МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:
Первый проректор

_____ А.А. Каракозов
(подпись)

«21» мая 2021 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В8 Обеспечение безопасности корпоративной информации
(код и наименование дисциплины согласно учебному плану)

Направление подготовки: 38.04.05 Бизнес-информатика
(код и наименование направления / специальности)

Магистерская программа: IT инновации в бизнесе
(наименование профиля / магистерской программы / специализации)

Программа: магистратура
(бакалавриат, магистратура, специалитет)

Форма обучения: очная, заочная
(очная, заочная, очно-заочная)

Форма обучения:	Очная	Заочная
Семестр(ы)	2	2
Общая трудоёмкость в ЗЕТ/часах	3 (108)	3 (108)
Контактная работа (час.)	55	20
Лекции (час.)	34	8
Практические (семинарские) занятия (час.)	-	-
Лабораторные работы (час.)	17	6
Самостоятельная работа (час.), в том числе	21	58
Курсовой проект(работа) (семестр/час.)	-	-
Индивидуальное задание (кол./час.)	-	1/9
Контроль (экзамен, час./зачёт)	экзамен, 36	экзамен, 36

Донецк, 2021 г.

Рабочая программа дисциплины «Обеспечение безопасности корпоративной информации» составлена в соответствии с учебными планами по направлению подготовки 38.04.05 «Бизнес-информатика», магистерская программа «IT инновации в бизнесе» для 2021 года приёма.

Составитель:
Доцент кафедры экономической кибернетики,
кандидат технических наук _______________ Харитонов Ю.Е.
(подпись) (Ф.И.О.)

Рабочая программа **рассмотрена и принята** на заседании кафедры экономической кибернетики.
Протокол от «_7_» _05_ 2021 года № 9

Заведующий кафедрой _______________ __Коломыцева А.О.____
(подпись) (Ф.И.О.)

Рабочая программа **одобрена учебно-методической комиссией** ДОННТУ по направлению подготовки 38.04.05 «Бизнес-информатика»
Протокол от «_19__» ___05___2021 года № __4___

Председатель _______________ Коломыцева А.О.___
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры экономической кибернетики.
Протокол от «_____» ________________20___ года № ________
Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры экономической кибернетики.
Протокол от «_____» ________________20___ года № ________
Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры экономической кибернетики.
Протокол от «_____» ________________20___ года № ________
Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры экономической кибернетики.
Протокол от «_____» ________________20___ года № ________
Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры экономической кибернетики.
Протокол от «_____» ________________20___ года № ________
Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

1 ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Обеспечение безопасности корпоративной информации» рассматривает теоретические и практические аспекты информационной безопасности и защиты информации.

Цель дисциплины – формирование у обучаемых знаний в области теоретических основ информационной безопасности корпоративных информационных систем; навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Учебные задачи дисциплины – сформировать у студентов теоретические *знания* основ информационной безопасности и защиты информации; принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты корпоративной информации от несанкционированного доступа; *умения* проводить анализ степени защищенности корпоративной информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем; *навыки практической деятельности* в реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты корпоративной информации; в разработке средств и систем защиты корпоративной информации.

В результате освоения дисциплины студент должен:

Знать: - угрозы информационной безопасности, основные принципов организации безопасной работы в информационных системах и в сети интернет; описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством (РО 1-З ПК-3);

- современные цифровые средства и технологии, используемые для обработки, анализа и передачи данных при решении поставленных задач; описывать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством (РО 1-З ПК-6).

Уметь: - определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО (РО 1-У ПК-3);

- выбирать современные цифровые средства и технологии для обработки, анализа и передачи данных с учетом поставленных задач; определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО (РО 1-У ПК-6).

Владеть: - методологией выбора технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации (РО 1-В ПК-3);

- технологией решения поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности; обосновать выбор технических и программных средств защиты персональных данных и данных орга-

низации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации (РО 1-В ПК-6).

