)[2,3,5,7] Указания для выполнения работы: -установить на сервер необходимую оснастку; -в соответствии с вариантом работы настроить на сервере требуемые правила; -проверить работоспособность созданного сервера.

5. Сканер уязвимостей OpenVas 8.0 {работа в малых группах} (4ч.)[2,3,4,7] Приобретение навыков сканирования компьютера с целью поиска и устранения уязвимостей. Указания для выполнения лабораторной работы: 1) Установить OpenVas на компьютер; 2) Создать новую политику и задачу сканирования в соответствии с вариантом работы; 3) Провести сканирование одного или нескольких компьютеров; 4) Просмотреть результаты сканирования; 5) Проанализировать полученные результаты.

6. Тестирование безопасности паролей системных служб и приложений путем эмуляции атак. {работа в малых группах} (4ч.)[2,3,4,7] Приобретение навыков проверки безопасности паролей системных служб и приложений на предмет подверженности взлому. Указания для выполнения лабораторной работы: 1) На компьютере под управлением операционной системы Windows XP/7 создать 3 учетные записи, для администратора и одного пользователя установить пароли, вход для второго пользователя сделать без пароля, так же на этом компьютере нужно развернуть FTP-сервер и создать двух клиентов: root и обычного пользователя; 2) С помощью программы Hydra с компьютера под управлением Kali Linux произвести тесты по перехвату паролей по SMB и FTP протоколу с помощью созданного и скаченного словаря паролей; 3) Установить на учетные записи более сложные пароли и повторить пункт 2, затем установить ограничения на количество попыток ввода пароля при аутентификации ОС и повторить пункт 2.

7. Тесты на проникновения СУБД MySQL {работа в малых группах} (4ч.)[3,4,7] Приобретение навыков проверки безопасности СУБД MysSQL на предмет подверженности взлому. Указания к выполнению лабораторной работы: 1) Установить и настроить MySQL Server 5.1; 2) Создать базу данных с 2 двумя таблицами, наполнить их информацией, а так же создать дополнительного пользователя admin без пароля, чтобы он мог подключаться только из localhost; 3) С помощью утилит Metaslpoit Framework и HexorBase получить доступ к MySQL серверу; 4) Подключиться к серверу с нескольких пользователей; 5) Показать пример работы с базой данных (удаление записей, таблиц, добавление и удаление пользователей, сохранение базы на компьютер); 6) Усложнить пароль для администратора и повторить пункты 3-5.

8. Обеспечение защиты от DoS-атак {работа в малых группах} (4ч.)[3,4,7] Приобретение навыков обеспечения защиты от атак типа отказ – в – обслуживании на примере веб-сервера apache2. Указания для выполнения лабораторной работы: 1) На компьютере под управлением операционной системы Windows Server 2016 настроить терминальный доступ и проверить его работоспособность с компьютеров-клиентов под управлением Windows и Ubuntu; 2) С помощью программы Torshammer, установленной на компьютере под управлением Kali Linux 2.0 произвести эмуляцию DoS-атаки на Windows Server 2003 до отказа-в-обслуживании сервера терминального доступа; 3) На компьютере под управлением Ubuntu установить и настроить веб-сервер apache2; 4) Провести тесты DoS-атак типа SYN и HTTP флуд программами Torshammer, PyLoris, Slowhttptest, установленные на компьютере под управлением Kali Linux 2.0; 5) Обнаружить данные атаки, реализовать меры по защиты от будущих подобных атак и проверить работоспособность реализованных мер.

Самостоятельная работа (96ч.)

