УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «__16__» ___мая___ 2023 __ г., протокол №__4/23_
Председатель _____/М.А.Волков
(подпись, расшифровка подписи)
«__16__» _____мая____ 20__23_г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Технология программной защиты в интернете
Факультет	Математики, информационных и авиационных технологий
Кафедра	Кафедра телекоммуникационных технологий и сетей
Курс	4

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: 1 сентября 2023 г.

Программа актуализирована на заседании кафедры: протокол №_1____ от _09__ 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
Смагин Алексей Аркадьевич.	Телекоммуникационных технологий и сетей	Д.т.н., профессор

СОГЛАСОВАНО
Заведующий кафедрой телекоммуникационных технологий и сетей, реализующей дисциплину и выпускающей
_____/_Смагин А.А ____/ *Подпись* *ФИО* «16» мая 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Цели освоения дисциплины: изучение теоретических основ программной защиты в интернет

Задачи освоения дисциплины:

В результате изучения дисциплины студенты должны

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 уровня развития 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:

Данная дисциплина является по выбору Б1.В.ДВ учебного плана подготовки бакалавра по направлению 09.03.02 - "Информационные системы и технологии".

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Теория информации», «Теория систем и системный анализ», «Системы мобильной связи», «Технологии обработки информации», «Методы и средства проектирования информационных систем и технологий». Студенты должны уметь приобретать, обрабатывать и использовать новую информацию в своей предметной области; знать основы построения инфокоммуникационных сетей и систем ; иметь навыки самостоятельной работы на компьютере и в компьютерных сетях; быть способным к компьютерному моделированию устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ.

Данная дисциплина является предшествующей для дисциплин: «Корпоративные информационные системы», «Направляющие среды систем передачи информации».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИС-

ЦИПЛИНЕ (МОДУЛЮ), 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 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-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,

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

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	проектов; навыками работы с программным обеспечением, использования программ;

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) ___5ЗЕТ_____

4.2. Объем дисциплины по видам учебной работы

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\18*
Семинары и практические занятия	18	18\18*
Лабораторные работы, практикумы	36	36\36*
Самостоятельная работа	72	72
Форма текущего контроля знаний и контроля самостоятельной работы	тестирование, защита лабораторных работ	тестирование, защита лабораторных работ
Курсовая работа	курсовая	курсовая
Виды промежуточной аттестации (экзамен, зачет)	экзамен	экзамен (36)
Всего часов по дисциплине	180	180

Форма обучения ____заочная_____

Вид учебной работы	Количество часов (форма обучения заочная)	
	Всего по плану	В т.ч. по сессиям
		14
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	40	40

Аудиторные занятия:	40	40
Лекции	12	12\12*
Семинары и практические занятия	14	14\14*
Лабораторные работы, практикумы	14	14\14*
Самостоятельная работа	131	131
Форма текущего контроля знаний и контроля самостоятельной работы	тестирование, защита лабораторных работ	тестирование, защита лабораторных работ
Курсовая работа	курсовая	курсовая
Виды промежуточной аттестации (экзамен, зачет)	экзамен	экзамен (9)
Всего часов по дисциплине	180	180

*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения

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 ____очная_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятияв интерактивной форме	Самостоятельная7анна7бота	
		Лекции	Практические занятия, семинары	Лабораторные работы,практикумы			
1	2	3	4	5	6	7	
1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПРОГРАММНОЙ ЗАЩИТЫ В ИНТЕРНЕТЕ	13	2	2	-	-	9	Отчет практического занятия
2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ	25	4	4	8	8	9	Отчет практического и лабораторного занятия
3. АТАКИ НА БЕСПРОВОДНЫЕ УСТРОЙСТВА	21	2	2	8	8	9	Отчет практического и лабораторного занятия

4. УЯЗВИМОСТИ	17	2	2	4	4	9	Отчет практического и лабораторного занятия
5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ	17	2	2	4	4	9	Отчет практического и лабораторного занятия
6. ОБЛАЧНЫЕ ТЕХНОЛОГИИ	17	2	2	4	4	9	Отчет практического и лабораторного занятия
7. СРЕДСТВА ЗАЩИТЫ	21	2	2	8	8	9	отчет
8. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ	13	2	2	-	-	9	Отчет практического занятия
Итого	180	18	18	36	36	72	Экзамен 36

