УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Безопасность вычислительных сетей**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	5 - очная форма обучения

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 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	Кафедра информационной безопасности и теории управления	Доцент,Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

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

Задачи освоения дисциплины:

изучение типовых угроз безопасности в вычислительных сетях;

изучение криптографических и программно-аппаратных методов обеспечения

информационной безопасности в вычислительных сетях;

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

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

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность вычислительных сетей» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-12, ОПК-13, ОПК-15.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Безопасность систем баз данных, Безопасность операционных систем, Научно-исследовательская работа, Подготовка к сдаче и сдача государственного экзамена, Программно-аппаратные средства защиты информации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	**знать**: основные принципы обеспечения безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем **уметь**: применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем **владеть**: навыками применения знаний в области безопасности вычислительных сетей, операционных систем и баз данных
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	**знать**: порядок администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем **уметь**: осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем **владеть**: навыками администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, инструментального мониторинга защищенности автоматизированных систем
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	**знать**: порядок диагностики и тестирования систем защиты информации автоматизированных систем **уметь**: организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем **владеть**: навыками организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 9 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 324 часа

Форма обучения: очная

Вид учебной работы	**Количество часов (форма обучения очная)**		
	Всего по плану	**В т.ч. по семестрам**	
		9	**10**
1	**2**	**3**	**4**
Контактная работа обучающихся с преподавателем в соответствии с УП	208	108	100
Аудиторные занятия:	208	108	100
Лекции	76	36	40
Семинары и практические занятия	56	36	20
Лабораторные работы, практикумы	76	36	40
Самостоятельная работа	80	36	44
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование	
Курсовая работа	Курсовая работа	-	Курсовая работа
Виды промежуточной аттестации (экзамен, зачет)	-	-	
Всего часов по дисциплине	324	144	180

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	**Всего**	**Виды учебных занятий**					**Форма текущего контроля знаний**
		Аудиторные занятия			**Занятия в интерактивной форме**	**Самостоятельная работа**	
		Лекции	**Практические занятия, семинары**	**Лабораторные работы, практикумы**			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Раздел 1. Типовые угрозы сетевой безопасности							
Тема 1.1. Сетевые	18	6	6	0	0	6	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
атаки							
Тема 1.2. Механизмы реализации атак в сетях TCP/IP	18	6	6	0	0	6	Тестирование
Тема 1.3. Методы перехвата сетевых соединений в сетях TCP/IP	18	6	6	0	0	6	Тестирование
Тема 1.4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	30	6	6	12	6	6	Тестирование
Раздел 2. Криптографические методы защиты информации в компьютерных сетях							
Тема 2.1. Криптографические протоколы обеспечения безопасности	30	6	6	12	4	6	Тестирование
Тема 2.2. Защита виртуальных частных сетей (VPN)	30	6	6	12	8	6	Тестирование
Тема 2.3. Разработка	24	8	4	8	8	4	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
защищенных сетевых приложений							
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях							
Тема 3.1. Средства защиты локальных сетей при подключении к Интернет	48	16	8	8	0	16	Тестирование
Тема 3.2. Защита серверов и рабочих станций	72	16	8	24	24	24	
Итого подлежит изучению	288	76	56	76	50	80	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Типовые угрозы сетевой безопасности

Тема 1.1. 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 1.2. 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 1.3. Методы перехвата сетевых соединений в сетях TCP/IP

Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру. Защита от атак.Методы перехвата сетевых соединений в сетях TCP/IP

Тема 1.4. 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 2.1. 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 2.2. 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 2.3. 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 3.1. 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 3.2. 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

Раздел 1. Типовые угрозы сетевой безопасности

Тема 1.1. Сетевые атаки

Вопросы к теме:

Очная форма

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.

Тема 1.2. Механизмы реализации атак в сетях TCP/IP

Вопросы к теме:

Очная форма

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

Тема 1.3. Методы перехвата сетевых соединений в сетях TCP/IP

Вопросы к теме:

Очная форма

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

Тема 1.4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Вопросы к теме:

Очная форма

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

Раздел 2. Криптографические методы защиты информации в компьютерных сетях

Тема 2.1. Криптографические протоколы обеспечения безопасности

Вопросы к теме:

Очная форма

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

Тема 2.2. Защита виртуальных частных сетей (VPN)

Вопросы к теме:

Очная форма

1. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
2. Организация туннелирования на различных уровнях модели ISO/OSI.
3. Достоинства и недостатки применения VPN.
4. Протокол IPSEC.
5. Протоколы AH и ESP.
6. Особенности работы протокола IP SEC в туннельном и транспортном режимах.
7. Протокол управления ключами ISAKMP/Oakley.

