УТВЕРЖДЕНО

решением Учёного совета факультета математики, информационных и авиационных технологий

от «21» мая 2024 г., протокол № 5/24

Председатель _____/ М.А. Волков

«21» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Технология программной защиты в интернете**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра телекоммуникационных технологий и сетей
Курс	4 - очная форма обучения; 4 - заочная форма обучения

Направление (специальность): 09.03.02 Информационные системы и технологии
Направленность (профиль/специализация): Разработка информационных систем
Форма обучения: очная, заочная
Дата введения в учебный процесс УлГУ: 01.09.2024 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
Липатова Светлана Валерьевна	Кафедра телекоммуникационных технологий и сетей	Доцент,Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

изучение теоретических основ программной защиты в интернет

Задачи освоения дисциплины:

Знать:

-место и роль информационной безопасности в системе национальной безопасности РФ, общие характеристики процессов сбора, передачи, обработки, накопления и хранения информации; основные принципы передачи и обработки информации в инфокоммуникационных системах; основы защиты информации и сведений, составляющих государственную тайну; методы защиты информации;

-принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

-операционные системы ПЭВМ, системы управления базами данных, принципы построения информационных систем, структуру систем документационного обеспечения, перечень и характеристики угроз информационным ресурсам;

-эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы, сигналы электросвязи, принципы построения систем и средств связи, методы анализа электрических цепей, базовые принципы контроля, диагностики, технического обслуживания и ремонта средств связи;

-принципы организации и проектирования сложных информационных систем в соответствии с требованиями по защите информации, основы технико-экономического обоснования проектов;

-современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач;

-перечень, назначение, принципы работы инструментальных средств и систем программирования;

-типовые задачи обеспечения информационной безопасности;

Уметь:

-применять достижения информатики и вычислительной техники, перерабатывать большие объёмы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

-организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровняразвития технологий защиты информации;

-анализировать и оценивать угрозы информационной безопасности объекта;

-устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации, осуществлять контроль технического состояния, диагностику неисправностей и ремонт базовых стандартных блоков средств и систем связи;

-проектировать средства и сети связи с учётом требований по защите информации на базе серийно выпускаемых узлов и блоков, а также синтезировать нестандартные решения и проекты невысокой сложности; проводить технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности;

-составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

-выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;

-разрабатывать алгоритмы решения типовых задач;

Владеть:

-- навыками переработки больших объёмов информации, целенаправленного поиска информации в различных источниках по профилю деятельности, в том числе в глобальных компьютерных системах, анализа инфокоммуникационных сетей и систем, их информационной безопасности и разработки мероприятий по её обеспечению;

-- навыками выполнения комплекса мер по информационной безопасности, управления процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

-- методами и средствами выявления угроз безопасности автоматизированным системам;

-- профессиональной терминологией, навыками чтения электронных схем, безопасного использования технических средств в профессиональной деятельности, базовыми практическими навыками тестирования, поиска неисправностей, технического обслуживания и ремонта средств и систем связи, в том числе сетевого оборудования;

-методами анализа и формализации информационных процессов объекта и связей между ними, базовыми навыками проектирования средств и сетей связи; использования стандартных и разработки нестандартных программных средств автоматизации проектирования; технико-экономического анализа и обоснования проектов;

-навыками работы с программным обеспечением, использования программ;

-методами расчёта и инструментального контроля показателей технической защиты информации;

-- навыками и методиками разработки алгоритмов для решения задач информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Технология программной защиты в интернете» относится к числу дисциплин блока Б1.В.1.ДВ.12, предназначенного для студентов, обучающихся по направлению: 09.03.02 Информационные системы и технологии.

В процессе изучения дисциплины формируются компетенции: ПК-9, ПК-11, ПК-13.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Операционные системы, Преддипломная практика, Надежность информационных систем, Научно-исследовательская работа, Выполнение и защита выпускной квалификационной работы.

