МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
в г. Новороссийске
Кафедра информатики и математики

УТВЕРЖДАЮ
Проректор по работе с филиалами
ФГБОУ ВО «Кубанский
государственный университет»
_____А.А. Евдокимов
«__» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки 01.03.02 Прикладная математика и информатика

Направленность (профиль) Математические и информационные технологии в цифровой экономике

Форма обучения Очная

Квалификация Бакалавр

Краснодар 2023

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 «Прикладная математика и информатика», утвержденного приказом Министерства образования и науки Российской Федерации № 9 от 10 января 2018 года и ОПОП.

Программу составил(и):

Дьяченко С.В., канд.физ.мат.
наук, доцент, доцент
кафедры информатики и математики

Рзун И.Г., канд.физ.мат.наук, доцент,
доцент кафедры информатики и математики

Маслова Е.Ю. преподаватель
кафедры информатики и математики

Рабочая программа дисциплины утверждена на заседании кафедры информатики и математики протокол № 11 от 30.05.2023.

И.о.заведующего кафедрой (выпускающей) Небылова Я.Г.

Рабочая программа одобрена на заседании Учебно-методической комиссии филиала протокол № 1 от 30.05.2023

Председатель УМК С.Е. Ратенко

Рецензенты:

1. О.В.Ковалёва – директор ООО «Форкода»
2. М.К.Кунина - директор по развитию ООО «АЙТИ БИЗНЕС ЮГ»

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Основы информационной безопасности» является формирования у студентов знаний и навыков по вопросам информационной безопасности и защите информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы информационной безопасности» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Код компетенции	**Наименование компетенции**	**Индикаторы достижения компетенции** (в рамках данной дисциплины)
ОПК-7	Способен использовать информационно-коммуникационные компьютерные технологии, базы данных, пакеты прикладных программ для решения инженерно-технических и технико-экономических задач планирования и управления работами по инновационным проектам	ОПК-7.1 Демонстрирует знания принципов работы современных информационных технологий ОПК-7.2 Грамотно использует принципы работы современных информационных технологий для решения задач профессиональной деятельности
ПК-1	Способен анализировать проект (инновацию) как объект управления	ПК-1.1. Демонстрирует знания ключевых принципов управления проектом (инновацией)

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы информационной безопасности» относится к обязательной части блока Б1. О.02.11.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Основы информационной безопасности»

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Код компетенции	**Наименование компетенции**	**Предшествующие дисциплины/ модули, практики***	**Последующие дисциплины/модули, практики***
ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Информатика и программирование	Основы применения данных дистанционного зондирования Земли и геоинформационных систем Теория автоматического управления Управление инновационными проектами Технологии виртуальной и дополненной реальности Системы управления базами данных Экономическая безопасность инновационного предприятия Теория инноваций Организация управления финансово-хозяйственной деятельностью на инновационном предприятии Управление рисками на инновационном предприятии

			Организация инновационного производства на предприятиях отрасли Управление собственностью на инновационном предприятии Преддипломная практика Подготовка к сдаче и сдача государственного экзамена Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-1	Способен анализировать проект (инновацию) как объект управления	Цифровые технологии на производстве Основы цифровой экономики Управление качеством инновационных продуктов Технико-экономическое проектирование на инновационном предприятии Стратегический менеджмент на инновационном предприятии Антикризисный менеджмент инновационного предприятия Вариативная компонента Введение в управление инновационными процессами Управление инновационной деятельностью в промышленности Управление инновациями на различных этапах жизненного цикла	Основы применения данных дистанционного зондирования Земли и геоинформационных систем Теория автоматического управления Управление инновационными проектами Технологии виртуальной и дополненной реальности Системы управления базами данных Экономическая безопасность инновационного предприятия Теория инноваций Организация управления финансово-хозяйственной деятельностью на инновационном предприятии Управление рисками на инновационном предприятии Организация инновационного производства на предприятиях отрасли Управление собственностью на инновационном предприятии Природоохранная деятельность Преддипломная практика Подготовка к сдаче и сдача государственного экзамена Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 6 зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы		Всего часов	Семестр	
			4	5
Контактная работа, ак.ч.			16	
Лекции (ЛК)		34	16	18
Лабораторные работы (ЛР)				
Практические/семинарские занятия (СЗ)			34	36
Самостоятельная работа обучающегося, ак.ч.		85	58	27
Контроль (экзамен), ак.ч.		27		27
Общая трудоемкость дисциплины	ак.ч.	216	108	108
	зач.ед.	6	3	3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины по видам учебной работы