Перечисленные результаты обучения являются основой для формирования следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки на основе определенных индикаторов их достижения:

ПК-3 - Способен осуществлять принятие решений в профессиональной деятельности на основе использования современных методов и программного инструментария сбора, обработки и анализа данных, в том числе больших данных.

ПК 6 – Способен проектировать и совершенствовать архитектуру и ИТ-инфраструктуру предприятия в соответствии с потребностями развития бизнеса.

2 МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к части, формируемой участниками образовательного процесса, учебного плана (Блок 1 «Дисциплины-модули»). Основывается на итогах дисциплин программ бакалавриата: «Базы данных», «Корпоративные информационные системы», «Информационно-коммуникационные технологии в экономике».

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при изучении дисциплин «Разработка мобильных приложений», «WEB-технологии в бизнесе», выполнении НИР, прохождении преддипломной практики, подготовке магистерской диссертации.

3 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Распределение учебных часов по темам дисциплины и видам занятий

№ темы	Наименование тем (содержательных модулей)	Количество часов				
		Всего	В том числе			
			Лекции	Практ. (Семин.)	Лабор.	СР
1	Тема 1. Обнаружение компьютерных атак. Введение	**8/6**	**4/1**		**2/0**	**2/5**
2	Тема 2. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией	**8/6**	**4/1**		**2/0**	**2/5**
3	Тема 3. Обнаружение компьютерных атак. Атаки на клиента	**8/6**	**4/1**		**2/0**	**2/5**
4	Тема 4. Обнаружение компьютерных атак. Выполнение кода	**8/7**	**4/1**		**2/1**	**2/5**
5	Тема 5. Обнаружение компьютерных атак. Разглашение информации и логические атаки	**8/7**	**4/1**		**2/1**	**2/5**

6	Тема 6. Технология межсетевого экранирования	**8/8**	**4/1**		**2/1**	**2/6**
7	Тема 7. Организация виртуальных частных сетей	**9/8**	**4/1**		**2/1**	**3/6**
8	Тема 8. Технологии защищенной обработки информации	**9/8**	**4/1**		**2/1**	**3/6**
9	Тема 9. Аудит информационной безопасности в компьютерных сетях	**6/7**	**2/0**		**1/1**	**3/6**
Индивидуальное задание		**0/9**				**0/9**
Итого по видам занятий		**72/72**	**34/8**		**17/6**	**21/58**
Контроль		**36/36**				
ИТОГО		**108**				

Формирование компетенций в результате освоения тем дисциплины

Компетенция	Темы дисциплины, нацеленные на формирование компетенций
ПК-3	Тема 1, Тема 2, Тема 3, Тема 4, Тема 5
ПК-6	Тема 6, Тема 7, Тема 8, Тема 9

3.2 Лекции

Тема 1. **Обнаружение компьютерных атак. Введение**

Содержание темы 1:

Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Литература к теме 1: [1, 2, 3, 7]

Тема 2. **Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией**

Содержание темы 2:

Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

Литература к теме 2: [1, 2, 3, 7]

Тема 3**. Обнаружение компьютерных атак. Атаки на клиента**

Содержание темы 3:

Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий.

Литература к теме 3: [1, 2, 3, 7]

Тема 4. **Обнаружение компьютерных атак. Выполнение кода**

Содержание темы 4:

Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА.

Литература к теме 4: [1, 2, 3, 7]

Тема 5. **Обнаружение компьютерных атак. Разглашение информации и логические атаки**

Содержание темы 5:

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.

Литература к теме 5: [1, 2, 3, 7]

Тема 6. **Технология межсетевого экранирования**

Содержание темы 6:

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. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

Литература к теме 6: [1, 2, 3, 7]

Тема 7. **Организация виртуальных частных сетей**

Содержание темы 7:

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. Установка защищенного соединения. Защита на транспортном уровне.

Литература к теме 7: [1, 2, 3, 7]

Тема 8. **Технологии защищенной обработки информации**

Содержание темы 8:

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.

