ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

УЧЕБНО-НАУЧНЫЙ ИНСТИТУТ
«ЭКОНОМИЧЕСКАЯ КИБЕРНЕТИКА»

Кафедра экономической кибернетики

УТВЕРЖДАЮ
Проректор по научно-методической и учебной работе
_____Е.И. Скафа
«17» апреля 2019 г.
М.П.

Рабочая программа учебной дисциплины

«БЕЗОПАСНОСТЬ СЕТЕЙ И ПРИЛОЖЕНИЙ»

Направление подготовки (специальность):	38.04.05 Бизнес-информатика
Магистерская программа:	ИТ-инновации в бизнесе
Программа подготовки:	академическая магистратура
Квалификация	магистр
Форма обучения:	очная

Донецк 2019

УТВЕРЖДАЮ
Директор Учебно-научного института
«Экономическая кибернетика»
_____ О.В. Снегин
«5» апреля 2019 г.

Программа составлена с учетом Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 38.04.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 08 апреля 2015 г. № 370 (с изменениями и дополнениями от 13.07.2017 г.).

Программа учебной дисциплины **«Безопасность сетей и приложений»** составлена на основе ГОС ВПО по направлению подготовки 38.04.05 Бизнес-информатика, утвержденному приказом Министерства образования и науки ДНР № 1007 от «28» сентября 2016 г., зарегистрированному в Министерстве юстиции ДНР от 18 октября 2016 г. № 1638; «Порядка об организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики», утверждённого приказом Министерства образования и науки ДНР «11» ноября 2017 г. №1171; учебных планов по направлению подготовки 38.04.05 Бизнес-информатика программы подготовки магистратуры (форма обучения: очная), утвержденных Ученым советом университета от 02.04.2019 г., протокол № 3.

Разработчик:
доцент кафедры экономической кибернетики
к.э.н. _____ Снегин О.В.

Программа учебной дисциплины утверждена на заседании кафедры моделирования экономики

Протокол № 9 от «21» марта 2019 г.

Зав. кафедрой экономической кибернетики _____ проф. Тимохин В.Н.

Программа учебной дисциплины одобрена учебно-методической комиссией Учебно-научного института «Экономическая кибернетика»

Протокол № 7 от «27» марта 2019 г.

Председатель учебно-методической
комиссии института _____ проф. Шаталова Т.С.

1. Область применения и место дисциплины в учебном процессе. Дисциплина «Безопасность сетей и приложений» относится к вариативной части Блока 1 «Дисциплины-модули», излагается студентам 1-го курса магистратуры в течение одного семестра, предусматривает текущий модульный контроль, а также сдачу экзамена, в конце семестра. Основывается на базе дисциплин бакалавриата: «Базы данных», «Корпоративные информационные системы», «Информационно-коммуникационные технологии в экономике», дисциплин магистратуры «Вэб-технологии в бизнесе», «Проект по модулю «Разработка вэб-приложений». «Виртуальные системы». Является основой для прохождение производственной, преддипломной практики, а также для написания магистерской диссертации.

2. Нормативные ссылки.

Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ.

Закон ДНР от 7 июля 2015 года № 55-IНС «Об образовании».

Закон ДНР от 28 марта 2016 года № 111-IНС «О внесении изменений в закон ДНР «Об образовании»«.

Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 38.04.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 08 апреля 2015 г. № 370 (с изменениями и дополнениями от 13.07.2017 г.)

ГОС ВПО по направлению подготовки 38.04.05 Бизнес-информатика, утвержденному приказом Министерства образования и науки ДНР № 1007 от «28» сентября 2016 г., зарегистрированному в Министерстве юстиции ДНР от 18 октября 2016 г. № 1638;

3. Структура дисциплины *(модуля)*.

Характеристика учебной дисциплины	
Направление подготовки	38.04.05 Бизнес-информатика
Магистерская программа	ИТ-инновации в бизнесе
Программа подготовки	академическая магистратура
Квалификация	магистр
Количество содержательных модулей	1
Дисциплина базовой / вариативной части образовательной программы	Базовая дисциплина Блока 1 «Дисциплины (модули)»
Формы контроля	1 модульный контроль, 1 экзамен во 2 семестре
Показатели	очная форма обучения
Количество зачетных единиц (кредитов)	3
Количество часов	108
Год подготовки	1
Семестр	2
Аудиторных часов, в том числе	36
- лекционных	18
- практических, семинарских	-
- лабораторных	18
- самостоятельной работы	72
в т.ч. индивидуальное задание	-
Недельное количество часов,	6
в т. ч. аудиторных	2

4. Описание дисциплины.

