УТВЕРЖДЕНО

решением Учёного совета факультета математики, информационных и авиационных технологий

от «21» июня 2019 г., протокол № 5/19

Председатель _____/ М.А. Волков

«21» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Защита в компьютерных сетях
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Направление (специальность)___ **09.03.03** Прикладная информатика (бакалавриат)___
код направления (специальности), полное наименование

Направленность (профиль/специализация)___ «Информационная сфера»_____
полное наименование

Форма обучения___очная_____
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «1»_сентября 2019 г.

Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент
Клочков Андрей Евгеньевич	ИБ и ТУ	Старший преподаватель

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационные технологии»
/_____/ Андреев А.С. / *(подпись) (Ф.И.О.)*	/_____/ Волков М.А. / *(подпись) (Ф.И.О.)*
« 21 » 06 2019 г.	« 21 » 06 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачи освоения дисциплины:

изучение типовых угроз безопасности в компьютерных сетях;

изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;

приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;

овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;

овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Защита в комьютерных сетях» изучается в 7 семестре и относится к дисциплина по выбору блока Б1 направления подготовки бакалавров 09.03.03 «Прикладная информатика»..

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Информатика и программирование», «Методы программирования и прикладные алгоритмы», «Технология программирования», «Опкрационные системы», « «Инфоромационная безопасность», позволяющими понять физическую сущность безопасности сетей ЭВМ.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информатики и вычислительной техники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при выполнении курсовой работы, выпускной квалификационной работы и в ходе практик.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**

1	2
ПК-7 - способность настраивать, эксплуатировать и сопровождать информационные системы и сервисы	**Знать:** средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций **Уметь:** эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций **Владеть:** навыками обеспечения эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций
ПК-8 - способность проводить тестирование компонентов программного обеспечения ИС	**Знать:** Возможности подсистемы информационной безопасности автоматизированной системы и их тестирования **Уметь:** администрировать и тестировать подсистему информационной безопасности автоматизированной системы **Владеть:** навыками администрирования подсистемы информационной безопасности автоматизированной системы

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	**Количество часов (форма обучения ___*дневная*_____)**			
	Всего по плану	**В т.ч. по семестрам**		
		7семестр		
1	2	3	**4**	5
Контактная работа обучающихся с преподавателем	54	54		
Аудиторные занятия:	54	54		
Лекции	18	18		
Практические и семинарские занятия				
Лабораторные работы	36	36		

(лабораторный практикум)				
Самостоятельная работа	54	54		
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - вопросы при защите лабораторных работ - рефераты на заданные темы		
1	2	3	4	5
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	зачёт	зачёт		
Всего часов по дисциплине:	108	108		

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения _____дневная_____

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинар	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Типовые угрозы сетевой безопасности							
1. Сетевые атаки	4	2				2	Тесты Т1
2. Механизмы реализации атак в сетях TCP/IP	4	2				2	Тесты Т2
3. Методы перехвата сетевых соединений в сетях TCP/IP	6	2		2		2	Тесты Т3
4. Примеры сетевых атак в	12	2		4		6	Тесты Т4,

сетях TCP/IP. Технические меры защиты от сетевых атак							Лаб. Раб. № 1
Раздел 2. Криптографические методы защиты информации в компьютерных сетях							
5. Криптографические протоколы обеспечения безопасности	10	2		2		6	Тесты Т5, Лаб. Раб. № 2
6. Защита виртуальных частных сетей (VPN	12	2		2		8	Тесты Т6, Лаб. Раб. № 3
7. Разработка защищенных сетевых приложений	8	2		2		4	Тесты Т7, Лаб. Раб. № 4
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях							
8. Средства защиты локальных сетей при подключении к Интернет	18	2		2		14	Тесты Т8, Лаб. Раб. № 5
9. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений	16	2		4		10	Тесты Т9, Лаб. Раб. № 6,7
Итого:	108	18		36		54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Типовые угрозы сетевой безопасности

Тема 1. Сетевые атаки

Стадии проведения сетевой атаки. Классификация сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

Тема 2. Механизмы реализации атак в сетях TCP/IP

Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ.