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**
ПК-9 Способен поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества	**знать**: место и роль информационной безопасности в системе национальной безопасности РФ, общие характеристики процессов сбора, передачи, обработки, накопления и хранения информации; основные принципы передачи и обработки информации в инфокоммуникационных системах; основы защиты информации и сведений, составляющих государственную тайну; методы защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации **уметь**: применять достижения информатики и вычислительной техники, перерабатывать большие объёмы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах; организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
	владеть: - навыками переработки больших объёмов информации, целенаправленного поиска информации в различных источниках по профилю деятельности, в том числе в глобальных компьютерных системах, анализа инфокоммуникационных сетей и систем, их информационной безопасности и разработки мероприятий по её обеспечению; - навыками выполнения комплекса мер по информационной безопасности, управления процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации
ПК-13 Способен проводить расчет экономической эффективности информационных систем и технологий	**знать**: принципы организации и проектирования сложных информационных систем в соответствии с требованиями по защите информации, основы технико-экономического обоснования проектов; современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач **уметь**: проектировать средства и сети связи с учётом требований по защите информации на базе серийно выпускаемых узлов и блоков, а также синтезировать нестандартные решения и проекты невысокой сложности; проводить технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; **владеть**: методами анализа и формализации информационных процессов объекта и связей между ними, базовыми навыками проектирования средств и сетей связи; использования стандартных и разработки нестандартных программных средств автоматизации проектирования; технико- экономического анализа и обоснования проектов; навыками работы с программным обеспечением, использования программ;
ПК-11 Способен оценивать надежность и качество функционирования информационных систем и технологий	**знать**: операционные системы ПЭВМ, системы управления базами данных, принципы построения информационных систем, структуру систем документационного обеспечения, перечень и характеристики угроз информационным ресурсам; эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы, сигналы электросвязи, принципы построения систем и средств связи, методы анализа электрических цепей, базовые принципы контроля, диагностики, технического обслуживания и ремонта средств связи

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	уметь: анализировать и оценивать угрозы информационной безопасности объекта; устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации, осуществлять контроль технического состояния, диагностику неисправностей и ремонт базовых стандартных блоков средств и систем связи **владеть**: - методами и средствами выявления угроз безопасности автоматизированным системам; - профессиональной терминологией, навыками чтения электронных схем, безопасного использования технических средств в профессиональной деятельности, базовыми практическими навыками тестирования, поиска неисправностей, технического обслуживания и ремонта средств и систем связи, в том числе сетевого оборудования

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 5 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 180 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		7
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	72	72
Аудиторные занятия:	72	72
Лекции	18	18
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	36	36
Самостоятельная работа	72	72
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)	Экзамен (36)	Экзамен

Вид учебной работы	**Количество часов (форма обучения очная)**	
	Всего по плану	**В т.ч. по семестрам**
		7
1	**2**	**3**
Всего часов по дисциплине	180	180

Форма обучения: заочная

Вид учебной работы	**Количество часов (форма обучения заочная)**	
	Всего по плану	**В т.ч. по семестрам**
		9
1	**2**	**3**
Контактная работа обучающихся с преподавателем в соответствии с УП	40	40
Аудиторные занятия:	40	40
Лекции	12	12
Семинары и практические занятия	14	14
Лабораторные работы, практикумы	14	14
Самостоятельная работа	131	131
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)	Экзамен (9)	Экзамен
Всего часов по дисциплине	180	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. Технологии защиты							
Тема 1.1. Теоретические основы технологий программной защиты в интернете	17	2	2	4	0	9	Тестирование
Тема 1.2. Классификация атак по уровням	19	2	4	4	0	9	Тестирование
Тема 1.3. Атаки на беспроводные устройства	19	2	4	4	0	9	Тестирование
Тема 1.4. Уязвимости	19	2	4	4	0	9	Тестирование
Тема 1.5. Атаки в виртуальной среде	15	2	0	4	0	9	Тестирование
Тема 1.6. Облачные технологии	19	2	4	4	0	9	Тестирование
Тема 1.7. Средства защиты	18	3	0	6	0	9	Тестирование
Тема 1.8. Нормативная документация	18	3	0	6	0	9	Тестирование
Итого подлежит изучению	144	18	18	36	0	72	