Литература к теме 8: [1, 2, 3, 7]

Тема 9. **Аудит информационной безопасности в компьютерных сетях**

Содержание темы 9:

Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы прове-

дения 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.

Литература к теме 9: [1, 2, 3, 7]

3.3 Лабораторные занятия

№ п/п	Тема занятия	Объем, час.	Литература
1	**Выявление типа атаки**	**2/0**	**[4, 6]**
2	**Атаки аутентификация и авторизация**	**2/0**	**[4, 6]**
3	**Атаки на клиента**	**2/0**	**[4, 6]**
4	**Атаки выполнения кода**	**2/1**	**[4, 6]**
5	**Атаки разглашения информации и логические атаки**	**2/1**	**[4, 6]**
6	**Межсетевое экранирование**	**2/1**	**[4, 6]**
7	**Организация VPN**	**2/1**	**[4, 6]**
8	**Защищенная обработка информации**	**2/1**	**[4, 6]**
9	**Аудит информационной безопасности**	**1/1**	**[4, 6]**
Итого:		**17/6**	

3.4 Практические занятия учебным планом не предусмотрены.

3.5 Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час.
1	**Изучение лекционного материала**	**10/24**
2	**Подготовка к лабораторным занятиям**	**11/25**
3	**Выполнение курсового проекта (36 часов)**	**-**
4	**Выполнение курсовой работы (27 часов)**	**-**
5	**Выполнение индивидуального задания (не менее 9 часов)**	**0/9**
Итого:		**21/58**

3.6 Курсовой проект (работа), индивидуальное задание

Курсовой проект (работа), индивидуальное задание по дисциплине учебным планом у студентов очной формы обучения не предусмотрены.

Для студентов заочной формы обучения предусмотрено индивидуальное задание [7].

4 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

4.1 Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Составляющая компетенции – полнота знаний

- нулевой уровень: неверные, не аргументированные, с множеством грубых ошибок ответы на вопросы. Уровень знаний ниже минимальных требований;
- минимальный уровень: даны не полные, неточные и неаргументированные ответы на вопросы. Допущено много грубых ошибок. Уровень знаний ниже минимальных требований;
- пороговый уровень: даны недостаточно полные, точные и аргументированные ответы на вопросы. Плохо знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено много негрубых ошибок;
- средний уровень: даны достаточно полные, точные и аргументированные ответы на вопросы. В целом знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;
- продвинутый уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;
- высокий уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько неточностей.

Составляющая компетенции – умения

- нулевой уровень: полное отсутствие понимания сути методики решения задачи, допущено множество грубейших ошибок / задания не выполнены вообще;
- минимальный уровень: слабое понимание сути методики решения задачи, допущены грубые ошибки. Решения не обоснованы. Не умеет использовать нормативно-техническую литературу. Не ориентируется в специальной научной литературе;
- пороговый уровень: достаточное понимание сути методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую литературу. Слабо ориентируется в специальной научной литературе;
- средний уровень: в целом понимает суть методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую и специальную научную литературу;
- продвинутый уровень: в целом понимает суть методики решения задачи, допущены неточности. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу;

- высокий уровень: понимает суть методики решения задачи. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу, передовой опыт.

Составляющая компетенции – владение навыками

- нулевой уровень: не демонстрирует владение навыками выполнения профессиональных задач. Не может выполнить задания;
- минимальный уровень: не демонстрирует владение навыками выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;
- пороговый уровень: владеет навыками выполнения профессиональных задач на пороговом уровне. Задания выполняет медленно и некачественно;
- средний уровень: владеет навыками выполнения профессиональных задач. Задания выполняет на среднем уровне по быстроте и качеству;
- продвинутый уровень: владеет уверенными навыками выполнения профессиональных задач. Быстро и качественно выполняет задания, иногда допуская незначительные погрешности;
- высокий уровень: владеет уверенными навыками выполнения профессиональных задач. Быстро и качественно выполняет задания, при необходимости демонстрируя творческий подход.