Цели и задачи. Целью изучения данной дисциплины является подготовка выпускников к автоматизированному решению прикладных задач; созданию новых конкурентоспособных информационных технологий и систем; подготовка выпускников к информационному обеспечению прикладных процессов; внедрению, адаптации, настройке и интеграции проектных решений по созданию ИС, сопровождению и эксплуатации современных ИС; подготовка выпускников к самообучению и непрерывному профессиональному самосовершенствованию.

Задачи: изучить теоретические основы функционирований Web-сети; основные стандарты Web-сети (HTTP, HTML, CSS, Javascript); понятие web-приложений и web-сервисов; основные подходы к разработке web-приложений; технологию разработки web-приложений Microsoft ASP.Net Web Forms; способы проектирования web-приложений; обеспечение безопасности web-приложений; обеспечить взаимосвязь с другими фундаментальными дисциплинами.

Требования к результатам освоения дисциплины.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ по направлению подготовки 38.04.05 «Бизнес-информатика» и основной образовательной программой высшего образования направления подготовки 38.04.05 «Бизнес-информатика» (ИТ-инновации в бизнесе).

Дисциплина нацелена на формирование профессиональных компетенций (ПК-8, ПК-9, ПК-19) выпускника.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки (профилю):

а) профессиональных (ПК):

проектная деятельность: способностью проектировать архитектуру предприятия (ПК-8);

способностью разрабатывать и внедрять компоненты архитектуры предприятия (ПК-9);

педагогическая деятельность:

готовностью проводить лекционные и практические занятия по управленческим и ИТ-дисциплинам (ПК-19)

В результате изучения учебной дисциплины студент должен *ориентироваться* в системе подходов и процедур к проектированию системы безопасности web-приложений предприятия;

знать:

основные понятия компьютерных сетей и систем телекоммуникации; основы объектно-ориентированного подхода к разработке программного обеспечения, основные киберугрозы и методы борьбы с ними.

уметь:

ставить и решать прикладные задачи с использованием современных информационно-коммуникационных технологий.

владеть: основами обеспечения защиты приложений от несанкционированного доступа.

5. Содержание дисциплины и формы организации учебного процесса.

Дисциплина «Безопасность сетей и приложений» предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельную работу студентов.

При проведении лекций и лабораторных работ используются мультимедийные презентации, раздаточные материалы. Лекции представляют собой систематические обзоры основных аспектов дисциплины. Лабораторные занятия дают возможность научить

применять полученные теоретические знания при выполнении и исследовании конкретных задач и ситуаций.

К методам изучения дисциплины «Безопасность сетей и приложений» следует отнести: лекции с освещением проблемных вопросов по модулям на основе сравнительного подхода; построение финансовой модели компании; ситуационное моделирование процессов; презентации для представления определенных исследований, результатов работы группы, отчеты о выполнении лабораторных работ; использование мультимедийных ресурсов. Самостоятельная работа студентов предусматривает подготовку к лабораторным работам, их выполнение, подготовку тезисов и эссе по отдельным вопросам изучаемых тем, изучение учебно-методической литературы, аннотаций статей, подготовку презентаций и докладов.

Порядковый номер и тема	**Краткое содержание темы**
Тема 1. Обнаружение компьютерных атак. Введение	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак.
Тема 2. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией	Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
Тема 3. Обнаружение компьютерных атак. Атаки на клиента	Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий.
Тема 4. Обнаружение компьютерных атак. Выполнение кода	Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА.
Тема 5. Обнаружение компьютерных атак. Разглашение информации и логические атаки	Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.
Тема 6. Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации,

Порядковый номер и тема	Краткое содержание темы
	возможности по анализу содержимого.
Тема 7. Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
Тема 8. Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
Тема 9. Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации

Порядковый номер и тема	Краткое содержание темы
	комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.

Тематический план.