Тема 3. Методы перехвата сетевых соединений в сетях TCP/IP

Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру. Защита от атак.

Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.

Раздел 2. Криптографические методы защиты информации в компьютерных сетях

Тема 5. Криптографические протоколы обеспечения безопасности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Тема 6. Защита виртуальных частных сетей (VPN)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.

Тема 7. Разработка защищенных сетевых приложений

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.

Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях

Тема 8. Средства защиты локальных сетей при подключении к Интернет

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.

Тема 9. Защита серверов и рабочих станций.

Средства и методы предотвращения и обнаружения вторжений. Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Цель. Лабораторный практикум по дисциплине направлен на изучение студентами всех современных подходов для обеспечения информационной безопасности современных операционных систем. Охватывает клиентские операционные системе (на базе Microsoft Windows 10 и Alt Linux), а также серверные операционное системы (на базе Microsoft Server 2026R2 и Alt Linux Server). В соответствии с руководящими документами обучение происходит на сертифицированные версиях операционных систем.

Методология основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Все работы обладают дифференцированной линейно растущей сложностью выполнению и созданы на основе стандартных практических задач современного предприятия. Поиск технической информации, а также подбор необходимого решения производиться

самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и процессе демонстрации полученного решения.
Результат. Полученные решения демонстрируются студентом для каждого из типа операционных систем. При необходимости демонстрируется ход выполнения работы.
Требования к оборудованию. Для выполнения работ студенты используют несколько виртуальных машин с различными версиями операционных систем. Возможно самостоятельное выполнение лабораторных работ вне лаборатории. Компьютер с жестким диском – 100 Gb, ОЗУ: 8 Gb, Windows 10 Pro, BaseAlt (Альт Рабочая станция, Альт сервер), Kali Linux, Oracle Virtual Box, Putty, PGP, Apache, nginx, Statistica, Origin. По желанию студента все виртуальные машины могут быть развернуты на выделенном сервере виртуальных машин в лаборатории. Для моделирования работы сетей используется CISCO Packet Tracer. Сеть лаборатории представляет собой гетерогенную сеть, включающую в себя индивидуальный набор следующего оборудования:

1. Коммутатор L2, L3.
2. Маршрутизатор L3 с функциями VPN.
3. Маршрутизатор Континет КШ 25.
4. Маршрутизатор VipNet Координатор.

Для поддержания работы сетей используется выделенный Коммутатор L3, L3 сконфигурированный для работы независимых сегментов сети.

Требования к оформлению лабораторной работы. Все файлы, используемые в лабораторной работе, должны быть представлены в одном каталоге и иметь наименования, описывающие хранимую в файле информацию. Например: ssh_client_key.txt – содержит информацию о клиентском ключе для SSH. Должен быть файл read.me с текстовым описанием всех настроек, которые были использованы для выполнения лабораторной работы разбитых на секции. Например:

```
[BaseAlt (Альт Рабочая станция, Альт сервер)Server]
IPv4=10.2.0.1/24
DNS=10.2.0.2
gateway: 10.2.0.3
; Обозначение комментария
```

Имена полей должны быть написаны латинскими буквами. Секции могут включать в себя подсекции.

Раздел 1. Типовые угрозы сетевой безопасности

Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Лабораторная работа № 1 (6 часов). **Строение сетей.**

Цель. Изучение базовых механизмов получения информации о конфигурации сети. Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ.
Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

- Для каждой из операционных систем установить следующее программное обеспечение:
  - Сканер безопасности Nmap (ZenMap - с графическим режимом)
  - Wireshark
  - Putty
  - whois

- tranceroute
- nslookup

- Произвести анализ сайта 80.250.180.133. Обнаружить все открытые порты и протоколы. Составить схему расположения данного ресурса. Установить DNS имена расположенных на указанном IP адресе серверов. ь
- Произвести подключение к серверу 62.76.32.162 по протоколу ssh (стандартный порт).
- Произвести перехват пакетов ssh протокола направляемых к данному серверу при помощи Wireshark. Внимание! Необходимо показать перехват пакетов при получение первого ключа шифрования SSH.
- Для обоих серверов указать номер автономной системы и её владельца.
- Подключиться к WiFi сети университета.
- Вычислить IP адрес шлюза выхода в Интернет.
- Определить протокол шифрования трафика.

