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

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/ Шубаева В.Г./
«28» августа 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Направление подготовки	09.03.03 Прикладная информатика
Направленность (профиль) программы	Управление бизнес-процессами и проектами
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составители:
_____/ к.ф.-м.н., доцент Васильева И.Н.
_____/ д.э.н., профессор Стельмашонок Е.В.

Санкт-Петербург
2020

СОДЕРЖАНИЕ

1.ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины: изучение основ, подходов, сложившихся международных практик и методик управления в сфере комплексной информационной безопасности и приобретение необходимых умений и навыков использования средств и методов защиты информационных технологий.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина *Б1.В.08* «Управление комплексной информационной безопасностью информационных технологий» относится к части, формируемой участниками образовательных отношений Блока 1.

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**
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	*УК-1.3.Анализирует источник информации с точки зрения временных и пространственных условий его возникновения.*	*Определяет виды и формы информации, подверженной угрозам, а также тенденции реализации возможных угроз и рисков информационной безопасности организации.*
ПК-6. Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	*ПК-6.2. Учитывает комплексную информационную безопасность при организации ИТ-инфраструктуры организации*	*Выявляет требования комплексной информационной безопасности к использованию информационных технологий в составе информационной инфраструктуры организации.*

4.ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа, из которых 36 часов самостоятельной работы обучающегося согласно РУП отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: экзамен.

Распределение фонда времени по темам дисциплины представлено в таблице 4.1.

Таблица 4.1 – Распределение фонда времени по темам дисциплины

Номер и наименование тем *и/или разделов/тем*	**Объем дисциплины (ак. часы)**			
	Контактная работа			**СРО**
	ЗЛТ	**ПЗ**	**ЛР**	
1	***2***	***3***	***4***	***5***
Тема 1. Основные понятия и задачи информационной безопасности.	2			8
Тема 2. Угрозы и риски информационной безопасности	2			8
Тема 3. Методы и средства защиты информационных технологий.	8	46		12
Тема 4. Правовое обеспечение информационной безопасности. Стандарты в области управления информационной безопасности.	4			12
Тема 5. Основы корпоративного управления в сфере информационной безопасности.	2			12
Тема 6. Система менеджмента информационной безопасности.	2			12
Тема 7. Назначение, структура и содержание управления комплексной системой защиты информации в организации.	2			12
Всего по дисциплине:	22	46		76

5.СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Тема 1. Основные понятия 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.

Тема 2. Угрозы и риски 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. Методы и средства защиты информационных технологий

Управление доступом. 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

Обеспечение целостности данных. 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.

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.

*Обеспечение конфиденциальности информации***.** Криптографические методы зашиты 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.

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

*Технология электронной подписи***.** Алгоритмы электронной подписи. Хэширование. Типы криптографических хэш-функций. Защищенная цифровая подпись. Цифровые сертификаты.

*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. 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 4. 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.

Тема 5. Основы корпоративного управления в сфере информационной безопасности.

Основные направления обеспечения информационной безопасности организации. Риск-ориентированный подход. Понятие корпоративной политики безопасности. Основные требования и подходы к разработке политики безопасности. Многоуровневый подход.

Управления информационной безопасностью на основе соответствий требованиям (compliance management). Анализ упущений (gap-анализ). Модель непрерывного совершенствования (замкнутый цикл менеджмента PDCA).

Тема 6. Система менеджмента информационной безопасности.

Процессы управления и обеспечения информационной безопасности. Эталонная модель процесса для управления ИБ (ГОСТ Р 57640-2017, ISO/IEC TS 33052:2016). Проблемы внедрения процессного подхода. Построение системы менеджмента информационной безопасности (СМИБ) на основе ISO/IEC 27001. Организационная структура системы менеджмента информационной безопасности. Система частных менеджментов. Сертификация соответствия СМИБ ISO/IEC 27001.

Тема 7. Назначение, структура и содержание управления комплексной системой защиты информации в организации.

Понятие, сущность и цели управления комплексной системой защиты информации.