Обобщенная оценка сформированности компетенций

- нулевой уровень: на нулевом уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;
- минимальный уровень: на минимальном уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;
- пороговый уровень: на пороговом уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;
- средний уровень: на среднем уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;
- продвинутый уровень: на продвинутом уровне сформированы: все составляющие; одна или две из трёх, остальные – на высоком уровне;
- высокий уровень: на высоком уровне сформированы все составляющие компетенций.

4.2 Вопросы к экзамену и пример экзаменационного билета

Перечень вопросов к экзамену

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».

Пример экзаменационного билета

ГОУВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра экономической кибернетики

Программа	Магистратура
Направление подготовки	38.04.05 Бизнес-информатика
Магистерская программа	IT инновации в бизнесе

Семестр 2/2
Учебная дисциплина: ***Обеспечение безопасности корпоративной информации***
Форма обучения очная/заочная

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. Используя тестовую площадку, осуществить вход в веб-приложение с правами администратора.

Утверждено на заседании кафедры «Экономическая кибернетика»
Протокол от «__»_____ 20__ г. №

Заведующий кафедрой _____ доц. Коломыцева А.О.

Экзаменатор _____ доц. Харитонов Ю.Е.

4.3 Критерии оценивания результатов освоения программы

Критерии оценивания общей успеваемости (формирование итоговой оценки)

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

Вид работы (очное отделение)	**Баллы**
Организационно-учебная работа студента в аудитории	5
Индивидуальная работа студента (выполнение лабораторных работ)	25
Самостоятельная работа	30
Количество баллов по результатам текущего контроля	**60**
Экзамен (2 теоретических вопроса – по 10 баллов, практическое задание – 20 баллов)	**40**
Общий итог	**100**

Вид работы (заочное отделение)	**Баллы**
Индивидуальная работа (выполненное задание (30 баллов), оформление (10 баллов) и защита (20 баллов) работы)	**60**
Экзамен (2 теоретических вопроса – по 10 баллов, практическое задание – 20 баллов))	**40**
Общий итог	**100**

Организационно-учебная работа студента в аудитории оценивается на основе таких критериев как посещаемость занятий, активность во время проведения лабораторных занятий (вопросы лектору по теме лекционного материала, участие в обсуждении пройденного материала, выполнение заданий с помощью компьютерных технологий, своевременное качественное выполнение лабораторных зада-

ний и т.п.).

Критерии оценивания самостоятельной работы.

Самостоятельная работа (включая выполнение СРС) максимально оценивается в 55 баллов. В разрезе отдельных видов работ оценивание осуществляется следующим образом.

Оценивание СРС и ИРС по дисциплине «Обеспечение безопасности корпоративной информации»

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	15
2. Письменное оформление расчетно-аналитической части*	Один раз в семестр	Проверка правильности выполненных заданий	5*2=10
Итого по ИРС			**25**
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 таблиц и графиков результирующих параметров	Один раз в семестр		1
3. Выполнение расчетных заданий			12
Итого по СРС (обязательные виды работ)			**15**
Самостоятельная работа (выборочные виды работ)			
1. 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	15
Итого по СРС (выборочные виды работ)			**15**
Всего по ИРС и СРС			**55**

***** – *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 итогового контроля по шкале.

Полученная итоговая оценка по 100 бальной шкале определяет оценку по государственной шкале и шкале ECTS:

Сумма баллов по 100-бальной шкале	Оценка по шкале ECTS	Оценка по государственной шкале
90-100	A	Отлично
80-89	B	Хорошо
75-79	C	
70-74	D	Удовлетворительно
60-69	E	
35-59	FX	Неудовлетворительно
0-34	F*	

*- с обязательным повторным изучением дисциплины

4.4 Перечень контрольных заданий и иных материалов, необходимых для оценки знаний, умений и навыков

ЗНАНИЕ – ПОНИМАНИЕ

Фонд тестовых заданий по дисциплине (лекции)

1. Аутентификация – это

А) предоставление определённому лицу или группе лиц прав на выполнение определённых действий