Раздел 2. Криптографические методы защиты информации в компьютерных сетях

Тема 5. Криптографические протоколы обеспечения безопасности

Лабораторная работа №2 (8 часов). **Удалённый доступ по протоколу SSH.**

Цель. Изучение возможностей протокола SSH для получения удалённого доступа к серверу. возможностей протокола SSH для получения удалённого доступа к серверу *Задача №1.* Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы.

- Установить систему openSSH сервер на ОС BaseAlt (Альт Рабочая станция, Альт сервер) и putty на ОС MS Windows.
- Создать ключ серверного шифрования информации.
- Установить соединение с данным сервером с другого клиента, на котором запущен WireShark. Перехватить ключ серверного шифрования.
- Запретить передачу ключа по отрытому каналу.
- Создать ключ клиента.
- Записать ключ клиента на отчуждаемый носитель информации.
- Установить соединение с другой ОС используя ключ клиента. Перехватить трафик и проанализировать полученные пакеты. Объяснить увиденный результат.
- Создать ключи шифрования на клиенте используя puttyGen. Переписать их на отчуждаемый носитель.
- Установить клиентские ключи шифрования для openSSH.
- Произвести соединение с сервером.

Задача №2. Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы.

- Отключить клиентский компьютер на ОС MS Windows от сети Интернет.
- Настроить работы протокола SSH в режиме PORT FORWARDING.
- Создать «проброс» порта из внутренней защищенной сети через сервер до сайта www.ulsu.ru и протоколов HTTP и HTTPS.
- Перехватить отправленные пакеты с информацией и продемонстрировать использование шифрования информации.

Тема 6. Защита виртуальных частных сетей (VPN)

Лабораторная работа №3 (8 часов). **Использование VPN.**

Цель. Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.
Задача №1. Создание защищенного межсетевого взаимодействия сетей.
Изменить конфигурацию сети.

1. Скачать на локальный жесткий диск три образа операционных систем: MS Windows 10, MS Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер).
2. Отключиться от общей сети лаборатории и включиться в один из маршрутизаторов MicroTik.
3. Назначить порты марштуризатора следующим образом: Порты №1,2 – VLAN1; Порты 3,4 – VLAN2;
4. Подключить виртуальные машины клиентских ОС к VLAN1.
5. Подключить виртуальную машину с сервером к VLAN2.
6. Создать ключи доступа и файлы конфигураций для клиентских компьютеров.
7. Установить VPN клиент и применить файлы конфигурации.
8. Передать файл по протоколу SMB в защищенной сети.

Задача №2. Использование АПКШ «Континент» для создания защищенной сети.
Изменить конфигурацию сети.

1. Подключить порт 3 к VLAN9.
2. Получить ключи шифрования для АПКШ «Континент» Сервер Доступа.
3. Подключить АПКШ «Континент» к VLAN1.
4. Настроить АПКШ «Континент» Сервер доступа в соответствии с руководством администратора.
5. Передать файл по протоколу SMB в защищенной сети.

Тема 7. Разработка защищенных сетевых приложений

Лабораторная работа №4 (8 часов). **Работа с сертификатами SSL.**

Цель. Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем.
Задача. Для выполнения лабораторной работы используются ОС MS Windows и BaseAlt (Альт Рабочая станция, Альт сервер).

- Необходимо установить и настроить следующее программное обеспечение: OpenSSL
- Выдать сертификат SSL на свое имя: SN - должно содержать вашу ФИО. Также сертификат должен содержать ваш действующий EMAIL адрес.
- Скачать сертификат открытого ключа для Корейко Александра Ивановича.
- Установить сертификат в ОС и настроить электронную почту таким образом, чтобы отправляемые письма содержали вашу электронную подпись и были зашифрованы для получателя Корейко Александр Иванович.
- Установить локальный web сервер (apache, nginx).
- Выдать сертификат для локального веб сервера.
- Продемонстрировать работу по безопасному https соединению.