№	Названия содержательных модулей и тем	Количество часов очная форма обучения				
		Всего	в том числе			
			лекции	практические занятия	лабораторные работы	самостоятельная работа
1	Тема 1. Обнаружение компьютерных атак. Введение	12	2		2	8
2	Тема 2. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией	12	2		2	8
3	Тема 3. Обнаружение компьютерных атак. Атаки на клиента	12	2		2	8
4	Тема 4. Обнаружение компьютерных атак. Выполнение кода	12	2		2	8
5	Тема 5. Обнаружение компьютерных атак. Разглашение информации и логические атаки	12	2		2	8
6	Тема 6. Технология межсетевого экранирования	12	2		2	8
7	Тема 7. Организация виртуальных частных сетей	12	2		2	8
8	Тема 8. Технологии защищенной обработки информации	12	2		2	8
9	Тема 9. Аудит информационной безопасности в компьютерных сетях	12	2		2	8
Итого		108	18	-	18	72

6. Темы лабораторных занятий.

Порядковый номер	Название темы	Кол-во часов
Лабораторная работа № 1	Выявление типа атаки	2
Лабораторная работа № 2	Атаки аутентификация и авторизация	2
Лабораторная работа № 3	Атаки на клиента	2
Лабораторная работа № 4	Атаки выполнения кода	2
Лабораторная работа № 5	Атаки разглашения информации и логические атаки	2
Лабораторная работа № 6	Межсетевое экранирование	2
Лабораторная работа № 7	Организация VPN	2
Лабораторная работа № 8	Защищенная обработка информации	2
Лабораторная работа № 9	Аудит информационной безопасности	2
ИТОГО		18

7. Самостоятельная работа.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей профессии, опытом проектной, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней.

Организация самостоятельной работы предусматривает следующие виды работ:

№ п/п	Виды самостоятельной работы студента	Объем, час.	
		очная	заочная
1	Изучение лекционного материала	20	25
2	Подготовка и выполнение лабораторных работ	20	25
3	Подготовка к выполнению заданий модульного контроля	6	11
4	Подготовка к экзамену	20	25
5	Решение и письменное оформление расчетно-аналитических заданий	6	10
6	Выполнение индивидуального задания	-	-
Итого:		72	96

8. Индивидуальные задания *(не предусмотрено программой подготовки по дисциплине)*

9.Контрольные вопросы

9.1 Теоретические вопросы

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов.
5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows.
6. Защита рабочих станций с использованием персональных сетевых фильтров.
7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.

8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.

9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.

10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.

11. Преимущества технологии терминального доступа. Обеспечение безопасности.

12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.

13.Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.

14.Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

15. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.

16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.

17. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

18.Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

19. Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист». Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «АванГард».

20.Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

21. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».

9.2 Практические вопросы

1. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.

2. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.

3. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.

4. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.

5. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых фильтров.

6. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.

7. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.

8. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.

9. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.

10. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.

11.С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.

12. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.

13.Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа ОС Windows Server 2003.

14. Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа ОС Windows Server 2003. Файл-сертификат открытого ключа прилагается.

15. Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа ОС Windows Server 2003.

16. Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

17. Осуществите криптографическую защиту сетевого трафика средствами СКЗИ StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

18. Организовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС Windows Server 2003.

19. Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.

20. Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMPпакетов большой длины.

21. Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.

22. Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users».

23. Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители.

24.Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping и широковещательной ICMP-посылки; утилиты icmpush (тип ICMPпакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.

25.С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС и запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа и версии ОС, а также сетевых сервисов.

26.С помощью программы NetCrunch, постройте карту сети компьютерного класса.

10.Образец экзаменационного билета

ГОУ ВПО «Донецкий национальный университет»
УНИ «Экономическая кибернетика»
Кафедра экономической кибернетики

Образовательно-квалификационный уровень Магистр — Очная форма обучения (**2** семестр)
Направление подготовки 38.04.05 Бизнес-информатика

Учебная дисциплина **«Безопасность сетей и приложений»**
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows.
2. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».
3. Результаты комплексного задания

Утверждено на заседании кафедры экономической кибернетики
Протокол №_ от_____ 201___ года

Зав. кафедрой _____Тимохин В.Н. *Экзаменатор* _____ Снегин О.В.

11.Образец тестового задания*(при наличии)*

Тест 3. Web-приложение - это ...

1. клиент-серверное приложение, в котором клиентом выступает браузер, а сервером выступает веб-сервер.
2. сайт в интернете.
3. сетевая игра.

12. Критерии оценивания

Критерии оценивания самостоятельной работы.

