

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Учетно-финансовый факультет
Кафедра бизнес-информатики

УТВЕРЖДАЮ
проректор

«17» апреля 2025 г.
МП П. А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ
ИНФОРМАЦИИ

Укрупненная группа направлений подготовки	27.00.00 Управление в технических системах
Программа высшего образования	Программа магистратуры
Направление подготовки	27.04.05 Инноватика
Направленность (профиль) образовательной программы	Цифровые технологии в бизнесе
Квалификация	Магистр
Форма обучения	Очная, заочная

Рабочая программа может быть адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2025

Рабочая программа дисциплины **«Обеспечение безопасности корпоративной информации»** для обучающихся по направлению подготовки 27.04.05 Инноватика (Профиль: Цифровые технологии в бизнесе) составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 27.04.05 Инноватика, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «04» августа 2020 г. № 875, Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2025 года.

Разработчик:

доцент кафедры бизнес-информатики,
канд. экон. наук, доцент

О.В. Снегин

Рабочая программа одобрена на заседании кафедры бизнес-информатики.
Протокол от 10.04.2025 г. № 8а.

Заведующий кафедрой

Т.О. Загорная

СОГЛАСОВАНО:

Декан учетно-финансового факультета
16.04.2025 г.

Н. В. Алексеенко

Учебно-методическая комиссия учетно-финансового факультета.
Протокол от 15.04.2025 г. № 6.
Председатель

А. А. Блажевич

Руководитель основной образовательной
программы, д-р экон. наук, проф.
10.04.2025 г.

Т. О. Загорная

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

дисциплины программы бакалавриата: Базы данных, Корпоративные информационные системы, Информационно-коммуникационные технологии в экономике; дисциплины магистратуры: Вэб-технологии в бизнесе, Разработка вэб-приложений.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Производственная практика: проектно-технологическая, Преддипломная практика.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	27.04.05 Инноватика (Магистерская программа: Цифровые технологии в бизнесе)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.3.2 Обеспечение безопасности корпоративной информации
Часть образовательной программы	Вариативная часть: выбор студента
Количество зачетных единиц / всего часов	3 / 108

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	2	3	0	34		74	108	зачет
Заочная	2	3	0	8		100	108	зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

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.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Профессиональные компетенции	Индикаторы	Результаты обучения
------------------------------	------------	---------------------

Профессиональные компетенции	Индикаторы	Результаты обучения
ПК-3. Способен проектировать и совершенствовать архитектуру и ИТ-инфраструктуру предприятия в соответствии с потребностями развития бизнеса	ПК-3.1. Выполняет проектирование целевой архитектуры процессов разработки и сопровождения требований к системам и управление качеством систем	ПК-3.1.1. Знает основные корпоративные информационные системы и базы данных; основные инновационные достижения в сфере развития современных информационных технологий
		ПК-3.1.2. Владеет современными технологиями в области средств передачи информации и проектирования информационных аналитических систем
	ПК-3.2 Осуществляет обоснование выбора методики управления инфраструктурой разработки и сопровождения требований к системам	ПК-3.2.1. Знает основные методики управления инфраструктурой предприятия.
		ПК-3.2.2. Умеет обосновывать выбор методики управления инфраструктурой предприятия.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Обнаружение компьютерных атак. Введение	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак.
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.
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.
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.
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.
6. Технология межсетевого	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с

экранирования	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, возможности по анализу содержимого.
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.
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.
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.