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

Форма обучения: заочная

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. Технологии защиты							
Тема 1.1. Теоретические основы технологий программной защиты в интернете	22	2	2	2	0	16	Тестирование
Тема 1.2. Классификация атак по уровням	22	2	2	2	0	16	Тестирование
Тема 1.3. Атаки на беспроводные устройства	22	2	2	2	0	16	Тестирование
Тема 1.4. Уязвимости	22	2	2	2	0	16	Тестирование
Тема 1.5. Атаки в виртуальной среде	22	2	2	2	0	16	Тестирование
Тема 1.6. Облачные технологии	22	2	2	2	0	16	Тестирование
Тема 1.7. Средства защиты	20	0	2	2	0	16	Тестирование
Тема 1.8. Нормативная документация	19	0	0	0	0	19	Тестирование
Итого подлежит изучению	171	12	14	14	0	131	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Технологии защиты

Тема 1.1. Теоретические основы технологий программной защиты в интернете

Модель OSI, Прикладной (7) уровень (Application Layer), Представительский (6) уровень (Presentation Layer), Сеансовый (5) уровень (Session Layer), Транспорт-ный (4) уровень (Transport Layer)

Тема 1.2. Классификация атак по уровням

Иерархические модели OSI, Атаки на физическом уровне (Концентраторы), Атаки на канальном уровне (Атаки на коммутаторы,Переполнение CAM-таблицы,VLAN Hoping), Атаки на сетевом уровне (Атаки на маршрутизаторы, Среды со статической маршрутизацией, Безопасность статической маршрутизации, Среды с динамической маршрутизацией, Среды с протоколом RIP, Безопасность протокола RIP, Ложные маршруты RIP, Понижение версии протокола RIP, Взлом хеша MD5, Обеспечение безопасности протокола RIP, Среды с протоколом OSPF, Безопасность протокола OSPF, Среды с протоколом BGP, Атака BGP Router Masquerading, Атаки на MD5 для BGP) Атаки на транспортном уровне (Транспортный протокол TCP, Известные проблемы, Атаки на TCP, IP-spoofing, TCP hijacking, Десинхронизация нулевыми данными, Сканирование сети, SYN-флуд, Атака Teardrop, Безопасность TCP (Атаки на UDP, UDP Storm), Безопасность UDP (Протокол ICMP, Методология атак на ICMP, Обработка сообщений ICMP, Сброс соединений (reset), Снижение скорости, Без-опасность ICMP Атаки на уровне приложений.(Угрозы IP-телефонии Возможные угрозы voip, Поиск устройств voip, Перехват данных, Отказ в обслуживании, Подмена номера) Атаки на диспетчеров (Хищение сервисов и телефонный спам, Анализ удаленных сетевых служб, ICMP как инструмент исследования сети, Утилита fping, Утилита Nmap, Использование «Broadcast ICMP», ICMP-пакеты, сообщающие об ошибках

Тема 1.3. Атаки на беспроводные устройства

Атаки на Wi-Fi, Протоколы защиты, Протокол WEP, Протокол WPA, Физическая защита, Сокрытие ESSID, Возможные угрозы, Отказ в обслуживании, Поддельные сети, Ошибки при настройке, Взлом ключей шифрования.

Тема 1.4. Уязвимости

Основные типы уязвимостей (Уязвимости проектирования, реализации и эксплу-атации), Примеры уязвимостей, Права доступа к файлам, Оперативная память, Объявление памяти, Завершение нулевым байтом, Сегментация памяти про-граммы, Переполнение буфера, Переполнения в стеке.

Тема 1.5. Атаки в виртуальной среде

Технологии виртуализации, Сетевые угрозы в виртуальной среде, Защита виртуальной среды, Trend Micro Deep Security, Схема защиты Deep Security, Защита веб-приложений

Тема 1.6. Облачные технологии

Принцип облака, Структура ЦОД, Виды ЦОД, Требования к надежности, Безопасность облачных систем

Тема 1.7. Средства защиты

Организация защиты от вирусов, Способы обнаружения вирусов, Проблемы антивиру-сов, Архитектура антивирусной защиты, Борьба с нежелательной почтой, Межсетевые экраны (Принципы работы межсетевых экранов, Аппаратные и программные МЭ, Спе-циальные МЭ, Средства обнаружения и предотвращения вторжений, Системы IDS/IPS), Мониторинг событий ИБ в Windows 2008 (Промышленные решения мониторинга событий, Средства предотвращения утечек), Каналы утечек, Принципы работы DLP, Сравнение систем DLP, Средства шифрования (Симметричное шифрование, Инфраструктура открытого ключа). Системы двухфакторной аутентификации (Принципы работы двухфакторной аутентификации, сравнение систем).

Тема 1.8. Нормативная документация

Политики ИБ, Политики безопасности, Регламент управления инцидентами, Ин-струментарий Backtrack

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Тема 1.1. Теоретические основы технологий программной защиты в интернете

Вопросы к теме:

Очная форма

Стек протоколов TCP/UDP/IP. (форма проведения – семинар). Коммутация пакетов. Модель OSI. Протокол TCP.

Тема 2.2. Классификация атак по уровням

Вопросы к теме:

Очная форма

Политика IT-безопасности. (форма проведения – практическое). Коммутация пакетов. Модель OSI. Протокол TCP. Протокол IP.

Канальный уровень Ethernet. Адресация на канальном уровне MAC-адрес.

Пакет ARP. Формат кадра Ethernet. Определение MAC-адреса.

Тема 3.3. Атаки на беспроводные устройства

Вопросы к теме:

Очная форма

Процесс передачи речи по IP сети. (форма проведения – семинар).

Шлюзы (Gateway, Медиа). Качественные характеристики речи пи передаче по IP. Характеристики кодеков IP телефонии. Протокол RTP (уровни, пакет, заголовок). Протокол SIP. (форма проведения – семинар). Протокол SIP в стеке протоколов сети IP. Сообщения протокола SIP. Агент пользователя. Адресация в сети SIP. Основные элементы сети SIP. Сообщения протокола SIP.

Тема 4.4. Уязвимости

Вопросы к теме:

Очная форма

Архитектура сетей поколения Softswitch. (форма проведения – семинар).

Декомпозиция шлюза. Взаимодействие сети ОКС №7 с сетью VoIP. Сценарии установления соединений.

Тема 5.5. Атаки в виртуальной среде

Тема 6.6. Облачные технологии

Вопросы к теме:

Очная форма

Структура сети IMS. (форма проведения – семинар). Архитектура IMS.

Сеть абонентского доступа. Функциональные элементы IMS. Сценарий регистрации пользователя в IMS.

Тема 7.7. Средства защиты

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цели: изучить международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Содержание: Задание 1 Открыть программный модуль «Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №1». Пройти тестирование по материалу изученной темы в разделе «Тест». Задание 2 Пользуясь инструкцией к выполнению задания в разделе «Практика»

программного модуля, выполнить задание.
Результаты: Код, отчет
Ссылка: https://libeldoc.bsuir.by/bitstream/123456789/9847/2/Pulko_uch.pdf
Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя
Цели: изучить законы Республики Беларусь по определению правовых и организационных основ отнесения сведений к государственным секретам и их защите, государственное регулирование и управление в области информации, информатизации и защиты информации
Содержание: 1. В списке оборудования компьютера убедиться в отсутствии устройств компании Aladdin (eToken, HASP). Если эти устройства присутствуют в списке оборудования – удалить их. 2. Удалить, если присутствует, программное обеспечение eToken и HASP. 3. Подключиться к компьютеру Centurion, открыть ресурс Q и войти в каталог setup. 4. Запустить программу setup.exe. 5. Следуя указаниям программы установки установить на компьютере программное обеспечение системы HASP. Установить компоненты помеченные ниже. 6. Подключить HASP к разъему USB компьютера. a) В случае правильной установки в электронном ключе HASP должен загореться световой индикатор. b) Если индикатор не загорается, обновить драйвер устройства вручную. 7. В списке оборудования компьютера найти подключенное устройство
Результаты: Код, отчет
Ссылка: https://www.dgunh.ru/content/files/15doc/lp-pi-pive-8.pdf
Защита папок и файлов
Цели: освоение навыков скрытия папок
Содержание: 1. Запустите программу. 2. Защитите программу паролем. 3. Настройте программу на сворачивание в трей при закрытии окна. 4. Настройте горячие клавиши для следующих операций: • Открытие программы. 28 • Включение защиты. • Выключение защиты. • Видимость трей-иконки. 5. Скройте папку Директория на диске D:\ . 6. Запустите Мой компьютер и убедитесь в том, что папка не видна. 7. Заблокируйте папку Директория на диске D:\ . 8. Запустите Мой компьютер и убедитесь в том, что папка видна, но не открывается.
Результаты: Код, отчет
Ссылка: https://www.dgunh.ru/content/files/15doc/lp-pi-pive-8.pdf
Шифрование данных
Цели: Получение теоретических и практических навыков работы с программными средствами шифрования данных
Содержание: Установить PGP, GPG <sudo apt-get install pgpgpg> Произвести операции шифрования и дешифрования над произвольными файлами. Для шифрования используйте команду <gpg -c>. Для дешифрования <gpg –decrypt-file> (В этом случае в директории зашифрованного файла будет создан расшифрованный. Если нужно лишь вывести на экран расшифрованное содержимое используйте <gpg –decrypt>) Установить TrueCrypt. Нам потребуется версия 7.1a. Скачать её можно здесь или здесь. Создать криптоконтейнер, примонтировать его как виртуальный диск. Поместить в криптоконтейнер какую-то информацию. Отмонтировать диск и переместить криптоконтейнер. Повторно примонтировать криптоконтейнер как виртуальный диск. Убедиться, что криптоконтейнер может передаваться и использоваться независимо. Установить LUKS/dm-crypt <sudo apt-get update>, <sudo apt-get install cryptsetup>. Создаем файл, где будем хранить зашифрованные данные. Самый простой способ <fallocate -l 512M /root/test1>, где /root - директория хранения файла, test1 - имя файла. Так же для создания этого файла можно использовать команду dd. <dd if=/dev/zero of=/root/test2 bs=1M count=512>. Третий способ - использовать команду dd и заполнить файл случайными данными. <dd if=/dev/urandom of=/root/test3 bs=1M count=512>.

Создать криптоконтейнер. <cryptsetup -y luksFormat /root/test1> (нужно будет согласиться переписать данные и задать пароль). Открыть контейнер. <cryptsetup luksOpen /root/test1 volume1>. (volume1 - имя контейнера, его мы задаем этой командой). При этом будет создан файл /dev/mapper/volume1. Создать в нем файловую систему <mkfs.ext4 -j /dev/mapper/volume1>. Создать папку для монтирования <mkdir /mnt/files>. Монтировать <mount /dev/mapper/volume1 /mnt/files> Теперь перенесем какие_ниибудь файлы в криптоконтейнер. Например, скопируем папку /etc <cp -r /etc/* /mnt/files>. Размонтировать <umount /mnt/files>. Теперь закрываем volume1. <cryptsetup luksClose volume1>. После этого наши данные зашифрованы. Чтобы открыть их выполним <cryptsetup luksOpen /root/test1 volume1> и <mount /dev/mapper/volume1 /mnt/files>
Результаты: Код, отчет
Ссылка: https://www.dgunh.ru/content/files/15doc/lp-pi-pive-8.pdf
Honeypot, Nmap
Цели: Получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети.
Содержание: Настройте сеть, состоящую из двух компьютеров. На одну из виртуальных машин устаните web-сервер <sudo apt-get install apache2>. На другую установите – Nmap <sudo apt-get install nmap>. Определите IP адрес виртуальной машины где установлен web-сервер apache. Произведите сканирование web-сервера всеми описанными методами (Изучение средств сканирования Nmap). Установите Honeyd. Ознакомьтесь с информацией по настройке Honeyd и стандартным содержимым файла /etc/honeypot/honeyd.conf. Настройте Honeypot изменив содержание файла /etc/honeypot/honeyd.conf . Запустите <farpd -d> . Запустите honeyd. <honeyd -d -f /etc/honeypot/honeyd.conf> Произведите сканирование сети с honeypot. Измените настройки Honeypot. Усложните конфигурационный файл. Добавьте несколько ловушек, измените информацию об ОС, информацию о роутере, об открытых портах и.т.д.. Запустите honeyd. <honeyd -d -f /etc/honeypot/honeyd.conf> Произведите сканирование.
Результаты: Код, отчет
Ссылка: https://www.dgunh.ru/content/files/15doc/lp-pi-pive-8.pdf
ЛВС, web-сервер с CMS.
Цели: Получить теоритических и практических навыков построения ЛВС и web-сервера на примере установки CMS.
Содержание: Установите на 4 виртуальные машины операционную систему Ubuntu Server. Условно назовем эти машины: Hacker, Server, WWW, DataBase. Настроите сеть. В настройках сети (По умолчанию Файл-> настройки-> сеть, на вкладке Виртуальные сети хоста) создаем 2 адаптера (По умолчанию 1 уже создан). Для каждого из них прописать разные IP-адреса 192.168.*.*, где * - любое число от 0 до 255 (Если хотите сделать все как на схеме, на первом оставьте значения по умолчанию - 192.168.56.1, а на втором 192.168.57.1). На уже имеющимся адаптере можете посмотреть настройки DHCP и, по аналогии, настроить DHCP для второго адаптера. DHCP-сервер будет выдавать всем подключенным в сеть машинам IP-адреса автоматически через определенные промежутки времени. В данной лабораторной работе настройка DHCP в VirtualBox никак не отразиться на ее выполнении, а наоборот, только упростит построение сети между виртуальными машинами. Теперь в настройках каждой из виртуальных машин выберите вкладку сеть. В машине Hacker создайте 2 адаптера. В первом, чтобы вы могли использовать интернет, выберите тип подключения NAT. Во втором - виртуальный адаптер хоста (если Вы делаете все по схеме выберите тот, где ip-адрес 192.168.56.*). На машине Server создайте 3 адаптера. Первый - чтобы использовать интернет. Второй - тот же виртуальный адаптер хоста, что и в машине Hacker. Третий - виртуальный адаптер хоста, но выбираете уже второй (если вы делаете все по схеме выбираете тот, где ip-адрес

192.168.57.*). На машинах WWW и DataBase создайте 2 адаптера. Первый - выход в интернет. Второй - виртуальный адаптер хоста (второй, тот где 196.168.57.*). Особенностью подключения типа виртуальный адаптер хоста, является то, что компьютер, на котором запущен VirtualBox так же доступен, что может помочь во второй части лабораторной работы. Настройка статического IP-адреса (если используется на DHCP). Настройка сети осуществляется с помощью создания виртуального адаптера хоста. При первичном запуске всех виртуальных машин необходимо внести изменения в файл /etc/network/interfaces.
Результаты: Код, отчет
Ссылка: https://www.dgunh.ru/content/files/15doc/lp-pi-pive-8.pdf
Нагрузочное тестирование web-сервера.
Цели: С помощью систем нагрузочного тестирования определить производительность web-серверов Apache и Nginx, добиться отказа в обслуживании.
Содержание: Тестирование на PHP-запросы: Определить максимальное число параллельных запросов, при котором сервер нас не будет блокировать. Провести тест при использовании максимального числа запросов. Тестирование на HTML-запросы: Определить максимальное число параллельных запросов Провести тест при использовании максимального числа запросов. Провести сравнение результатов и сформировать выводы.
Результаты: Код, отчет
Ссылка: https://www.dgunh.ru/content/files/15doc/lp-pi-pive-8.pdf