Общая оценка знаний студентов по дисциплине проводится по 100-балльной шкале согласно следующим критериям:

Вид работы	Баллы
Организационно-учебная работа студента в аудитории	5
Индивидуальная работа студента (выполнение лабораторных работ)	25
Самостоятельная работа	10
Модульная контрольная работа	20
Количество баллов по результатам текущего контроля	60
Итоговый контроль (экзамен)	40
Общий итог	100

Организационно-учебная работа студента в аудитории оценивается на основе таких критериев как посещаемость занятий, активность во время проведения лекционных и лабораторных занятий (вопросы лектору по теме лекционного материала, участие в обсуждении пройденного материала, самостоятельность в выполнении этапов лабораторных

работ и т.п.).

Самостоятельная и индивидуальная работа (включая выполнение СРС и ИРС) максимально оценивается в 35 баллов. В разрезе отдельных видов работ оценивание осуществляется следующим образом.

Оценивание СРС и ИРС по дисциплине «Безопасность Web-приложений»

Вид работы	Плановые сроки выполнения	Формы контроля и отчетности	Максимальное количество баллов
Индивидуальная работа (обязательные виды работ)			
1. Выполнение лабораторных работ по дисциплине	Один раз в неделю	Защита лабораторных работ	10
2. Решение и письменное оформление расчетно-аналитических заданий*	Один раз в течение зачетного модуля	Проверка правильности выполненных заданий	10
Итого по ИРС			**20**
Самостоятельная работа (обязательные виды работ)			
1. Подготовка аннотированного списка литературы по теме	Один раз в семестр	Обсуждение подготовленных материалов во время аудиторных занятий	2
2. Разработка web-сайта	Один раз в семестр		1
3. Выполнение заданий по администрированию			2
Итого по СРС (обязательные виды работ)			**5**
Самостоятельная работа (выборочные виды работ)			
1. Анализ web-приложения	Один раз в семестр	Обсуждение проведенной работы во время лабораторного занятия	1
3. Анализ конкретной производственной ситуации и разработка рекомендаций по модификации web-приложения	Один раз в семестр	Обсуждение проведенной работы во время лабораторного занятия или консультации	2
4. Написание реферата по исследуемой проблематике	Один раз в семестр	Защита материалов реферата во время практического занятия или консультации	2
5. Написание научных работ, участие в научных студенческих конференциях и семинарах	Один раз в семестр	Обсуждение с преподавателем подготовленных материалов, представление в печать, выступление с докладами на научных студенческих конференциях и семинарах	5
Итого по СРС (выборочные виды работ)			**10**
Всего по ИРС и СРС			**35**

***** *– данный вид работы является обязательной индивидуальной работой студента, однако с целью получения дополнительных баллов предоставляется возможность выполнения данного вида работы как одного из видов СРС.*

Критерии оценивания задания модульного контроля.

Максимальная общая сумма баллов, которую может получить студент, успешно выполнив все виды заданий, составляет 20 баллов.

1. Каждое правильно выполненное тестовое задание оценивается в 0,65 балла. Итого 20 правильных ответов – 13 баллов.

2. Решение задачи: правильное решение, сделан полный точный вывод – 7 баллов; правильное решение, но вывод неточный (неполный) – 6 баллов; правильное решение, но есть ошибки в расчетах, вывод не точный или отсутствует – 4-5 баллов; есть ошибки в ходе решения – 2-3 балла; приведены частично определенные формулы или сделаны определенные расчеты – 1 балл; нет решения – 0 баллов. Итого 1 правильно решенная задача – 7 баллов.

Критерии оценивания билета

Для выполнения заданий экзаменационного билета в соответствии с действующим положением оценка выставляется по четырехбальной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

В основу критерия оценки положена полнота и правильность выполнения задания. Кроме того, учитывается способность студента анализировать, систематизировать и синтезировать полученные знания; принимать обоснованные и аргументированные управленческие решения и прогнозировать предполагаемый результат от принятия решений. Студент должен излагать изученный материал в письменном виде логично, последовательно, с соблюдением требований высшей школы.

Для определения качества ответа на билет каждый правильный и полный ответ на содержащиеся в ней задания оценивается определенным количеством баллов:

Номер задания	Количество баллов за задание
1	10
2	15
3	15
Итого	*40*

За неполный и неаргументированный ответ на задания 1-3 снимается от 4 до 7 баллов.