Тема 2.3. Разработка защищенных сетевых приложений

Вопросы к теме:

Очная форма

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

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

Тема 3.1. Средства защиты локальных сетей при подключении к Интернет

Вопросы к теме:

Очная форма

1. Межсетевые экраны (МЭ).
2. Место и роль МЭ в обеспечении сетевой безопасности.
3. Классификация МЭ.
4. Требования к МЭ.
5. Основные возможности и схемы развертывания МЭ.
6. Достоинства и недостатки МЭ.
7. Построение правил фильтрации.
8. Методы сетевой трансляции адресов (NAT).
9. Шлюзы уровня приложений.
10. Реализация сетевой политики безопасности с использованием МЭ.
11. Методы обхода межсетевых экранов.

Тема 3.2. Защита серверов и рабочих станций

Вопросы к теме:

Очная форма

1. Средства и методы предотвращения и обнаружения вторжений.
2. Системы обнаружения вторжений (СОВ).
3. Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
4. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
5. Классификация СОВ.
6. Выявление атак на основе сигнатур атак и выявления аномалий.
7. Аудит прикладных служб.
8. Средства обнаружения уязвимостей сетевых служб.

9. Способы противодействия вторжениям.
10. Системы виртуальных ловушек (Honey Pot и Padded Cell).

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Строение сетей
Цели: 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.
Содержание: 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.
Результаты: Изучены базовые механизмы получения информации о конфигурации сети. Получены навыки работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729
Удалённый доступ по протоколу SSH
Цели: Изучение возможностей протокола SSH для получения удалённого доступа к серверу. возможностей протокола SSH для получения удалённого доступа к серверу
Содержание: 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.
Результаты: Изучены возможности протокола SSH для получения удалённого доступа к серверу. возможности протокола SSH для получения удалённого доступа к серверу
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729
Использование VPN
Цели: Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи
Содержание: 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.
Результаты: Изучены возможности программного обеспечения VPN для создания защищенных компьютерных сетей. Получены навыки работы со стандартным программным обеспечением для создания защищенных каналов связи
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729
Работа с сертификатами SSL
Цели: Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем
Содержание: 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.
Результаты: Изучены возможности центров сертификации (Certificate Authorities). Получены навыки работы с криптографическими ключами.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729
Моделирование виртуальной сети
Цели: Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным

оборудованием компании CISCO. Решение практических задач
Содержание: 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".
Результаты: Студенты ознакомлены с методами моделирования сетей, с телекоммуникационным оборудованием. Получены навыки решения практических задач
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729
Обнаружение вторжений
Цели: Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий
Содержание: 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.
Результаты: Изучены возможности современного программного обеспечения для обнаружения вторжений. Освоены работа с правилами безопасности, анализ журналов событий
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729
АПКШ «Континент» Обнаружение вторжений
Цели: Изучение возможностей комплекса АПКШ «Континент» для регистрации вторжений в локальную сеть
Содержание: 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».
Результаты: Изучены возможности комплекса АПКШ «Континент» для регистрации вторжений в локальную сеть
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10729

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы курсовой работы

Тема 1. Разработка защищённой системы контроля компьютеров, периферийного оборудования и программного обеспечения в доменной сети
Тема 2. Разработка лабораторного практикума по изучению СЗИ от НСД Dallas Lock
Тема 3. Разработка диспетчера доступа для типовой информационной системы
Тема 4. Анализ эффективности использования физических средств защиты
Тема 5. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в изображении
Тема 6. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в аудиофайлах
Тема 7. Разработка подсистемы разграничения доступа СУБД предприятия
Тема 8. Разработка подсистемы защиты сайта от SQL-инъекции
Тема 9. Разработка системы аутентификации для информационной системы типового предприятия
Тема 10. Безопасность обработки данных облачными сервисами
Тема 11. Обеспечение безопасности и администрирование операционной системы специального назначения Astra Linux Special Edition
Тема 12. Организация масштабируемой сети ViPNet
Тема 13. Разработка системы обнаружения объектов с использованием биометрии