Форма обучения ____заочная_____

Название разделов и тем	**Всего**	**Виды учебных занятий**					**Форма текущего контроля знаний**
		Аудиторные занятия			**Занятияв интерактивной форме**	**Самостоятельная работа**	
		Лекции	**Практические занятия, семинары**	**Лабораторные работы,практикумы**			
1	**2**	**3**	**4**	**5**	**6**	**7**	
1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПРОГРАММНОЙ ЗАЩИТЫ В ИНТЕРНЕТЕ		1	1	-	-	16	Отчет практического занятия
2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ		1	1	2	2	16	Отчет практического и лабораторного занятия
3. АТАКИ НА БЕСПРОВОД-		1	2	2	2	16	Отчет практиче-

НЫЕ УСТРОЙ-СТВА							ского и лабора-торного занятия
4. УЯЗВИМО-СТИ		1	2	2	2	16	Отчет практиче-ского и лабора-торного занятия
5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ		2	2	2	2	16	Отчет практиче-ского и лабора-торного занятия
6. ОБЛАЧНЫЕ ТЕХНОЛОГИИ		2	2	3	3	17	Отчет практиче-ского и лабора-торного занятия
7. СРЕДСТВА ЗАЩИТЫ		2	2	3	3	17	отчет
8. НОРМАТИВ-НАЯ ДОКУМЕН-ТАЦИЯ		2	2	-	-	17	Отчет практиче-ского за-нятия
Итого	180	12	14	14	14	131	Экзамен

5. СОДЕРЖАНИЕ ДИСЦИЛИНЫ (МОДУЛЯ)

Тема 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 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, Безопасность 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 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 4.. УЯЗВИМОСТИ

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

Тема 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 6.ОБЛАЧНЫЕ ТЕХНОЛОГИИ

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

Тема 7. СРЕДСТВА ЗАЩИТЫ

Организация защиты от вирусов, Способы обнаружения вирусов, Проблемы антивирусов, Архитектура антивирусной защиты, Борьба с нежелательной почтой, Межсетевые экраны (Принципы работы межсетевых экранов, Аппаратные и программные МЭ, Специальные 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 8. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ

Политики ИБ, Политики безопасности, Регламент управления инцидентами, Инструментарий Backtrack

6. ТЕМЫ СЕМИНАРСКИХ ЗАНЯТИЙ

Тема 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПРОГРАММНОЙ ЗАЩИТЫ В ИНТЕРНЕТЕ

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

   Тема 2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ
2. Политика IT-безопасности. (форма проведения – практическое).
   2.1. Коммутация пакетов.
   2.2. Модель OSI.
   2.3. Протокол TCP.
   2.4. Протокол IP.
3. Канальный уровень Ethernet.
   3.1. Адресация на канальном уровне MAC-адрес.
   3.2. Пакет ARP.
   3.3. Формат кадра Ethernet.
   3.4. Определение MAC-адреса

   Тема 3. АТАКИ НА БЕСПРОВОДНЫЕ УСТРОЙСТВА
4. Процесс передачи речи по IP сети. (форма проведения – семинар).
   4.1. Шлюзы (Gateway, Медиа).
   4.2. Качественные характеристики речи пи передаче по IP.
   4.3. Характеристики кодеков IP телефонии.
   4.4. Протокол RTP (уровни, пакет, заголовок).
5. Протокол SIP. (форма проведения – семинар).
   5.1. Протокол SIP в стеке протоколов сети IP.
   5.2. Сообщения протокола SIP.
   5.3. Агент пользователя.
   5.4. Адресация в сети SIP.
   5.5. Основные элементы сети SIP.
   5.6. Сообщения протокола SIP.