Перевод общего числа баллов, полученных за выполнение заданий, входящих в билет, в экзаменационную оценку производится по шкале:

35-40 баллов	Отлично – A
30-34 баллов	Хорошо – B
27-29 баллов	Хорошо – C
25-26 баллов	Удовлетворительно – Д
20-24 баллов	Удовлетворительно – E
15-19 баллов	Неудовлетворительно - FX

Критерии оценивания итогового контроля по шкале.

Оценка ECTS	Сумма баллов за все виды учебной деятельности	Оценка по государственной шкале (экзамен, дифференциальный зачет)	Оценка по государственной шкале (зачет)
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено

C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

13. Материально-техническое обеспечение учебного процесса.

Лекционные и лабораторные занятия по дисциплине «Безопасность сетей и приложений» проводятся в учебных лабораториях:

– учебная лаборатория для проведения занятий лекционного типа, практических и лабораторных занятий, текущего контроля и промежуточной аттестации (ауд. № 101: г. Донецк, ул. Челюскинцев, 198а) - комплект учебной мебели на 14 посадочных места, комплект рабочего места преподавателя, магнитная доска; компьютер в комплекте с выходом в сеть мультимедийный проектор, ноутбук учебные, учебно-методические материалы для организации учебного процесса.

– учебная аудитория для проведения занятий лекционного типа, практических, текущего контроля и промежуточной аттестации (ауд. № 203: г. Донецк, ул. Челюскинцев, 198а. - комплект учебной мебели на 60 посадочных места, комплект рабочего места преподавателя, магнитная доска.

14. Рекомендованная литература.

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
Основная литература			
1.	Снегин О.В. Безопасность сетей и приложений : учебное пособие О.В. Снегин. – Донецк, ГОУ ВПО «ДонНУ». – 2019. – 101 с.	1	+
2.	Снегин О.В. Сетевая безопасность : учебно-практ. пособие О.В. Снегин. – Донецк, ГОУ ВПО «ДонНУ». – 2019. – 121 с.	1	+
3.	Милославская, Н.Г. Интрасети: доступ в Internet, защита : учеб. пособие для студентов вузов, обучающ. по спец. «Комплекс. обеспечение информ. безопасности автоматизир. систем» / Н.Г. Милославская, А.И. Толстой. - М. : ЮНИТИ, 2000. - 527 с.	1	-
4.	Информационная безопасность открытых систем [текст] : учебник для студентов вузов, обучающихся по специальности 075500 (090105) - «Комплексное обеспечение информационной безопасности автоматизированных систем» : [в 2 т.]. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. - М. : Горячая Линия-Телеком, 2006. - 535 с.	9	-
Дополнительная литература			

5.	Паркер, Тим. TCP/IP / Т. Паркер, К. Сиян ; Пер. с англ.: Е. Матвеев. - 3-е изд. - М. и др. : Питер, 2004. - 859 с.	2	-
6.	Лапонина, О. Р. Межсетевое экранирование : учеб. пособие / О. Р. Лапонина. - М. : Интернет-ун-т информ. технологий : Бином. Лаб. знаний, 2007. - 343 с.	4	-
7.	Брэгг Роберта. Безопасность сетей : полное рук. / Р. Брэгг, М. Родс-Оусли, К. Страссберг ; пер. с англ. Г. Трубникова, Я. Майсовой, М. Фадеевой. – Москва : ЭКОМ : Бином. Лаб. знаний, 2006. - 912 с.	2	-
8.	Олифер, В.Г. Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Москва [и др.] : Питер, 2010. - 943 с.	15	-

15. Программное обеспечение:

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений);
4. Лицензии GPL, Apache, BSD для свободного программного обеспечения: AnyLogic, Arena, Audit Expert, FreeLab, Cache, Scilab, R Studio, Powersim, Win QSB, MSM, Project expert, Sales expert, Statistica, Maple, Python, Eclipse, Free Pascal, Marketing Exper, Tries Mode, Prolog, ER-win, Антивирус Касперского, statistica neural networks, Linux Fedora, Libre Office, Adobe Acrobat Reader, xPDF, Oracle, Blender, 1С Предприятие, Business Studio, Visual Basic, КОМПАС-3D LT, Paint.NET, Gimp.

Рабочая программа рассмотрена и переутверждена на заседании кафедры моделирования экономики с изменениями (без изменений) на 20___ год.

Протокол № ___ от ___.___.20___г.
Зав. кафедрой В.Н. Тимохин