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы курсовой работы

Тема 1. Методы и средства шифрования данных при передаче через интернет.
Тема 2. Анализ современных технологий аутентификации пользователей в веб-приложениях.
Тема 3. Защита персональных данных в облачных сервисах: методы и подходы.
Тема 4. Сравнительный анализ систем предотвращения вторжений в корпоративных сетях.
Тема 5. Разработка и внедрение системы защиты от DDoS-атак на уровне приложений.
Тема 6. Современные технологии защиты от фишинга и спуфинг-атак в Интернете.
Тема 7. Безопасность беспроводных сетей Wi-Fi: угрозы и меры защиты.
Тема 8. Применение блокчейн-технологий для повышения безопасности транзакций в Интернете.
Тема 9. Инструменты и методы анализа защищенности веб-приложений.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Модель OSI, Прикладной (7) уровень (Application Layer).
2. Представительский (6) уровень (Presentation Layer).
3. Сеансовый (5) уровень (Session Layer).
4. Транспортный (4) уровень (Transport Layer).
5. Иерархические модели OSI
6. Атаки на физическом уровне (Концентраторы)
7. Атаки на канальном уровне (Атаки на коммутаторы,Переполнение CAM-таблицы,VLAN Hoping)
8. Атаки на сетевом уровне Атаки на маршрутизаторы
9. Среды со статической маршрутизацией, Безопасность статической маршрутизации

10. Среды с динамической маршрутизацией
11. Среды с протоколом RIP, Безопасность протокола RIP
12. Ложные маршруты RIP, Понижение версии протокола RIP, Взлом хеша MD5, Обеспечение безопасности протокола RIP
13. Среды с протоколом OSPF, Безопасность протокола OSPF
14. Среды с протоколом BGP, Атака BGP Router Masquerading, Атаки на MD5 для BGP
15. Анализ удаленных сетевых служб, ICMP как инструмент исследования сети, Утилита fping, Утилита Nmap, Использование «Broadcast ICMP», ICMP-пакеты, сообщающие об ошибках
16. Атаки на диспетчеров (Хищение сервисов и телефонный спам)
17. Атаки на уровне приложений.(Угрозы IP-телефонии Возможные угрозы VoIP, Поиск устройств VoIP, Перехват данных, Отказ в обслуживании, Подмена номера)
18. Безопасность UDP Протокол ICMP, Методология атак на ICMP, Обработка сообщений ICMP, Сброс соединений (reset), Снижение скорости, Безопасность ICMP
19. Безопасность TCP (Атаки на UDP, UDP Storm)
20. Десинхронизация нулевыми данными, Сканирование сети, SYN-флуд, Атака Teardrop
21. Атаки на транспортном уровне Транспортный протокол TCP, Известные проблемы, Атаки на TCP, IP-spoofing, TCP hijacking
22. Атаки на Wi-Fi
23. Протоколы защиты: Протокол WEP, Протокол WPA
24. Физическая защита, Сокрытие ESSID, Возможные угрозы, Отказ в обслуживании
25. Поддельные сети, Ошибки при настройке, Взлом ключей шифрования.
26. Основные типы уязвимостей (Уязвимости проектирования, реализации и эксплуатации), Примеры уязвимостей
27. Права доступа к файлам, Оперативная память, Объявление памяти, Завершение нулевым байтом, Сегментация памяти программы, Переполнение буфера, Переполнения в стеке.
28. Технологии виртуализации, Сетевые угрозы в виртуальной среде, Защита виртуальной среды, Trend Micro Deep Security, Схема защиты Deep Security, Защита веб-приложений
29. Принцип облака, Структура ЦОД, Виды ЦОД, Требования к надежности, Безопасность облачных систем
30. Мониторинг событий ИБ в Windows 2008 (Промышленные решения мониторинга событий, Средства предотвращения утечек)
31. Каналы утечек, Принципы работы DLP, Сравнение систем DLP
32. Средства шифрования (Симметричное шифрование, Инфраструктура открытого ключа)
33. Системы двухфакторной аутентификации(Принципы работы двухфакторной аутентификации, Сравнение систем)
34. Политика ИБ, Политики безопасности
35. Регламент управления инцидентами
36. Инструментарий Backtrack