Наименование раздела дисциплины	Содержание раздела (темы)	Виды учебно

		й работы
Раздел 1 Сущность, задачи и проблемы информационной безопасности	Тема 1.1. Термин «высокотехнологический», современные подходы к его пониманию. Тема 1.2. Классификация наукоемких отраслей. Инновационный процесс как объект управления. Инновационный процесс: понятие, структура, содержание работ в высокотехнологических отраслях	Л, СР Л, СР
Раздел 2 Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ**.**	Тема 2.1 Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна.	Л, СР
Раздел 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.	Тема 3.1 Общие положения. Концептуальные документы в области информационной безопасности. Важнейшие федеральные нормативные правовые акты. Законы, касающиеся охраны интеллектуальной собственности. Положения Гражданского кодекса РФ по защите информации. Международное сотрудничество. Кодекс об административных правонарушениях. Уголовный кодекс и защита информации. Основные подзаконные акты в области информационной безопасности. Указы Президента РФ, постановления Правительства РФ, ведомственная нормативная база.	Л, СР
Раздел 4 Угрозы информационной безопасности. Управление рисками.	Тема 4.1. Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные Общая характеристика анализа и управления рисками. Шкалы. Оценка на основе выявления слабого звена. Оценка рисков на основе рассмотрения этапов вторжения. Программные средства, используемые для анализа рисков: CRAMM, RiskWatch, COBRA, Buddy System, RA Software Tool, ПО «Авнгард».	Л, СР
Раздел 5 Методы нарушения конфиденциальности, целостности и доступности информации.	Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные. Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных. Функции защиты информации. Стратегии защиты информации: оборонительная стратегия, наступательная стратегия, упреждающая стратегия. Архитектура систем защиты информации. Модели защиты информации.	Л, СР
Раздел 6 Причины, виды, каналы утечки и искажения информации.	Тема 6.1 Подходы к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования для вычислительных систем обработки конфиденциальной информации. Три группы требований. Стратегия, подотчетность, гарантии. Факторы, влияющие на требуемый уровень защиты информации.	Л, СР
Раздел 7 Функции и задачи защиты информации. Проблемы региональной информационной безопасности.	Тема 7.1. Методы формирования функций защиты. Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение	Л, СР

	требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на психику человека. Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	
Раздел 8 Информационные и автоматизированные системы.	Тема 8.1 Определения информационной (ИС) и автоматизированной системы (АС) обработки информации. ГОСТы на АС. Типовые виды структуры АС. Виды воздействия на информацию в ИС и АС. Угрозы безопасности АС и их классификация. Меры противодействия угрозам безопасности АС. Уязвимости АС. Принципы построения системы защиты АС.	Л, СР
Раздел 9 Технические каналы утечки информации**.**	Технические каналы утечки информации (ТКУИ) и способы их перекрытия. Пассивная и активная защита от утечки информации по техническим каналам. Определение, классификация и общая характеристика ТКУИ. Визуальные и акустические каналы. Защита информации в телефонных каналах. Защита от побочных электромагнитных излучений и наводок (ПЭМИН). Технические закладки. Способы обнаружения ТКУИ. Способы и методы перекрытия ТКУИ. Требования к выбору и оборудованию помещений для АС обработки данных по условиям защиты от ТКУИ. Понятие контролируемой территории и методы определения ее размеров. Общие сведения о защищенных средствах ЭВТ. Особенности защиты персональной вычислительной техники от утечки информации по техническим каналам.	Л, СР
Раздел 10 Технические средства обеспечения безопасности объекта	Определение и основные цели защиты современных объектов. Технические средства обеспечения защиты объекта: определение, системная классификация, общий анализ. Технические средства и системы охраны территории, зданий и помещений. Технические средства наблюдения и контроля за перемещением людей и предметов. Технические средства и системы опознавания людей. Технические средства и системы управления доступом на территорию, в здания и помещения, к средствам обработки и хранения информации. Методы выбора технических средств, общие сведения о рынке технических средств обеспечения безопасности.	Л, СР
Раздел 11 Программно-аппаратные средства обеспечения информационной безопасности.	Тема 11.1. Программно-аппаратные средства (ПАС) обеспечения защиты информации от несанкционированного доступа (НСД). СЗИ НСД “Аккорд”. Угрозы безопасности НСД. Основные концепции обеспечения защиты от НСД. Принципы программно-аппаратной защиты информации.	Л, СР
Раздел 12 Методы контроля доступа к информации.	Тема 12.1 Математические модели управления доступом к информации. Тема Потоковая модель доступа. Политика безопасности и модель доступа. Способы анализа моделей доступа и политик безопасности. Механизмы разграничения доступа в современных операционных системах. Электронные ключи. Идентификационные карточки, брелоки. Назначение, принципы устройства, возможности. Типы карточек. Принципы и методы использования. Программно-аппаратное обеспечение использования карточек. Биометрическая аутентификация. Единая биометрическая система (ЕБС) России.	Л, СР
Раздел 13 Вредоносные программы.	Тема 13.1 Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок Особенности взаимодействия с программно-аппаратными средствами защиты. Методика применения средств борьбы с вредоносными закладками на этапе эксплуатации систем. Системы разграничения доступа и защиты от ВЗ. Предупреждение и минимизация последствий воздействия ВЗ. Краткая характеристика мер защиты: юридические, административные и организационные, аппаратно-программные. Компьютерные вирусы. Классификация. Жизненный цикл. Основные каналы распространения вирусов и других вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ. Средства защиты от копирования. Примеры средств и технологий. Вопросы правовой защиты.	Л, СР