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ, ЗАЧЕТУ

Вопросы к экзамену

1. Назначение и функции защищенных сетевых приложений
2. Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI
3. Программный интерфейс OpenSSL
4. Характеристика программно-аппаратных средств обеспечения безопасности в вычислительных сетях
5. Основные средства защиты локальных сетей при подключении к Интернет
6. Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности
7. Классификация МЭ.
8. Основные требования к МЭ.
9. Основные возможности и схемы развертывания МЭ
10. Достоинства и недостатки МЭ.
11. Построение правил фильтрации
12. Методы сетевой трансляции адресов (NAT).
13. Шлюзы уровня приложений
14. Реализация сетевой политики безопасности с использованием МЭ.
15. Основные методы обхода межсетевых экранов
16. Проблемы защиты серверов и рабочих станций
17. Системы обнаружения вторжений (СОВ)
18. Средства и методы предотвращения и обнаружения вторжений

19. Назначение и возможности средств обнаружения вторжений на хосты
20. Протоколы и сетевые службы
21. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности
22. Классификация СОВ
23. Выявление атак на основе сигнатур атак и выявления аномалий
24. Аудит прикладных служб
25. Средства обнаружения уязвимостей сетевых служб
26. Средства обнаружения уязвимостей сетевых служб
27. Системы виртуальных ловушек (Honey Pot и Padded Cell)

Вопросы к зачету

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.

6. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI

7.

8. Основные механизмы реализации атак в сетях TCP/IP

9. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP

10.

11. Методы сканирования портов

12. Методы обнаружения пакетных сниферов

13. Методы обхода МЭ

14. Методы обхода МЭ

15. Имперсонация вслепую

16.

17. Десинхронизация TCP-соединений

18. Атаки, направленные на сетевую инфраструктуру

19. Защита от атак, направленных на сетевую инфраструктуру

20. Примеры сетевых атак в сетях TCP/IP

21. Принуждение к ускоренной передаче

22. Атаки, направленные на отказ в обслуживании

23. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации

24. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации

25. Основные технические меры защиты от сетевых атак

26. Основные криптографические методы защиты информации в вычислительных сетях

27. Протоколы аутентификации на прикладном уровне

28. Протокол Kerberos

29. Протокол Kerberos

30. Протокол SSL/TLS

31. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI

32. Назначение, основные возможности, принципы функционирования и варианты реализации VPN

33. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN

34. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах

35. Протокол управления ключами ISAKMP/Oakley

36. Использование протокола L2TP для организации виртуальных частных сетей

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Типовые угрозы сетевой безопасности			
Тема 1.1. Сетевые атаки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 1.2. Механизмы реализации атак в сетях TCP/IP	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 1.3. Методы перехвата сетевых соединений в сетях TCP/IP	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 1.4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Раздел 2. Криптографические методы защиты информации в компьютерных сетях			
Тема 2.1. Криптографические протоколы обеспечения безопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 2.2. Защита виртуальных частных сетей (VPN)	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 2.3. Разработка защищенных сетевых приложений	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях			
Тема 3.1. Средства защиты локальных сетей при подключении к Интернет	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 3.2. Защита серверов и рабочих станций	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	24	Вопросы к экзамену

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Запечников С.В. Основы построения виртуальных частных сетей : учебное пособие / С.В. Запечников, Н.Г. Милославская, А.И. Толстой ; Запечников С.В.; Милославская Н.Г.; Толстой А.И. - Москва : Горячая линия - Телеком, 2011. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991202152.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0215-2. / .— ISBN 0_242559

2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов ; Душкин А.В.; Барсуков О.М.; Кравцов Е.В.; Славнов К.В. - Москва : Горячая линия - Телеком, 2016. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204705.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0470-5. / .— ISBN 0_250838

дополнительная

1. Бирюков А.А. Информационная безопасность: защита и нападение : монография / А.А. Бирюков ; Бирюков А.А. - Москва : ДМК-пресс, 2017. - 434 с. - URL: https://www.studentlibrary.ru/book/ISBN9785970604359.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-97060-435-9. / .— ISBN 0_253659

2. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; В. Г. Спицын. - Томск : Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. - 148 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Весь срок охраны авторского права. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/13936.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-4332-0020-3. / .— ISBN 0_121542

3. Криптография и безопасность цифровых систем : учебное пособие / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев [и др.] ; В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко; под редакцией А. И. Астайкин. - Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2011. - 411 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Весь срок охраны авторского права. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/60851.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-9515-0166-0. / .— ISBN 0_136164

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Безопасность вычислительных сетей» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. М. Иванцов ; УлГУ, ФМИиАТ. - 2021. - 14 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10729. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_261315.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Альт рабочая станция
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и

практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

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	Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО