МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по образовательной деятельности
В.Г. Шубаева
«24» мая 2023 г.

Основы информационной безопасности

Рабочая программа дисциплины

Направление подготовки/ *Специальность*	*10.03.01 Информационная безопасность*
Направленность (профиль) программы/ *Специализация*	*Безопасность компьютерных систем (в экономике и управлении)*
Уровень высшего образования	*Бакалавриат*
Форма обучения	*очная*
Год набора	*2023*

Составитель*(и)*:

д.э.н, Стельмашонок Елена Викторовна
к.т.н, Сухостат Валентина Васильевна

Часов по учебному плану	144	**Виды контроля в семестрах:**
в том числе:		
контактная работа	64	Экзамен: семестр 1
самостоятельная работа	44	
практическая подготовка	0	
часов на контроль	36	

Распределение часов дисциплины:

Семестр:	1
Вид занятий	Часы
Лекционные занятия	36
Практические занятия	28
Лабораторные работы	
Итого аудиторных часов	**64**
Самостоятельная работа	44
Часы на контроль	36
Итого академических часов	**144**
Общая трудоемкость в зачетных единицах	**4**

Санкт-Петербург
2023

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель:	Способствовать освоению студентами необходимого начального объема знаний в области информационной безопасности, умений и навыков использования современных программных средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О Основы информационной безопасности относится к обязательной части Блока 1.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.02 - Определяет место и роль информационной безопасности в системе национальной безопасности Российской Федерации; приобретает теоретические знания в области основных направлений информационной безопасности	Знать: место, роль и основные проблемы обеспечения информационной безопасности в системе национальной безопасности Российской Федерации. Уметь: анализировать и оценивать угрозы информационной безопасности объекта защиты. Владеть: профессиональной терминологией и методами анализа специальной литературы по вопросам обеспечения информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*

Номер и наименование тем и/или разделов/тем	Содержание дисциплины	Объем дисциплины (академические часы)			
		Контактная работа			СРО
		ЗЛТ	ПЗ	ЛР	
Тема 1. Введение. Составляющие национальных интересов Российской Федерации в информационной сфере.	Предмет и задачи дисциплины. Значение и место дисциплины в подготовке бакалавров информационной безопасности. Научная и учебная взаимосвязь дисциплины «Основы информационной безопасности» с другими дисциплинами рабочего учебного плана. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения	4			2

	дисциплины. Понятие и современная концепция национальной безопасности. Теоретические основы национальной политики в сфере защиты информации. Место информационной безопасности в системе национальной безопасности. Задачи в области обеспечения информационной безопасности Российской Федерации. Реализация Стратегии национальной безопасности Российской Федерации до 2020. Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Особенности обеспечения информационной безопасности в различных сферах общественной жизни. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Понятия информационной войны и информационного оружия. Проблема общемирового противодействия угрозам информационной безопасности.				
Тема 2. Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации.	Существующие подходы к содержательной части понятия «защита информации». Методологическая основа раскрытия сущности и определения понятия защиты информации. Цели защиты информации. Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации. Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации. Проблема информационной безопасности предприятия. Причины актуальности и важности проблемы обеспечения информационной безопасности. Достоверная информация и ценность информации. Право собственника информации на ее использование и защиту от доступа к ней. Уровни секретности сведений, составляющих государственную тайну. Перечень конфиденциальных сведений. Критерии, условия и принципы отнесения информации к защищаемой. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. Пути получения информации. Методы оценки количества информации. Информация как объект права собственности. Субъекты информационных отношений по отношению к определенной информации. Полномочия, включающие право собственности. Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.	2			3
Тема 3. Основные определения и задачи	Понятие безопасности автоматизированной информационной системы. Понятие защиты информации. Конфиденциальность, целостность,	4			3

информационной безопасности. Риски и угрозы информационной безопасности.	доступность. Субъекты, заинтересованные в обеспечении информационной безопасности. Уровни обеспечения информационной безопасности. Системы обеспечения информационной безопасности. Понятие угрозы информационной безопасности. Основные виды и источники угроз информационной безопасности. Внутренние и внешние угрозы. Понятие уязвимости информационной системы, атаки на систему. Понятие риска. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Политика безопасности. Информационные риски. Управление рисками. Качественный и количественный анализ риска. Методики оценки рисков. Модель оценки рисков. Экономические последствия атак на информацию. Структура ущерба предприятия от реализации угроз информационной безопасности.				
Тема 4. Методы обнаружения и блокирования угроз информационной безопасности. Классификация методов и средств защиты информации.	Этапы процесса осуществления атаки на информационную систему. Классификация систем обнаружения атак. Обманные системы. Системы контроля целостности и системы анализа журналов регистрации. Системы регистрации событий. Определение методов и технологий защиты информации. Обобщенные категории методов защиты информации. Организационные меры защиты информации. Технологические методы и средства защиты информации. Криптографические и правовые методы защиты информации. Особенности защиты на разных уровнях информационной системы. Противодействие инсайдерской деятельности.	2			3
Тема 5. Антивирусная защита.	Вредоносное программное обеспечение. Классификация вредоносных программ. Понятие компьютерного вируса. Троянские программы. Основные типы компьютерных вирусов. Основные классы вредоносных программ по характеру воздействия на компьютерную систему. Основные тенденции развития вирусных технологий. Возможные последствия вирусных атак. Методы и средства антивирусной защиты.	2			3
Тема 6. Системы идентификации и аутентификации.	Системы идентификации и аутентификации: основные определения, типы, область применения, классификация. Парольная защита. Общие подходы к построению парольных систем. Выбор паролей. Методы взлома паролей. Методы выбора паролей.	2	2		3
Тема 7. Разграничение доступа.	Дискреционное и мандатное управление доступом. Уровни доступа. Ролевое управление доступом. Двухуровневое назначение прав доступа.	2	2		3
Тема 8. Криптографические методы защиты информации.	Основы современной криптографии. Понятия и определения современной криптографии. Стойкость шифра. Стойкость алгоритмов шифрования. Классификация криптографических алгоритмов. Исторические шифры. Требования, предъявляемые к современным алгоритмам шифрования.	4	8		3

	Симметричные алгоритмы шифрования. Алгоритмы шифрования с открытым ключом.				
Тема 9. Стеганографические методы защиты информации.	Исторические методы стеганографии. Цифровая стеганография. Определения и методы цифровой стеганографии. Стегосистема. Области применения компьютерной стеганографии.	2	8		3
Тема 10. Технология электронной подписи.	Алгоритмы электронной подписи. Хеширование. Типы криптографических хеш-функций. Защищенная цифровая подпись. Цифровые сертификаты.	2	2		3
Тема 11. Методы защиты в операционных системах. Защита офисных документов.	Оценка безопасности операционной системы. Структура операционной системы. Инструменты настройки безопасности ОС Windows. Аутентификация пользователей Windows. Защищенная файловая система NTFS. Средства шифрования ОС Windows. Безопасное уничтожение данных. Методы защиты системных файлов в Windows. Защита работы пользователей в сети Windows. Защита офисных документов. Технологии защиты баз данных.	2	6		3
Тема 12. Сетевые технологии защиты.	Основные принципы организации сетевой защиты. Типичные угрозы безопасности и уязвимости сетевых информационных систем. Классификация способов несанкционированного доступа и жизненный цикл атак. Нападения на политику безопасности и процедуры административного управления. Нападения на постоянные и сменные компоненты системы защиты. Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей. Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки. Туннелирование. Технология виртуальных частных сетей. Защищенные сетевые протоколы.	2			3
Тема 13. Защита в Интернет.	Угрозы безопасности работы в сети Интернет, предотвращение их реализации. Безопасная доставка e-mail сообщений.	2			3
Тема 14. Нормативно-правовое обеспечение информационной безопасности.	Правовые меры защиты информации. Государственное регулирование в сфере информационной безопасности. Правовые режимы доступа к информации. Виды тайн. Персональные данные. Государственные регулирующие органы РФ. Компьютерные преступления.	2			3
Тема 15. Стандарты информационной безопасности.	Основные международные стандарты информационной безопасности. Процессы управления информационной безопасностью. Процесс управления рисками организации и его процедуры. Проблемы применения стандартов информационной безопасности.	2			3

Контроль:				**36**
Всего по дисциплине:	**36**	**28**	**0**	**44**

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Рекомендуемая литература

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Электронные ресурсы**
1. Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В. Сухостат, И.Н. Васильева .— Санкт-Петербург : Изд-во СПбГЭУ, 2019 .— 103 с.	http://opac.unecon.ru/elibrary ... D%D0%BE%D1%81%D1%82%D0%B8.pdf
2. Нестеров, С. А. Информационная безопасность: учебник и практикум. — Электрон. дан. — Москва: Юрайт, 2019. — 321 с.	https://urait.ru/bcode/434171
3. Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий. — Электрон. дан. — Москва : Русайнс, 2019 .— 226 с.	https://book.ru/book/932909
4. Васильева И.Н. Информационные технологии и защита информации: учебное пособие / И.Н. Васильева, Е.В. Стельмашонок.— Санкт-Петербург: Изд-во СПбГИЭУ, 2011.— 271 с.	http://opac.unecon.ru/elibrary/bibl/fulltext/Study/7864.pdf
5. Основы информационной безопасности : лабораторный практикум : направление подготовки -10.03.01 Информационная безопасность : направленность - Безопасность компьютерных систем (в экономике и управлении) / Минобрнауки России, С.-Петерб. гос. экон. ун-т, Каф. вычисл. систем и программирования ; [сост. И.Н. Васильева]Санкт-Петербург : [б. и.], 20211 файл (3,28 МБ)	http://opac.unecon.ru/elibrary ... B%D0%B0%D0%B1%D0%9F%D1%80.pdf

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства

- 7-Zip
- LibreOffice
- ОС Альт образование 10

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)

№	Наименование СПБД/ ИСС
1.	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2.	Научная электронная библиотека eLIBRARRY – www.elibrary.ru
3.	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4.	База данных ПОЛПРЕД Справочники – www.polpred.com
5.	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary www.oecd-ilibrary.org
6.	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
7.	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
8.	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
9.	Электронная библиотечная система BOOK.ru - www.book.ru
10.	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
11.	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
12.	Электронная библиотека СПбГЭУ– opac.unecon.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование учебных аудиторий, перечень	Адрес (местоположение) учебных аудиторий
Ауд. 2010 Учебная аудитория (для проведения занятий лекционного типа и	191023, г. Санкт-

занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 60 посадочных мест, рабочее место преподавателя, стол м/м - 1 шт., доска меловая - 2 шт., кафедра - 1 шт., стул - 2 шт., Компьютер Intel i3-2100 2.4 Ghz /4Gb/500Gb/Acer V193 19" - 1 шт., Мультимедийный проектор Optoma x 400 - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»
Ауд. 2032 Компьютерный класс (для проведения практических занятий, курсового проектирования (выполнения курсовых работ) с применением вычислительной техники). Оборудован мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 25 посадочных мест, рабочее место преподавателя (стол 1шт., кресло 1шт.), доска маркерная на колесиках 1 шт., маркерная доска на ножках 1шт., вешалки стойки 1шт., стол 2шт., стульев 4шт., доска обьявлений 1шт., жалюзи 2шт., Компьютер Intel I5-7400/16Gb/1Tb/ видеокарта NVIDIA GeForce GT 710/Монитор. DELL S2218H - 25 шт., Интерактивная доска SMARTB 680 - 1 шт., Шкаф телекоммуникационный настенный ЦМО ШРН-Э-6.650 - 1 шт., Коммутатор ProCurve Switch 2626 - 1 шт., Терминальная станция тонкий клиент в составе Sun Ray 2 client - 1 шт., Стойка для интерактивной доски 660x680 - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»
Ауд. 2021 Лаборатория "Лабораторный комплекс"Специализированная мебель и оборудование: Учебная мебель на 22 посадочных места (22 компьютерных стола, черных кресел 22шт.) Учебная мебель на 42 посадочных мест (парт 21 шт.,) рабочее место преподавателя (компьютерный стол 1шт.)доска, меловая 3-х секционная 1шт., доска маркерная на колесиках 1 ш., часы 1 шт., кафедра 1шт., стол 1шт., тумбочка 1шт., стул изо 4шт., вешалка стойка 2шт., жалюзи 3шт. Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Установка демонстрационных учебных фильмов - 1 шт., Компьютер в комплектации системный блок Intel pentium x2 g3250 клавиатура+мышь L (жесткий диск500gb,монитор philips 21.5') - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