Б) процедура проверки подлинности

В) процедура присвоения прав

Г) ни один из ответов не является правильным

2. Авторизация – это

А) предоставление определённому лицу или группе лиц прав на выполнение определённых действий

Б) процедура проверки подлинности

В) процедура присвоения прав

Г) ни один из ответов не является правильным

3. Какие существуют виды подбора в теории безопасности web-приложений

А) прямой и непрямой

Б) прямой и косвенный

В) прямой и обратный

Г) существует только один вид подбора

4. Интерфейсы администрирования через Web наиболее подвержены атаке типа

А) недостаточная аутентификация

Б) недостаточная авторизация

В) подбор

Г) предсказуемое значение идентификатора сессии

5. В каком типе атак злоумышленнику помощь может оказать наличие словаря

А) недостаточная аутентификация

Б) недостаточная авторизация

В) подбор

Г) предсказуемое значение идентификатора сессии

6. Использование для административного доступа ссылки в корневой директории сервера /admin/ является уязвимостью для атаки типа

А) недостаточная аутентификация

Б) недостаточная авторизация

В) подбор

Г) предсказуемое значение идентификатора сессии

7. Аутентификация на Web-сервере часто требует от пользователя

А) запоминания пароля

Б) запоминания парольной фразы

В) запоминания гиперссылки

Г) правильные варианты А и Б

8. Для доказательства того, что аутентификация была успешно пройдена, используется

А) логин

Б) пароль

В) идентификатор

Г) ip-адрес

9. SessionId=12345678;Role=User – это значение файла

А) hosts

Б) cookie

В) list

Г) url

10. Идентификатор сессии сохраняется в

А) системных файлах

Б) папке браузера

В) скрытых полях форм

Г) HTML

11. Определяет набор действий, которые может совершать пользователь, служба или приложение

А) процедура аутентификации

Б) процедура авторизации

В) процедура присвоения идентификатора

Г) ни один из ответов не является правильным

12. Таймаут сессии – это

А) срок действия идентификатора сессии

Б) срок действия роли пользователя

В) продолжительность сессии

Г) время неактивности пользователя

13. Какая уязвимость может позволить злоумышленнику воспользоваться историей браузера для просмотра страниц пользователя

А) недостаточная аутентификация

Б) подбор пароля

В) отсутствие таймаута сессии

Г) недостаточная авторизация

14. Можно выделить два типа систем управления сессиями на основе идентификаторов

А) разрешающий и строгий

Б) нестрогий и запрещающий

В) разрешающий и не разрешающий

Г) строгий и нестрогий

15. Какое понятие заключается в невредимости web-ресурсов

А) целостность

Б) доступность

В) аутентичность

Г) конфиденциальность

16. Используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированы Web-сервером, а не переданы из внешнего источника.

А) недостаточная аутентификация

Б) недостаточная авторизация

В) подмена содержимого

Г) логическая атака

17. Позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя.

А) подмена содержимого

Б) Cross-site Scripting

В) логическая атака

Г) разглашение информации

18. При использовании данной уязвимости злоумышленник посылает серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа.

А) HTTP Response Splitting

Б) Cross-site Scripting

В) логическая атака

Г) разглашение информации

19. Позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы.

А) логическая атака

Б) переполнение буфера

В) атака на функции форматирования строк

Г) подмена содержимого

20. При использовании этих атак путь исполнения программы модифицируется методом перезаписи областей памяти

А) Buffer Overflow

Б) HTTP Response Splitting

В) Cross-site Scripting

Г) Format String Attack

21. Открытый протокол для создания запросов и управления службами каталога совместимыми со стандартом X.500

А) HTTP

Б) OLED
В) LDAP
Г) FTP

22. Атаки этого класса направлены на выполнение команд операционной системы на Web-сервере путем манипуляции входными данными.