Раздел 14 Основы криптографической защиты информации.	Тема 14.1Основные понятия и задачи криптологии (криптографии). Цели и задачи криптологии. Секретность, целостность, аутентичность, неотказуемость, неотслеживаемость, анонимность. Понятие о криптографических примитивах и протоколах. Криптография с секретным и открытым ключом, плюсы и минусы. Причины и предпосылки появления новых направлений в криптографии. Введение в криптосистемы с секретным ключом (симметричные). Теоретическая и практическая стойкость. Блочные криптосистемы. Краткая характеристика стандартов DES, AES(Rijndael), ГОСТ 28147-89. Сравнение с новым ГОСТ Р 34.12- 2015 («Магма» и «КузНечик»). Генераторы псевдослучайных чисел и последовательностей. Поточные криптосистемы. Математические основы современной криптологии. Односторонние функции. Односторонние функции с секретом. Криптосистемы с открытым ключом (ассиметричные). Система RSA. Понятие о цифровой подписи. Краткая характеристика стандартов на цифровую подпись DSS, ГОСТ Р 34,10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012. Криптографические функции хеширования. Основные характеристики. Практические применения. Проблемы управления криптографическими ключами. Открытое распределение ключей. Инфраструктуры открытых ключей и стандарт X.509. Защита электронного документооборота с использованием электронной цифровой подписи. Примеры программно-аппаратных средств криптографической защиты: пакет PGP, пакет Криптон, СКЗИ «Верба-О», ПК «Inter-PRO»	Л, СР
Раздел 15 Обеспечение информационной безопасности операционных систем.	Тема 15.1Проблемы обеспечения ИБ ОС. Угрозы безопасности ОС. Понятие защищенной ОС. Архитектура подсистемы защиты ОС. Основные функции подсистемы защиты ОС. Разграничение доступа к объектам ОС. Аудит.	Л, СР
Раздел 16 Основы безопасности сетевых технологий.	Тема 16.1 Введение в Internet и Intranet. Способы нападения на сети и защита от межсетевого доступа. Особенности для различных уровней модели ISO/OSI. Технологии межсетевых экранов. Функции МЭ. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ. Персональные и распределенные сетевые экраны. Проблемы безопасности МЭ. Критерии оценки межсетевых экранов. Построение защищенных виртуальных сетей VPN. Варианты построения. Средства обеспечения безопасности VPN. Защита на канальном и сеансовом уровнях. Протоколы PPTP, L2TP, SSL/TLS, SOCKS. Защита на сетевом уровне. Протокол IPSEC. Основные схемы применения, преимущества средств безопасности IPSEC. Безопасность удаленного доступа к локальной сети. Централизованный контроль. Управление доступом по схеме однократного входа с авторизацией. Технологии обнаружения атак. Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS. Методы реагирования. Угрозы и уязвимости беспроводных сетей.	Л, СР
Раздел 17 Организационно-правовое обеспечение защиты информации.	Тема 17.1Сущность и роль организационно-правовых аспектов информационной безопасности. Человек как главное звено в системе защиты информации и как злоумышленник. Нормативная правовая база информационной безопасности. Закон РФ “Об информации, информационных технологиях и о защите информации”. Виды и категории информации ограниченного доступа: государственная и другие виды тайн. Закон РФ “О государственной тайне”, “О коммерческой тайне”, “О персональных данных”, “О национальной платежной системе”, “О безопасности критической информационной инфраструктуры Российской Федерации”. Государственная система лицензирования и сертификации деятельности в области защиты информации. Указ Президента РФ “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области	Л, СР