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. Технологии защиты			
Тема 1.1. Теоретические основы технологий программной защиты в интернете	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.2. Классификация атак по уровням	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.3. Атаки на беспроводные устройства	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.4. Уязвимости	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.5. Атаки в виртуальной среде	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.6. Облачные технологии	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.7. Средства защиты	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	9	Вопросы к экзамену, Тестирование
Тема 1.8. Нормативная документация	Проработка учебного материала с использованием ресурсов учебно-	9	Вопросы к экзамену, 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.)***
	методического и информационного обеспечения дисциплины.		

Форма обучения: заочная

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. Технологии защиты			
Тема 1.1. Теоретические основы технологий программной защиты в интернете	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 1.2. Классификация атак по уровням	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 1.3. Атаки на беспроводные устройства	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 1.4. Уязвимости	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 1.5. Атаки в виртуальной среде	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 1.6. Облачные технологии	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Вопросы к экзамену, Тестирование
Тема 1.7. Средства защиты	Проработка учебного материала с	16	Вопросы к экзамену,

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.)***
	использованием ресурсов учебно-методического и информационного обеспечения дисциплины.		Тестирование
Тема 1.8. Нормативная документация	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	19	Вопросы к экзамену, Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Богатырев Владимир Анатольевич. Информационные системы и технологии. Теория надежности : Учебное пособие для вузов / В.А. Богатырев. - Москва : Юрайт, 2021. - 318 с. - (Высшее образование). - https://urait.ru/bcode/469873. - https://urait.ru/book/cover/35AC05A7-6617-420A-B612-92D913F069DF. - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-00475-5 : 929.00. / .— ISBN 0_277594

2. Казарин Олег Викторович. Надежность и безопасность программного обеспечения : Учебное пособие Для бакалавриата и магистратуры / О.В. Казарин, И.Б. Шубинский ; Казарин О. В., Шубинский И. Б. - Москва : Юрайт, 2019. - 342 с. - (Высшее образование). - URL: https://urait.ru/bcode/441287 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-05142-1 : 819.00. / .— ISBN 0_274007

дополнительная

1. Жарков А. В. Криптографические протоколы : учеб.-метод. рекомендации по выполнению лаб. работ / А. В. Жарков ; УлГУ, ФМиИТ, Каф. прикл. математики. - Ульяновск : УлГУ, 2011. - ил. - Загл. с экрана. - Имеется печ. аналог. - Электрон. текстовые дан. (1 файл : 1,99 Мб). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_1388

2. Суворова Галина Михайловна. Информационная безопасность : Учебное пособие для вузов / Г.М. Суворова ; Суворова Г. М. - Москва : Юрайт, 2022. - 253 с. - (Высшее образование). - URL: https://urait.ru/bcode/496741 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-13960-0 : 819.00. / .— ISBN 0_317760

3. Кравченко, Ю. А. Информационные и программные технологии. Ч.1. Информационные

технологии : учебное пособие / Ю. А. Кравченко, Э. В. Кулиев, В. В. Марков ; Ю. А. Кравченко, Э. В. Кулиев, В. В. Марков. - Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2017. - 112 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/87417.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-9275-2495-2 (ч.1), 978-5-9275-2494-5. / .— ISBN 0_149575

учебно-методическая

1. Курилова О. Л. Методические рекомендации для семинарских (практических) занятий и самостоятельной работы по дисциплине «Технология программной защиты в интернете» для студентов направлений 09.03.02 «Информационные системы и технологии» / О. Л. Курилова, В. Г. Козловский, В. П. Смолеха ; УлГУ, ФМИиАТ. - 2022. - 121 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/14545. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_503961.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Alt Linux
- LibreOffice
- Oracle VM VirtualBox

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	Доцент Кандидат технических наук, Доцент	Липатова Светлана Валерьевна
	Должность, ученая степень, звание	ФИО