– учебно-методической документацией;

– локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;

– графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

- фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
- базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
- профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
- индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные профессиональные специализированные области знаний, определяемые представителями рынка труда;
- метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Контрольные вопросы и задания к промежуточной аттестации

1 Актуальность решения проблем информационной безопасности.
2 Вредоносное программное обеспечение. Классификация вредоносных программ.
3 Понятие компьютерного вируса. Основные типы компьютерных вирусов.
4 Троянские программы.
5 Методы и средства антивирусной защиты.
6 Классификация антивирусных программ.
7 Парольная защита. Общие подходы к построению парольных систем.
8 Методы получения паролей.
9 Системы идентификации и аутентификации: основные определения, типы, область применения, классификация.
10 Конфиденциальность, целостность, доступность.
11 Методы выбора паролей
12 Субъекты, заинтересованные в обеспечении информационной безопасности.
13 Дискреционное и мандатное управление доступом.
14 Понятие угрозы информационной безопасности. Основные виды и источники угроз информационной безопасности.
15 Ролевое управление доступом.
16 Понятие уязвимости информационной системы, атаки на систему.
17 Цифровая стеганография. Определения и методы цифровой стеганографии.
18 Исторические методы стеганографии.
19 Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации.
20 Стегосистема. Области применения компьютерной стеганографии.
21 Политика безопасности.
22 Понятия и определения современной криптографии.
23 Стойкость криптоалгоритмов.
24 Основные международные стандарты информационной безопасности.
25 Исторические шифры замены.
26 Исторические шифры перестановки.
27 Проблемы применения стандартов информационной безопасности.
28 Симметричные алгоритмы шифрования.
29 Классификация криптографических алгоритмов.
30 Алгоритмы шифрования с открытым ключом.
31 Персональные данные. Защита персональных данных
32 Алгоритмы электронной подписи. Хеширование.
33 Государственное регулирование в сфере информационной безопасности.
34 Защищенная электронная подпись. Цифровые сертификаты.
35 . Компьютерные преступления.
36 Этапы процесса осуществления атаки на информационную систему. Классификация систем обнаружения атак.
37 Противодействие инсайдерской деятельности.
38 Типичные угрозы безопасности и уязвимости сетевых информационных систем.
39 Пути получения информации.
40 Способы противодействия несанкционированному сетевому и межсетевому доступу.

41 Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
42 Использование межсетевых экранов (Firewall). Критерии их оценки.
43 Безопасность работы в сети Интернет. Основные угрозы при работе в Интернет.
44 Безопасная доставка e-mail сообщений.
45 Классификация методов и средств защиты информации.
46 Обеспечение информационной безопасности на государственном уровне.
47 Обеспечение информационной безопасности на уровне предприятия.
48 Безопасность работы в сети Интернет. Угроза активного содержимого.
49 Безопасность работы в сети Интернет. Угроза удаленного администрирования.
50 Безопасность работы в сети Интернет. Угроза вмешательства в личную жизнь.

1.2 Темы письменных работ

Рабочей программой дисциплины не предусмотрено.

1.3 Контрольные точки

Номер контрольной точки	Тип контрольной точки	Способ проведения	Номера тем
1	Эссе	письменно	3-8
2	Индивидуальное задание	с помощью технических средств и информационных систем	9
3	Текущий контроль	с помощью технических средств и информационных систем	1-15

1.4 Другие объекты оценивания

Рабочей программой дисциплины не предусмотрено.

1.5 Самостоятельная работа обучающегося

Наименования самостоятельной работы	Номера тем
Подготовка к лекционным и практическим занятиям	1-15
Подготовка к экзамену	1-15

1.6 Шкала оценивания результата

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.

Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся:**

Формой итогового контроля по дисциплине является экзамен (или дифференцированный зачет), итоговая оценка формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
<=54	неудовлетворительно
55-69	удовлетворительно
70-84	хорошо
>=85	отлично

Шкала оценивания результата

2 (балл до 54)	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
3 (балл 55-69)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.
4 (балл 70-84)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
5 (балл 85-100)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.