

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



УТВЕРЖДАЮ

Проректор по учебной и
методической работе

/Шубаева В.Г./

« 17 » 06 20 19 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль) программы	Цифровизация экономической деятельности
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составитель:

 д.э.н., профессор Стельмашонок Е.В.

Санкт-Петербург

2019

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ.....	3
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ	4
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ	4
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА.....	6
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ	6
7.1. Методические указания для обучающегося по освоению дисциплины.....	6
7.2. Организация самостоятельной работы.....	7
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	7
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	7
9.1. Учебно-методическое и информационное обеспечение дисциплины.....	7
9.2. Материально-техническое обеспечение учебного процесса.....	9
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	9
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ.....	10

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины: приобрести необходимые теоретические знания в области информационной безопасности, сформировать умения и навыки работы пользователя для защиты информации в операционной среде.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина *Б1.О.19 «Информационная безопасность»* относится к обязательной части Блока 1, и является обязательной для освоения обучающимся вне зависимости от направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы, представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными в образовательной программе индикаторами достижения компетенций

Код и наименование компетенции выпускника	Код и наименование индикаторов компетенций	Планируемые результаты обучения по дисциплине
1	2	3
<i>ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</i>	<i>ОПК-3.1: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2: умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3: Готовит обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</i>	- знание основных задач информационной безопасности, мер, методов и средств обеспечения защиты информационных систем от угроз нарушения целостности, доступности и конфиденциальности. -умение использовать полученные знания в области обеспечения защиты программ и данных при решении своих профессиональных задач. -владение терминологией, используемой в законах в области информационной безопасности, основными требованиями регуляторов.

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов

Форма промежуточной аттестации: зачет.

Распределение фонда времени по темам дисциплины представлено в таблице 4.1

Таблица 4.1 – Распределение фонда времени по темам дисциплины

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
Тема 1. Основные определения и задачи информационной безопасности.	2			8
Тема 2. Риски и угрозы информационной безопасности	2			8
Тема 3. Обеспечение целостности информации. Антивирусная защита.	2			8
Тема 4. Системы идентификации и аутентификации. Парольные системы.	2			8
Тема 5. Обеспечение конфиденциальности информации. Криптографические и стеганографические методы защиты.	2	8		8
Тема 6. Технология электронной подписи	2	4		8
Тема 7. Управление доступом. Защищенные операционные системы. Защита документов	2	4		8
Тема 8. Методы защиты сетевых информационных технологий.	2			8
Тема 9. Правовое обеспечение информационной безопасности	2			10
Всего по дисциплине:	18	16		74

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Тема 1. Основные определения и задачи информационной безопасности

Понятие безопасности автоматизированной информационной системы. Понятие защиты информации. Конфиденциальность, целостность, доступность. Субъекты, заинтересованные в обеспечении информационной безопасности. Уровни обеспечения информационной безопасности. Классификация мер и методов защиты информации. Политика безопасности.

Тема 2. Риски и угрозы информационной безопасности

Понятие угрозы информационной безопасности. Системная классификация угроз информационной безопасности. Понятие уязвимости информационной системы, атаки на систему.

Информационные риски. Управление рисками. Качественный и количественный анализ риска.

Противодействие инсайдерской деятельности.

Тема 3. Обеспечение целостности информации. 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.

Тема 4. Системы идентификации и аутентификации. Парольные системы.

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.

Тема 5. Обеспечение конфиденциальности информации. Криптографические и стеганографические 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. Симметричные алгоритмы шифрования. Алгоритмы шифрования с открытым ключом.

Исторические методы стеганографии. Цифровая стеганография. Определения и методы цифровой стеганографии. Стегосистема. Области применения компьютерной стеганографии.

Тема 6. Технология электронной цифровой подписи

Алгоритмы электронной цифровой подписи. Хеширование. Типы криптографических хеш-функций. Защищенная цифровая подпись. Цифровые сертификаты.

Тема 7. Управление доступом. Защищенные операционные системы.

Дискреционное и мандатное управление доступом. Уровни доступа. Ролевое управление доступом. Двухуровневое назначение прав доступа.

Защищенные операционные системы. 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.

Тема 8. Методы защиты сетевых информационных технологий.

Основные принципы организации сетевой защиты. Типичные угрозы безопасности и уязвимости сетевых информационных систем. Классификация способов несанкционированного доступа и жизненный цикл атак.

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. Безопасность работы в сети Интернет. Безопасная доставка e-mail сообщений.

Тема 9. Правовое обеспечение информационной безопасности. Стандарты в области информационной безопасности.