   Тема 4. 4. УЯЗВИМОСТИ
6. Архитектура сетей поколения Softswitch. (форма проведения – семинар).
   6.1. Декомпозиция шлюза.
   6.2. Взаимодействие сети ОКС №7 с сетью VoIP.
   6.3. Сценарии установления соединений.

   Тема 5. 5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ
7. Структура сети IMS. (форма проведения – семинар).
   7.1. Архитектура IMS.
   7.2. Сеть абонентского доступа.
   7.3. Функциональные элементы IMS
   7.4. Сценарий регистрации пользователя в IMS

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

1. Лабораторная работа «Способы первичной защиты компьютера»
2. Лабораторная работа «Защита от WEB-euhjp»
3. Лабораторная работа «Защита от атак из интернгета»
4. Лабораторная работа «Настройка системы защиты WINDOWS/XP»

5. Лабораторная работа «Групповые политики»

Полное содержание работ представлено в Смолеха, В. П. Межсетевое взаимодействие систем и сетей NGN [Электронный ресурс] : лабораторный практикум / В. П. Смолеха, В. Г. Козловский, О. Л. Курилова ; под ред. А. А. Смагина. - Ульяновск : УлГУ, 2018. **URL:** http://lib.ulsu.ru/MegaPro/Download/MObject/1604/Smoleha2018.pdf

8. ТЕМАТИКА РЕФЕРАТОВ

«Данный вид работы не предусмотрен УП».

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. Атаки на транспортном уровне Транспортный протокол TCP, Известные проблемы, Атаки на TCP, IP-spoofing, TCP hijacking
16. Десинхронизация нулевыми данными, Сканирование сети, SYN-флуд, Атака Teardrop
17. Безопасность TCP (Атаки на UDP, UDP Storm)
18. Безопасность UDP Протокол ICMP, Методология атак на ICMP, Обработка сообщений ICMP, Сброс соединений (reset), Снижение скорости, Безопасность ICMP
19. Атаки на уровне приложений.(Угрозы IP-телефонии Возможные угрозы VoIP, Поиск устройств VoIP, Перехват данных, Отказ в обслуживании, Подмена номера)
20. Атаки на диспетчеров (Хищение сервисов и телефонный спам)

21. Анализ удаленных сетевых служб, ICMP как инструмент исследования сети, Утилита fping, Утилита Nmap, Использование «Broadcast ICMP», ICMP-пакеты, сообщающие об ошибках
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. Организация защиты от вирусов, Способы обнаружения вирусов, Проблемы антивирусов, Архитектура антивирусной защиты
31. Борьба с нежелательной почтой
32. Межсетевые экраны (Принципы работы межсетевых экранов, Аппаратные и программные МЭ, Специальные МЭ, Средства обнаружения и предотвращения вторжений, Системы IDS/IPS)
33. Мониторинг событий ИБ в Windows 2008 (Промышленные решения мониторинга событий, Средства предотвращения утечек)
34. Каналы утечек, Принципы работы DLP, Сравнение систем DLP
35. Средства шифрования (Симметричное шифрование, Инфраструктура открытого ключа)
36. Системы двухфакторной аутентификации(Принципы работы двухфакторной аутентификации, Сравнение систем)
37. Политика ИБ, Политики безопасности
38. Регламент управления инцидентами
39. Инструментарий Backtrack

1. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Форма обучения _____очная_____

Название разделов и тем	**Вид самостоятельной работы**	**Объем в часах**	**Форма контроля (*решения задач, реферата и др.)***
Тема 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПРОГРАММНОЙ	*Проработка учебного материала, подготовка отчета, подготовка к сдаче экзамена*	9	*Проверка отчета по практическойй работе*

ЗАЩИТЫ В ИНТЕРНЕТЕ			
Тема 2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	9	*Проверка отчета по лабораторной работе*
Тема 3. АТАКИ НА БЕСПРОВОДНЫЕ УСТРОЙСТВА	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	9	*Проверка отчета по лабораторной работе*
Тема 4. УЯЗВИМОСТИ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	9	*Проверка отчета по лабораторной работе*
Тема 5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	9	*Проверка отчета по лабораторной работе*
Тема 6. ОБЛАЧНЫЕ ТЕХНОЛОГИИ	*Проработка учебного материала, подготовка к сдаче экзамена.*	9	*Проверка отчета по практическойй работе*
Тема 7. СРЕДСТВА ЗАЩИТЫ	*Проработка учебного материала, подготовка к сдаче экзамена.*	9	*Проверка отчета по практическойй работе*
Тема 8. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ	*Проработка учебного материала, подготовка к сдаче экзамена.*	9	*Проверка отчета по практическойй работе*