А) OS Commanding
Б) HTTP Response Splitting
В) Cross-site Scripting
Г) Format String Attack

23. Специализированный язык программирования, позволяющий создавать запросы к серверам СУБД

А) OQL
Б) PQL
В) SQL
Г) JAVA

24. Атаки данного класса позволяют злоумышленнику передать исполняемый код, который в дальнейшем будет выполнен на Web-сервере

А) SSI Injection
Б) SQL Injection
В) PQL Injection
Г) Format String Attack

25. Данный язык разработан для предоставления возможности обращения к частям документа на языке XML.

А) SQL
Б) XPath 1.0
В) JAVA
Г) C++

26. Атаки данного класса направлены на получение дополнительной информации о Web- приложении. Используя эти уязвимости, злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления.

А) логическая атака
Б) разглашение информации
В) недостаточная авторизация
Г) подбор паролей

27. Используется злоумышленником для получения информации об используемых сервером и клиентом операционных системах, Web-северах и браузерах.

А) Web Server/Application Fingerprinting
Б) SSI Injection
В) OS Commanding
Г) HTTP Response Splitting

28. Данная техника атак направлена на получения доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера

А) SSI Injection

Б) HTTP Response Splitting
В) Path Traversal
Г) OS Commanding

29. Данные атаки направлены на использование функций Web-приложения с целью обхода механизмов разграничения доступа

А) SQL Injection
Б) OS Commanding
В) Path Traversal
Г) Abuse of Functionality

30. При этой атаке, используя функции Web-приложения, злоумышленник может исчерпать критичные ресурсы системы, или воспользоваться уязвимостью, приводящий к прекращению функционирования системы

А) SQL Injection
Б) DDoS
В) Path Traversal
Г) Insufficient Anti-automation

ПРИМЕНЕНИЕ

Типовые вопросы и задания для лабораторных занятий

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; ути-

литы 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.

Типовые задания для домашней работы:
самостоятельная работа

Подготовка к лабораторным занятиям, подготовка к модульному контролю, подготовка к экзамену. Также проработка следующих вопросов:

1. Средства реализации атак.
2. Атаки с использованием промежуточных узлов и территорий.
3. Сигнатурный анализ и обнаружение аномалий.
4. Архитектура СОА.
5. Проблемы, связанные с СОА.
6. Написание правил фильтрации, возможности по анализу содержимого.
7. Защищенный обмен электронной почтой.
8. Создание единого пространства безопасности на базе Active Directory.
9. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.

Практические домашние задания:

Подготовка сообщений на тему:

1. Выявление типа атаки
2. Атаки аутентификация и авторизация
3. Атаки на клиента
4. Атаки выполнения кода
5. Атаки разглашения информации и логические атаки
6. Межсетевое экранирование
7. Организация VPN
8. Защищенная обработка информации
9. Аудит информационной безопасности

План сообщения:

1. Определение.
2. Краткая информация.
3. Особенности осуществления.
4. Исторические примеры.

5. Способы борьбы.
6. Вывод.

ТВОРЧЕСТВО

Индивидуальное задание

Цель: Идентификация и анализ угроз в корпоративном портале управления данными предприятия (объект выбрать самостоятельно).

Задачи:

1. Используя тестовую площадку, команда студентов получает доступ к веб-приложению и осуществляет в нем различные действия с правами администратора.
2. Используя тестовую площадку, команда студентов осуществляет поиск уязвимостей и разрабатывает рекомендации по их устранению.
3. Подготовка доклада и презентации о проделанной командной работе с тестовой площадкой.
4. Подготовка доклада и презентации о выявлении и построении схемы информационных потоков защищаемой информации на предлагаемом веб-ресурсе.

5 РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

I Основная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/87995.html. — Режим доступа: для авторизир. пользователей.
2. Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102011.html. — Режим доступа: для авторизир. пользователей.
3. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102070.html. — Режим доступа: для авторизир. пользователей.
4. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-

Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98349.html. — Режим доступа: для авторизир. пользователей.