	<p>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 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.</p>
--	--

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – **очная**, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1. Обнаружение компьютерных атак. Введение		2		4	8
2. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией		4		4	12
3. Обнаружение компьютерных атак. Атаки на клиента		4		4	12
4. Обнаружение компьютерных атак. Выполнение кода		4		4	12
5. Обнаружение компьютерных атак. Разглашение информации и логические атаки		4		4	12
6. Технология межсетевого экранирования		4		5	13
7. Организация виртуальных частных сетей		4		5	13
8. Технологии защищенной обработки информации		4		5	13
9. Аудит информационной безопасности в компьютерных сетях		4		5	13
ИТОГО ПО КОМПОНЕНТУ ОПОП	0	34		74	108

6.2. Форма обучения – **заочная**, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего

1. Обнаружение компьютерных атак. Введение		0,5		10	10,5
2. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией		0,5		10	10,5
3. Обнаружение компьютерных атак. Атаки на клиента		1		10	11
4. Обнаружение компьютерных атак. Выполнение кода		1		10	11
5. Обнаружение компьютерных атак. Разглашение информации и логические атаки		1		12	13
6. Технология межсетевого экранирования		1		12	13
7. Организация виртуальных частных сетей		1		12	13
8. Технологии защищенной обработки информации		1		12	13
9. Аудит информационной безопасности в компьютерных сетях		1		12	13
ИТОГО ПО КОМПОНЕНТУ ОПОП	0	8		100	108

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные 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».

7.2. Лабораторные работы

1. Обнаружение компьютерных атак. Введение
2. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией
3. Обнаружение компьютерных атак. Атаки на клиента
4. Обнаружение компьютерных атак. Выполнение кода
5. Обнаружение компьютерных атак. Разглашение информации и логические атаки
6. Технология межсетевого экранирования
7. Организация виртуальных частных сетей
8. Технологии защищенной обработки информации
9. Аудит информационной безопасности в компьютерных сетях.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Виды работ	Баллы
Организационно-учебная работа в аудитории	35
Самостоятельная работа	30
Модульная контрольная работа	10
ИТОГО	75
Зачет	25
Общий итог	100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено

70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия по дисциплине «Обеспечение безопасности корпоративной информации» проводятся в 8-м учебном корпусе (г. Донецк, ул. Челюскинцев, д. 198а) университета. Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя. Выход в Интернет проводной или с использованием Wi-Fi.

Индивидуальные и групповые консультации студентам для проведения самостоятельной работы предоставляются на кафедре бизнес-информатики, находящейся в 8 учебном корпусе (ауд. 518).

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете 8-го учебного корпуса (ауд. 105), материально-техническую базу учебной лаборатории кафедры «Бизнес-информатики».

В процессе обучения студенты имеют возможность использовать учебные материалы по дисциплине «Обеспечение безопасности корпоративной информации», размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

10. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

10.1. Основная литература

1. Снегин О.В. Безопасность сетей и приложений : учебное пособие О.В. Снегин. – Донецк, ГОУ ВПО «ДонНУ». – 2019. – 101 с.
2. Снегин О.В. Сетевая безопасность : учебно-практ. пособие О.В. Снегин. – Донецк, ГОУ ВПО «ДонНУ». – 2019. – 121 с.
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.
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.

10.2. Дополнительная литература

1. Паркер, Тим. TCP/IP / Т. Паркер, К. Сиян ; Пер. с англ.: Е. Матвеев. - 3-е изд. - М. и др. : Питер, 2004. - 859 с.

2. Лапони́на, О. Р. Межсетевое экранирование : учеб. пособие / О. Р. Лапони́на. - М. : Интернет-ун-т информ. технологий : Бином. Лаб. знаний, 2007. - 343 с.
3. Брэ́гг Роберта. Безопасность сетей : полное рук. / Р. Брэ́гг, М. Родс-Оусли, К. Страссберг ; пер. с англ. Г. Трубникова, Я. Майсовой, М. Фадеевой. – Москва : ЭКОМ : Бином. Лаб. знаний, 2006. - 912 с.
4. Олифер, В.Г. Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Москва [и др.] : Питер, 2010. - 943 с.

11. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.
2. **eLIBRARY.RU:** научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. –Текст: электронный.
3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.
4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.
7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.
8. **Электронный архив ДонГУ:** раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

12. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).