Форма обучения _____заочная_____

Название разделов и тем	**Вид самостоятельной работы**	**Объем в часах**	**Форма контроля (*решения задач, реферата и др.)***
Тема 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПРОГРАММНОЙ ЗАЩИТЫ В ИНТЕРНЕТЕ	*Проработка учебного материала, подготовка отчета, подготовка к сдаче экзамена*	16	*Проверка отчета по практическойй работе*
Тема 2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	16	*Проверка отчета по лабораторной работе*
Тема 3. АТАКИ	*Проработка учебного материала, подго-*	16	*Проверка от-*

НА БЕСПРОВОДНЫЕ УСТРОЙСТВА	*товка отчета по лабораторной работе, подготовка к сдаче экзамена.*		*чета по лабораторной работе*
Тема 4. УЯЗВИМОСТИ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	16	*Проверка отчета по лабораторной работе*
Тема 5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	16	*Проверка отчета по лабораторной работе*
Тема 6. ОБЛАЧНЫЕ ТЕХНОЛОГИИ	*Проработка учебного материала, подготовка к сдаче экзамена.*	17	*Проверка отчета по практическойй работе*
Тема 7. СРЕДСТВА ЗАЩИТЫ	*Проработка учебного материала, подготовка к сдаче экзамена.*	17	*Проверка отчета по практическойй работе*
Тема 8. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ	*Проработка учебного материала, подготовка к сдаче экзамена.*	17	*Проверка отчета по практическойй работе*

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

Основная

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741
2. Кравченко Ю.А., Информационные и программные технологии. Часть 1. Информационные технологии : учебное пособие / Кравченко Ю. А. - Ростов н/Д : Изд-во ЮФУ, 2017. - 112 с. - ISBN 978-5-9275-2495-2 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785927524952.html

Дополнительная

1. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193

2. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2022. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490026
3. Голицына, О. Л. Информационные системы и технологии : учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. — Москва : ФОРУМ : ИНФРА-М, 2021. — 400 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-592-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1138895

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, ИФФВТ. - 2022. - 121 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/14545. - Режим доступа: ЭБС УлГУ. - Текст : электронный.

Согласовано:
Специалист ведущий НБ УлГУ Боброва Н.А. _____/_____2023
Должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение
- ОС MS Windows;
- ОС Linux;
- пакет приложений MS Office, Мой Офис;
- MS Visual Studio

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, [2023]. – 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, [2023]. - 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, [2023]. – 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, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – 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, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - 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, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – 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.

Согласовано:

начальник УИТТ / Бурдин П.П. /

Должность сотрудника УИТиТ ФИО подпись дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ИЛИ ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитории для проведения лекций, семинаров и лабораторных занятий, для проведения текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций.

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для предоставления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной инфромационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе, указывается в соответствии со сведениями о материально-техническом обеспечении и оснащенности образовательного процесса, размещенными на официальном сайте УлГУ в разделе «Сведения об образовательной организации».

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 особенностейАудитории для проведения лекций, семинарских занятий, для проведения лабораторных работ, для проведения текущего контроля и промежуточной аттестации.

Разработчик _____ зав. кафедрой ТТС Смагин А.А.

подпись *должность* *ФИО*

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1	Внесение изменений в п.п. в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» в пункт в) (см. ниже)	Смагин А.А.		12.09.2024

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

в) Профессиональные базы данных, информационно-справочные 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 : элек-
тронный.
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 / ОООВысшая 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/

Согласовано:

Начальник ОИ	Тюленева Н.А.		21.05.2024
Должность сотрудника	ФИО	подпись	дата