Правовые меры защиты информации. Государственное регулирование в сфере информационной безопасности. Доктрина информационной безопасности РФ. Закон 149 ФЗ «Об информации, информационных технологиях и защите информации». Правовые режимы доступа к информации. Виды тайн. Персональные данные. Государственные регулирующие органы РФ. Компьютерные преступления. Стандарты в области информационной безопасности.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия

№ темы	Тема занятия	Вид занятия / Оценочное средство
1	2	3
5	Соккрытие сообщения методом знаков одинакового начертания Стеганография в ASCII-логотипах Анализ шифра табличной перестановки Криптоанализ шифра простой замены Изучение шифра RSA	ПЗ: <i>Решение практических задач.</i>
6	Использование цифровой подписи проектов VBA Изучение электронной цифровой подписи Эль-Гамала	ПЗ: <i>Решение практических задач.</i>
7	Создание учетных записей пользователей, шифрование и управление доступом к файлам и папкам на локальном компьютере Защита документов MS WORD Защита книг MS EXCEL Защита баз данных MS ACCESS	ПЗ: <i>Решение практических задач.</i>

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1. Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине в самом начале учебного курса, обучающийся должен ознакомиться с учебно- методической документацией:

- рабочей программой дисциплины: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся;
- порядком проведения текущего контроля успеваемости и промежуточной аттестации;
- графиком консультаций преподавателей кафедры.

Систематическое выполнение учебной работы на занятиях лекционных и семинарских типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины обучающимся следует:

- слушать, конспектировать излагаемый преподавателем материал;
- ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;
- задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;
- выполнять задания практических занятий полностью и в установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратиться к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим

письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 – недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2. Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к ограничениям их здоровья.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ темы	Вид самостоятельной работы
1	2
5- 7	Подготовка к практическим занятиям
1-4	Самостоятельное изучение темы
8-9	Самостоятельное изучение темы

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В рамках реализации дисциплины «Информационная безопасность» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 5,6,7.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по изучению программных средств защиты информации.

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1. Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое обеспечение дисциплины

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	Основная/ дополнительная литература	Книгообеспеченность	
		Кол-во экз. в библ. СПбГЭУ	Электронные ресурсы
Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Электрон. дан. — Москва : РИОР : ИНФРА-М,	основная	—	https://znaniu.m.com/catalog/document?id=359537

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	Основная/ дополнительная литература	Книгообеспеченность	
		Кол-во. экз. в библ. СПбГЭУ	Электронные ресурсы
2020. — 336 с.			
Нестеров Ф.А. Информационная безопасность : учебник и практикум . — Электрон. дан. — Москва : Издательство Юрайт, 2019. — 321 с.	основная	—	ЭБС Юрайт
Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В. Сухостат, И.Н. Васильева .— Санкт-Петербург : Изд-во СПбГЭУ, 2019 .— 103 с. — Сведения доступны также по Интернету: opac.unicon.ru .	основная	35	ЭБ OPAC.UNEC ON.RU
Васильева И.Н: Информационные технологии и защита информации: учебное пособие /И.Н. Васильева, Е.В. Стельмашонок.— Санкт-Петербург: СПбГИЭУ, 2011.— 271 с. – Сведения доступны также по Интернету: opac.unicon.ru .	дополнительная	71	ЭБ OPAC.UNEC ON.RU
Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий : словарь . — Электрон. дан. — Москва : Русайнс, 2019. — 226 с.	дополнительная	—	ЭБС BOOK.ru
Мельников В.П. Информационная безопасность и защита информации : учебное пособие / В.П.Мельников, С.А.Клейменов, А.М.Петраков ; под ред.С.А.Клейменова .— 5-е изд., стер. — Москва : Академия, 2011 .— 336 с.	дополнительная	25	—

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
1	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2	Научная электронная библиотека eLIBRARY – 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

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
2	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
3	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
4	Электронная библиотечная система BOOK.ru - www.book.ru
5	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
6	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
7	Электронная библиотека СПбГЭУ– opac.unicon.ru

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№	Наименование ПО
1	Microsoft Windows Professional (КОНТРАКТ № 244/20 «26» июня 2020 г.)
2	Microsoft Office Professional (КОНТРАКТ № 244/20 «26» июня 2020 г.)
3	7-Zip (freeware)

Таблица 9.2.2 – Перечень учебных аудиторий для проведения учебных занятий, оснащенных оборудованием и техническими средствами обучения

Наименование учебных аудиторий, перечень оборудования и технических средств обучения	Адрес (местоположение) учебных аудиторий
Ауд. 2025 Компьютерный класс (для проведения практических занятий, с применением вычислительной техники). Специализированная мебель и оборудование: Учебная мебель на 19 посадочных мест (19 компьютерных столов, 19 черных кресел), рабочее место преподавателя (компьютерный стол 1 шт., кресло 1 шт.), доска маркерная на колесиках 1 шт., стол 3 шт., кресло черное 2 шт., стул из 5 шт. Компьютер Intel i5 7400/1Tb/8Gb/Philips 243V5Q 23' - 20 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»

10. 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.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).