УТВЕРЖДЕНО

решением Учёного совета факультета математики,
информационных и авиационных технологий

от «21» июня 2019 г., протокол № 5/19

Председатель _____ / М.А. Волков
«21» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Направление (специальность)_ 11.03.02 Инфокоммуникационные технологии и системы связи____
код направления (специальности), полное наименование

Направленность (профиль/специализация) Интернет и гетерогенные сети
полное наименование

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

Дата введения в учебный процесс УлГУ: «__01_»__сентября__2020___г.

Программа актуализированана заседании кафедры: протокол №_1_ от 1 сентября 2021 г.
Программа актуализированана заседании кафедры: протокол №_1_ от 1 сентября 2022 г.
Программа актуализированана заседании кафедры: протокол №_1_ от 1 сентября 2023 г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Козловский Вячеслав Геннадьевич	Телекоммуникационных технологий и сетей	Доцент кафедры, кандидат технических наук, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой, реализующей дисциплину	Заведующий выпускающей кафедрой
_____/___Смагин А.А.____/ *Подпись* *ФИО* «_____»_____20_____г.	(_____/___Смагин А.А.___/ *Подпись* *ФИО* «_____»_____20_____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.6 учебного плана подготовки бакалавра по направлению 11.03.02 Инфокоммуникационные технологии и системы связи, профиль Интернет и гетерогенные сети.

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 ДИСЦИПЛИНЕ (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-1Способен к развитию коммутационных подсистем и сетевых платформ, сетей передачи данных, транспортных сетей и сетей радиодоступа, спутниковых систем связи	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-2способность организовывать и проводить экспериментальные испытания с целью оценки качества предоставляемых услуг, соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов	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 кон-

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	троля, 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-8Способен проводить расчеты по проекту сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных программ	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 обос-

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	нования проектов; навыками работы с программным обеспечением, использования программ;
ПК-11Способен осуществлять развитие транспортных сетей и сетей передачи данных, включая сети радиодоступа, спутниковых систем, коммутационных подсистем и сетевых платформ	Знать: перечень, назначение, принципы работы инструментальных средств и систем программирования; типовые задачи обеспечения информационной безопасности; Уметь: выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; разрабатывать алгоритмы решения типовых задач; Владеть: методами расчёта и инструментального контроля показателей технической защиты информации; - навыками и методиками разработки алгоритмов для решения задач информационной безопасности

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) ___4ЗЕТ_____

4.2. Объем дисциплиныпо видам учебной работы

Вид учебной работы	Количество часов 144 (форма обучения__очная___)	
	Всего по плану	В т.ч. по семестрам
		7
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	18	18
Семинары и практические занятия	18	18
Лабораторные работы	18	18
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы	Рефераты, отчеты по лабораторным работам	Рефераты, отчеты по лабораторным работам
Курсовая работа	Курсовая работа	Курсовая работа
Виды промежуточной аттестации	Экзамен	Экзамен

(экзамен, зачет)	36	36
Всего часов по дисциплине	144	144

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	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы,практикумы			
1	2	3	4	5	6	7	
1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПРОГРАММНОЙ ЗАЩИТЫ В ИНТЕРНЕТЕ		2	2			6	Отчет практического занятия
2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ		4	4	4	4	12	Отчет практического и лабораторного занятия
3. АТАКИ НА БЕСПРОВОДНЫЕ УСТРОЙСТВА		2	2	4	4	10	Отчет практического и лабораторного занятия
4. УЯЗВИМОСТИ		2	2	2	2	12	Отчет практического и лабораторного занятия
5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ		2	2	2	2	6	Отчет практического и лабораторного занятия
6. ОБЛАЧНЫЕ ТЕХНОЛОГИИ		2	2	2	2	4	Отчет практического и лабораторного

							занятия
7. СРЕДСТВА ЗАЩИТЫ		2	2	4	4	2	отчет
8. НОРМАТИВ-НАЯ ДОКУМЕН-ТАЦИЯ		2	2			4	Отчет практиче-ского за-нятия
Итого	144	18	18	18	18	54	Экзамен 36

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), Транспортный (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 ЗАЩИТЫ В ИНТЕРНЕТЕ	*Проработка учебного материала, подготовка отчета, подготовка к сдаче экзамена*	6	*Проверка отчета по практическойй работе*
Тема 2. КЛАССИФИКАЦИЯ АТАК ПО УРОВНЯМ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	12	*Проверка отчета по лабораторной работе*
Тема 3. АТАКИ НА БЕСПРОВОДНЫЕ УСТРОЙСТВА	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	10	*Проверка отчета по лабораторной работе*
Тема 4. УЯЗВИМОСТИ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	12	*Проверка отчета по лабораторной работе*
Тема 5. АТАКИ В ВИРТУАЛЬНОЙ СРЕДЕ	*Проработка учебного материала, подготовка отчета по лабораторной работе, подготовка к сдаче экзамена.*	6	*Проверка отчета по лабораторной работе*
Тема 6. ОБЛАЧНЫЕ ТЕХНОЛО-	*Проработка учебного материала, подготовка к сдаче экзамена.*	4	*Проверка отчета по прак-*

ГИИ			*тической работе*
Тема 7. СРЕДСТВА ЗАЩИТЫ	*Проработка учебного материала, подготовка к сдаче экзамена.*	2	*Проверка отчета по практической работе*
Тема 8. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ	*Проработка учебного материала, подготовка к сдаче экзамена.*	4	*Проверка отчета по практической работе*

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

Основная

1. 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. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2018. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://www.biblio-online.ru/bcode/414248

2. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://www.biblio-online.ru/bcode/451108

Учебно-методическая

1. Курилова О. Л. Межсетевое взаимодействие сетей NGN : лабораторный практикум / О. Л. Курилова, В. Г. Козловский, В. П. Смолеха; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2019.http://lib.ulsu.ru/MegaPro/Download/MObject/2010

Согласовано:

_____/_____/_____/_____Дол
Должность сотрудника научной библиотеки ФИО подпись дата

б)Программное обеспечение:_Аппаратно-программный комплекс «Сотсби OSI»

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2018]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2018]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.3. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2018]. - Режим доступа: https://e.lanbook.com.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2018].

3. База данных периодических изданий [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2018]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. Национальная электронная библиотека [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2018]. - Режим доступа: https://нэб.рф.

5. Электронная библиотека диссертаций РГБ [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2018]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

Согласовано:

_____/_____/_____/_____

Должность сотрудника УИТиТФИО подпись дата

2. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитория 24а для проведения лекций, семинарских занятий, выполнения лабораторных работ и практикумов и проведения текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций.

Аудитория укомплектована специализированной мебелью, учебной доской. мультимедийным оборудованием для предоставления информации большой аудитории оснащена компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной инфромационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования – аппаратно-программный комплекс «СОТСБИ OSI»/

3. 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.

Разработчик _____ доцент кафедры Козловский В.Г.

подпись должность ФИО