- Отчет по лабораторной работе должен содержать файл электронного письма в формате SMIME, а также файл сертификата.

Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях

Тема 8. Средства защиты локальных сетей при подключении к Интернет

Лабораторная работа №5 (8 часов). **Моделирование виртуальной сети.**

Цель. Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным оборудованием компании CISCO. Решение практических задач.
Задание. Выполняется в программном обеспечении Cisco Packet Tracer

- Ваша фирма переезжает в новый бизнес-центр, где она арендовала 3 помещения, на 1-м, 2-м и 3-м этаже. У вас есть ограниченный набор оборудования:
- 3 коммутатора Cisco 2960
- Маршрутизатор Cisco 1941
- роутер Cisco WRT300N
- Вас попросили разработать схему сети со следующими требованиями:
- Любой компьютер компании может связываться с любым другим компьютером, но при этом, каждое помещение должно быть изолировано.
- На третьем этаже должна быть установлена WiFi точка доступа. Точка должна иметь пароль ulsu30years, должны выдаваться первые 20 адресов. SSID должен быть скрыт.
- На втором этаже установлен WEB сервер. Доступ к нему должны иметь все компьютеры по локальному имени "sharepoint".
- На первом этаже 3 рабочих места, на втором 2 рабочих места и сервер, третий 10 рабочих мест, в том числе 5 беспроводных.
- К сетевому оборудованию должен быть предоставлен безопасный доступ по SSH. Для доступа к оборудованию вас попросили создать административную виртуальную сеть "mi6".

Тема 9. Защита серверов и рабочих станций.

Лабораторная работа №6 (8 часов). **Обнаружение вторжений.**

Цель. Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий.
Задача. Установка и настройка систем обнаружения вторжений в сети. Проведение атаки на защищенный сегмент сети. Для проведения атаки рекомендуется использовать специализированный дистрибутив ОС – Kali Linux.

- На ОС семейства BaseAlt (Альт Рабочая станция, Альт сервер) следует установить и настроить систему обнаружения вторжений Snort
- При помощи утилит предустановленных в дистрибутив Kali Linux произвести атаку на любой свой компьютер, подключенный к системе обнаружения вторжений Snort.

- Показать, как Snort обнаружил атаку на ваш ресурс.
- Создать правило, обнаруживающие ICMP атаки на ваш ресурс.
- Анализировать журнал событий и продемонстрировать обнаружение атаки.

Тема 9. Защита серверов и рабочих станций.

Лабораторная работа №7 (8 часов). **АПКШ «Континент» Обнаружение вторжений**

Цель. Изучение возможностей комплекса АПКШ «Континент» для регистрации вторжений в локальную сеть.
Задача. Ознакомление с сертифицированными системами обнаружения вторжений в сети. Работа с правилами фильтрации и обнаружения атак.
Изменить конфигурацию сети.

1. Отключить рабочую станцию от локальной сети лаборатории и подключиться к маршрутизатору MicroTik.
2. Настроить порты маршрутизатора №1,2,3 в VLAN1.
3. Настроить порт маршрутизатора №4 в режим MIRRORING («зеркалирование»).
4. Подключить АПКШ «Континент» к порту №4.
5. Настроить АПКШ «Континент» Система обнаружения вторжений в режиме PROMISCUOUS_MODE.
6. Произвести ICMP атаку в сети.
7. Продемонстрировать результаты работы правил на АПКШ «Континент».

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Контрольные работы, курсовые работы и рефераты не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Стадии проведения сетевой атаки.
2. Классификация сетевых угроз, уязвимостей и атак.
3. Атаки на реализации сетевых протоколов, отдельные узлы и службы.
4. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
5. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.
6. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.
7. Методы сканирования портов.
8. Методы обнаружения пакетных сниферов. Методы обхода МЭ.
9. Имперсонация вслепую. Десинхронизация TCP-соединений.
10. Атаки, направленные на сетевую инфраструктуру.
11. Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании.
12. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации.
13. Технические меры защиты от сетевых атак.
14. Протоколы аутентификации на прикладном уровне.
15. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS.
16. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.
17. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
18. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN.