	шифрования информации". Закон РФ "Об электронной цифровой подписи". Уголовно- правовое регулирование защиты информации.	
Раздел 18 Стандарты информационной безопасности.	Тема18.1 Исторический очерк развития зарубежных стандартов информационной безопасности. Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга». Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности. Канадские критерии безопасности компьютерных систем. ГОСТ Р ИСО/МЭК 15408-2002, как аутентичный вариант общих критериев безопасности ИТ. Функциональные требования безопасности. Требования доверия к безопасности. Стандарты ISO/IEC 17799: 2002 (BS 7799:2000). Стандарты по менеджменту информационной безопасности ISO/IEC 27001-27040. Немецкие стандарты BSI. Стандарты SysTrust, SCORE, GIAC. Стандарты для беспроводных сетей. Отечественные стандарты информационной безопасности. Стандарты обеспечение информационной безопасности организаций банковской системы Российской Федерации. ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2 – 2018. Стандарты информационной безопасности в Интернете (IETF, RFC).	Л, СР
Раздел 19 Сертификация и аттестация в области информационной безопасности.	Тема 19.1 Назначение и общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Декларирование соответствия. Обязательная сертификация. Проведение сертификационных испытаний: принципы проведения испытаний, документы сертификационных испытаний. Сертификация продукции, ввозимой из-за границы РФ. Сертификация на региональном и международном уровнях.	Л, СР

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	**Оснащение аудитории**	**Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины** (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническим средствами мультимедиа презентаций	
Семинарская	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническим средствами мультимедиа презентаций Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа презентаций Комплект	
Лаборатория	Аудитория для проведения лабораторных работ, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и оборудованием	

Для самостоятельной работы обучающихся	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС	.

аудитория для самостоятельной работы обучающихся указывается обязательно

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1) Бондарев В.В. Введение в информационную безопасность автоматизированных систем (2-е издание). – М.: МГТУ им. Н.Э. Баумана. 2018. – 252с.
2) Организационно-правовое обеспечение информационной безопасности. под редакцией А.А. Александрова, М.П. Сычева – М.: МГТУ им. Н.Э. Баумана. 2018. – 292с.
3) Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. – М.: Горячая линия – телеком, 2018. – 314с

Дополнительная литература

1) Астахов А. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.
2) Bayuk J., CyberForensics: Understanding Information Security Investigations, Humana Press, 2010, - 200 с.
3) Bidgoli H., Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management Book, Wiley, - 1152 с.
4) Lance Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Osborne Media, 2010, - 396 с.
5) Moore T., Pym D., Ioannidis C., Economics of Information Security and Privacy, Springer, 2010, - 320 с.
6) Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006. - 544 с.
7) Варфоломеев А.А. Основы информационной безопасности. – М.: РУДН, - 412 с.
8) Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю., Теоретические основы компьютерной безопасности, – М: Радио и связь, 2000. -192 с.
9) Конеев И., Беляев А. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003. -752с.
10) Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2001г., -148 с.
11) Обеспечение информационной безопасности бизнеса, под ред. Курило А.П., Альпина Паблишерз, 2011, - 392 с.
12) Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006. – 400 с.
13) Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.
14) Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. – М.: Гелиос АРВ, 2005. - 192 с.

15) Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003. - 192 с.
16) Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие. – М.: Гелиос АРВ, 2004. - 144 с.
17) Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск.: БЕЛЛІТФОНД, 2005. -304 с.
18) Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2006. - 528 стр.
19) Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998. -336 с.
20) Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. пособие. - М.: ИД «ФОРУМ»: ИНФРА-М,2008. -416 с.
21) Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учеб. пособие. – М.: Гелиос АРВ, 2005. - 224 с.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1) Электронно-библиотечная система (ЭБС) РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров:

- ЭБС РУДН http://lib.rudn.ru/MegaPro/Web
- ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru
- ЭБС «Юрайт» http://www.biblio-online.ru
- ЭБС «Консультант студента» www.studentlibrary.ru
- ЭБС «Лань» http://e.lanbook.com/
- ЭБС «Троицкий мост»

2) Базы данных и поисковые системы:

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1) Курс лекций по дисциплине «Основы информационной безопасности»

** все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины в ТУИС*

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Основы информационной безопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

* ОМ и БРС формируются на основании требований соответствующего локального нормативного акта