II Дополнительная литература

5. Терминологический словарь по предметам кафедры «Бизнес-информатика» / составители Я. А. Донченко [и др.]. — Симферополь : Университет экономики и управления, 2020. — 240 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/108063.html. — Режим доступа: для авторизир. пользователей.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методические издания, разработанные в ДОННТУ:

6. Методические рекомендации для проведения лабораторных занятий по дисциплине «Обеспечение безопасности корпоративной информации» [Электронный ресурс]: для обучающихся по направлению подготовки 38.04.05 «Бизнес-информатика» всех форм обучения / ГОУВПО «ДОННТУ», каф. экон. кибернетики; сост.: Ю.Е. Харитонов, В.А. Белоусов. – 1,09 Мб. – Донецк: ДонНТУ, 2021. – 1 файл. - Систем. требования: Acrobat Reader. http://ed.donntu.org/books/21/m7225.pdf

7. Методические рекомендации к выполнению самостоятельной работы и контрольных работ по дисциплине «Обеспечение безопасности корпоративной информации» [Электронный ресурс]: для обучающихся по направлению подготовки 38.04.05 «Бизнес-информатика» всех форм обучения / ГОУВПО «ДОННТУ», каф. экон. кибернетики; сост.: Ю.Е. Харитонов. – 59,8 Кб. – Донецк: ГОУВПО «ДОННТУ», 2021. – 1 файл. - Систем. требования: Acrobat Reader. http://ed.donntu.org/books/21/m7224.pdf

Электронно-информационные ресурсы

ЭБС ДОННТУ – http://donntu.org/library

IPR BOOKS https://www.iprbookshop.ru/

Internet-ресурсы

УГТУ-УПИ. – URL: http://library.ustu.ru

Портал информационно-образовательных ресурсов УрФУ. – URL: http://study.urfu.ru. (СК № 11639 http://study.urfu.ru/view/aid_view.aspx?AidId=11639; УМКД№11096: http://study.urfu.ru/view/aid_view.aspx?AidId=11096)

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Учебная аудитория № 11.506, учебный корпус 11. для проведения занятий лекционного и лабораторного типа, групповых и индивидуальных консультаций,

текущего контроля и промежуточной аттестации. Мультимедийное оборудование: компьютер-ноутбук, проектор, экран. Специализированная мебель: доска аудиторная, парты. UBUNTU (бесплатная версия 18.04), OpenOffice (бесплатная версия 4.1.6).

2. Компьютерный класс №11.203, учебный корпус 11, для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная мебель: доска аудиторная, парты, столы. Оборудование: ноутбук на базе процессора Intel Core I5; стационарные компьютеры на базе процессоров Intel Celeron; мультимедийный проектор, экран; подключение к сети Internet по Wi-Fi. Программное обеспечение: MS Windows 10 (лицензия OEM), MS Windows 7 (лицензия OEM); OpenOffice (бесплатная версия 4.1.6); Microsoft Office 2007 Professional (лицензия Microsoftt № 00045-577-942-543); AnyLogic 8.6.0. PLE (ограниченная лицензия для обучения); PowerSim Express 10 (ограниченная лицензия для обучения); Python Anaconda 3.0 (открытая лицензия); MS SQL Server (открытая лицензия); MS Visual Studio 2010 Professional (лицензия MSDN AA и VMware AP); ARIS (ограниченная лицензия для обучения); 1С Предприятие 8.3 (ограниченная лицензия для обучения); Business Studio 3.0 (демонстрационная версия).

3. Помещения для самостоятельной работы с возможностью подключения к сети Internet и обеспечением доступа в электронную информационно-образовательную среду организации: читальные залы, учебные корпуса 2,3 (компьютерная техника с возможностью подключения к сети Internet и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ДОННТУ) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств. ОС - Alt Linux (лицензия GNU LGPL), Libreoffice 5.3.4 (лицензия GNU LGPL) - общественная лицензия MPL 2.0/ Grub loader for ALT Linux - лицензия GNU LGPL v3/ Mozilla Firefox - лицензия MPL2.0, Moodle (Modular Object-Oriented Dynamic Learning Environment) - лицензия GNU GPL.