19.Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах.
20. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.
21.Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.
22.Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности.
23.Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ.
24.Достоинства и недостатки МЭ. Построение правил фильтрации.
25.Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений.
26.Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.
27.Системы обнаружения вторжений (СОВ).
28.Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
29.Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
30.Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий.
31.Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб.
32.Способы противодействия вторжениям.
33.Системы виртуальных ловушек (Honey Pot и Padded Cell).

8. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Типовые угрозы сетевой безопасности Тема 1. Сетевые атаки	Подготовка к лекции, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 2. Механизмы реализации атак в сетях TCP/IP	Подготовка к лекции, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 3. Методы перехвата сетевых соединений в сетях TCP/IP	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	12	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Криптографические методы защиты информации в компьютерных сетях. Тема 5. Криптогра-	Подготовка к лекции, подготовка к сдаче экзамена	10	Тесты перед лекцией, экзамен

фические протоколы обеспечения безопасности			
Раздел 2. Тема 6. Защита виртуальных частных сетей (VPN)	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	5	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 7. Разработка защищенных сетевых приложений	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	5	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях Тема 8. Средства защиты локальных сетей при подключении к Интернет	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	5	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 3. Тема 9. Защита серверов и рабочих станций	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	9	Тесты перед лекцией, тесты на семинаре, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Запечников С.В., Основы построения виртуальных частных сетей [Электронный ресурс]: Учебное пособие для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И. - 2-е изд., стереотип. - М.: Горячая линия - Телеком, 2011. - 248 с. - ISBN 978-5-9912-0215-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202152.html

2. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html

2. Бирюков А.А. Информационная безопасность: защита и нападение / Бирюков А. А. - Москва: ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785970604359.html

дополнительная

1. Запечников, С. В. Основы построения виртуальных частных сетей : учебное пособие для вузов / Запечников С. В. , Милославская Н. Г. , Толстой А. И. - 2-е изд. , стереотип. - Москва: Горячая линия - Телеком, 2011. - 248 с. - ISBN 978-5-9912-0215-2. - Текст: электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991202152.html

2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

2.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

2.4 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/

3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" [Электронный ресурс] : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий, Каф. информ. безопасности и теории управления. - Электрон. текстовые дан. (1 файл : 352 КБ). - Ульяновск : УлГУ, 2017 URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915/Andreev_2017.pdf

2. Андреев А. С.Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" [Электронный ресурс] / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Ульяновск : УлГУ, 2015. Режим доступа http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf

3. Клочков А. Е. Методические указания для самостоятельной работы студентов по дисциплине «Защита в компьютерных сетях» для студентов бакалавриата по направлению подготовки 09.03.03 «Прикладная информатика» и специалитета по специальности 10.05.01 «Компьютерная безопасность» очной формы обучения / А. Е. Клочков; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 285 КБ). - Текст : электронный. http://lib.ulsu.ru/ProtectedView/Book/ViewBook/10239

Согласовано:

Гл. библиотекарь НБ УлГУ / Полина Н.Ю. / _____ / 05.06.2020
Должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: https://www.biblio-online.ru. – Режим

доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: http://znanium.com. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008. – Режим доступа : для авториз. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2020].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2020]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2020]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение: электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/. – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

7. Электронная библиотека диссертаций РГБ [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2020]. - Режим доступа: https://dvs.rsl.ru.

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

9. Образовательные ресурсы УлГУ:

9.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата

Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

9.2. Образовательный портал УлГУ. – URL: http://edu.ulsu.ru. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

Зам. нач. УИиТ / Клочкова А.В. /_____/ 05.06.2020
Должность сотрудника УИТиТ ФИО подпись дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских, лабораторных занятий: 3/317, 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

Используемые технические средства:

- система защиты конфиденциальной информации и персональных данных «Secret Disk;
- электронный замок "Соболь";
- персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken;
- система защиты от НСД «Dallas Lock»;
- персональное средство криптографической защиты информации «ШИПКА»;
- программно-аппаратный комплекс VipNet».

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО

Разработчик: _____ ст. преподаватель кафедры Клочков Андрей Евгеньевич

подпись должность ФИО