1. Подготовка к лекциям. {с элементами электронного обучения и дистанционных образовательных технологий} (16ч.)[5,6,7,9]

2. Подготовка к защите лабораторных работ {использование общественных ресурсов} (44ч.)[1,2,3,4,10,11,12,13,14,15,16]

3. Подготовка к промежуточной аттестации (экзамен). {использование общественных ресурсов} (36ч.)[5,6,7,8,9]

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. Чугунов Г.А., Методические указания по выполнению лабораторных

работ по дисциплине «Сети и телекоммуникации». – Барнаул: Изд-во АлтГТУ, 2012. – 17с.; Источник: электронная библиотека образовательных ресурсов АлтГТУ. Реж.доступа http://elib.altstu.ru/eum/download/vsib/tugunov-sit.pdf

2. Шарлаев Е.В. Вычислительные сети. Учебно-методическое пособие/ Е.В. Шарлаев; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2015. - 86 с.;Источник: электронная библиотека образовательных ресурсов АлтГТУ. Реж. доступа http://elib.altstu.ru/eum/download/ivtib/uploads/sharlaev-e-v-ivtiib-569e03fec1d87.pdf

3. Шарлаев Е.В. Администрирование глобальных вычислительных сетей: Учебно-методическое пособие.- Барнаул, АлтГТУ, 2010. -122с. Источник: электронная библиотека образовательных ресурсов АлтГТУ. Режим доступа http://new.elib.altstu.ru/eum/download/vsib/sharlaev_gvs.pdf (Методические указания к выполнению лабораторных работ)

4. Рыбин В.В., Шарлаев Е.В. Безопасность вычислительных сетей. Лабораторный практикум: учебно-методическое пособие; Алт. гос. техн. ун–т им. И.И. Ползунова, - Барнаул: 2017. - 71 с.; Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/RybinSharlaev_BezopVSLP_ump.pdf

6. Перечень учебной литературы

6.1. Основная литература

5. Зензин, А.С. Информационные и телекоммуникационные сети: учебное пособие / А.С. Зензин; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск: НГТУ, 2011. - 80 с.: табл., схем. - ISBN 978-5-7782-1601-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228912 (15.05.2019).

6. Сети и телекоммуникации : учебное пособие для бакалавров / составители И. В. Винокуров. — Москва : Ай Пи Ар Медиа, 2022. — 105 с. — ISBN 978-5-4497-1418-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/115699.html (дата обращения: 15.02.2022). — Режим доступа: для авторизир. пользователей

7. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102069.html (дата обращения: 15.02.2022). — Режим доступа: для авторизир. пользователей

6.2. Дополнительная литература

8. Проскуряков, А.В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : [16+] / А.В. Проскуряков. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 202 с. : ил. –

Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=561238 (дата обращения: 23.04.2021). – Библиогр.: с. 195-196. – ISBN 978-5-9275-2792-2. – Текст : электронный.

9. Гурчикова, А.С. Состав и функции сетевого оборудования ККС/ А.С. Гурчикова. -Москва: Лаборатория книги, 2012. -134 с.: табл., схем. - ISBN 978-5-504-00259-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=142472

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

10. Интернет-сайт открытого программного обеспечения OpenNET (http://opennet.ru/)

11. Интернет-сайт компании Cisco-Россия (http://www.cisco.ru/)

12. Операционная система Linux Ubuntu (http://www.ubuntu.com)

13. Программный продукт виртуализации для операционных систем http://www.virtualbox.org)

14. Сетевой сканер Nmap (http://nmap.org)

15. Анализатор сетевого трафика Wireshark (http://www.wireshark.org)

16. Графический симулятор сети GNS3 (http://www.gns3.net)

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
1	Cisco Packet Tracer
2	Debian
2	Windows

№пп	Используемое программное обеспечение
3	Dev-C++
3	Антивирус Kaspersky
4	Dia
5	FreeBSD
6	GIMP
7	Git
8	Hyper-V Server
9	Kaspersky Endpoint Security для бизнеса Расширенный
11	Linux
12	Mozilla Firefox
13	PostgreSQL
14	Qt Creator Open Source
15	SQLite
16	Squid
17	ViPNet client (демо-версия)
18	ViPNet Coordinator (демо-версия)
19	ViPNet CSP
20	VirtualBox
22	Windows Server
23	Wine
24	Wireshark
25	Xen
27	7-Zip

№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».