Принципы управления комплексной системой защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системой защиты информации. Структура и содержание общей технологии управления комплексной системой защиты информации.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия

№ темы	Тема занятия	Вид занятия / Оценочное средство
1	*2*	*3*
3	Сокрытие сообщения методом знаков одинакового ания Стеганография в ASCII-логотипах Анализ шифра табличной перестановки Криптоанализ шифра простой замены Изучение шифра RSA Использование цифровой подписи проектов VBA Изучение электронной цифровой подписи Эль-Гамаля Создание учетных записей пользователей, вание и управление доступом к файлам и папкам на ном компьютере Защита документов MS WORD Защита книг MS EXCEL Защита баз данных MS ACCESS	ПЗ: *Решение практических задач*.

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***
1- 7	*Подготовка к экзамену.*
3	*Подготовка к практическим занятиям и выполнение индивидуальных заданий.*

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В рамках реализации дисциплины «*Управление комплексной информационной безопасностью информационных технологий*» 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 теме 3.

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**
Васильева И.Н: Информационные технологии и защита информации: учебное пособие / И.Н.	Основная	71	ЭБ OPAC.UNEC

Васильева, Е.В. Стельмашонок.— Санкт-Петербург: СПбГИЭУ, 2011.— 271 с. – Сведения доступны также по Интернету: opac.unecon.ru.			ON.RU
Нестеров С.А. Информационная безопасность : учебник и практикум. — Электрон. дан. — Москва : Издательство Юрайт, 2019. — 321 с.	Основная	–	ЭБС Юрайт
Барабанова, М.И. Открытые системы и сети. Комплексная безопасность в системах и сетях современного предприятия : учебник / М.И. Барабанова, В.И. Кияев, А.В. Саитов ; под ред. В.И. Кияева .— Санкт-Петербург : Изд-во СПбГЭУ, 2019 .— 495 с. — Сведения доступны по Интернету: opac.unecon.ru .	Дополнительная	45	ЭБ OPAC.UNECON.RU
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с.	Дополнительная	–	https://znanium.com/catalog/document?id=358722

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
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

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.unecon.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.

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.

Таблица 9.2.1 – Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (ПО)

№	Наименование ПО
1	Microsoft Windows Professional
2	Microsoft Office Professional
3	7-Zip (freeware)
4	FireFox 77.0.1 (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. 2022 Лаборатория "Лабораторный комплекс". Специализированная мебель и оборудование: Учебная мебель на 19 посадочных мест (19 компьютерных стола, 19 черных кресел) рабочее место преподавателя (компьютерный стол 1 шт., кресло 1 шт.), доска меловая односекционная 1 шт., доска маркерная на колесиках 1 шт., стол 1 шт., стул 1 шт., жалюзи 1 шт., вешалка стойка 1ш т., Компьютер Intel i5 4460/1Тб/8Гб/монитор Samsung 23" - 1 шт., Компьютер Intel i5 4460/1Тб/8Гб/ монитор Samsung 23" - 18 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. 2018 Компьютерный класс (для проведения практических занятий, с применением вычислительной техники). Специализированная мебель и оборудование: Учебная мебель на 16 посадочных мест (16 компьютерных столов, 16 черных кресел), рабочее место преподавателя 2стола+1кресло, доска меловая 1 шт., доска маркерная на колесиках 1 шт., вешалка стойка 1 шт., стул изо10 шт., Компьютер Intel I5-7400/16Gb/1Tb/ видеокарта NVIDIA GeForce GT 710/Монитор. DELL S2218H - 17 шт., Точка беспроводного доступа Wi-Fi Тип1 UBIQUITI UAP-AC-PRO - 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 64 посадочных места, рабочее место	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

преподавателя, доска меловая 3-х секционная - 1 шт., доска маркерная на колесиках - 1 шт., часы - 1 шт., кафедра - 1 шт., стол - 1 шт., тумбочка - 1 шт., стул изо - 4 шт., вешалка стойка - 2 шт., жалюзи - 3 шт., Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Ноутбук HP 250 G6 1WY58EA- 2 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.	

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).