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.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рабочая программа дисциплины

Направление подготовки	38.03.05 Бизнес-информатика
Направленность (профиль) программы	Деловая аналитика
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составители:
_____/д.э.н., профессор Стельмашонок Е.В.

Санкт-Петербург
2020

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 5
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 6
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 7
7.1. Методические указания для обучающегося по освоению дисциплины 7
7.2. Организация самостоятельной работы 7
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 8
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8
9.1 Учебно-методическое и информационное обеспечение дисциплины 8
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 9

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: дать студентам необходимые знания, умения и навыки в области защиты информации.

Задачи:

- определение места и роли информационной безопасности в системе национальной безопасности Российской Федерации;
- приобретение теоретических знаний в области основных направлений информационной безопасности;
- формирование умения использования современных программных средств защиты информации;
- выработка практических навыков работы пользователя для защиты данных в операционной среде;
- закрепление теоретических знаний по обработке и защите информации в среде пакетов прикладных программ универсального назначения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В. "Информационная безопасность" относится к вариативной части Блока 1, является обязательной для освоения обучающимся после выбора обучающимся 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 планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
1	2	3
ПК-9 Организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ - инфраструктуры предприятия	ПК-9	**Декомпозиция II** **Знать:** основные технологии и методы обеспечения информационной безопасности ИТ - инфраструктуры предприятия **З (II)(ПК-9)** **Уметь:** применять методы обеспечения информационной безопасности ИТ - инфраструктуры предприятия **У (II) (ПК-9)** **Владеть:** способами организации построения защищенных систем и управления информационной безопасностью ИТ - инфраструктуры предприятия **В (II) (ПК-9)**

ПК-11 Умение защищать права на интеллектуальную собственность	ПК-11	**Знать:** действующее законодательство по защите прав на интеллектуальную собственность, основы организации информационной безопасности для защиты прав на интеллектуальную собственность **З (ПК-11)** **Уметь:** выбирать необходимые методы и средства защиты прав на интеллектуальную собственность, методы информационной безопасности для обеспечения экономической информационной безопасности **У (ПК-11)** **Владеть:** навыками работы со средствами защиты информации, приемами защиты прав на интеллектуальную собственность **В (ПК-11)**

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

Форма промежуточной аттестации: зачет - 6 семестр.

Распределение фонда времени по темам дисциплины по очной форме обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	*2*	*3*	*4*	*5*
Раздел 1. Основы информационной безопасности				
1. 1. Основные определения и задачи информационной безопасности	1			3
1.2. Риски и угрозы информационной безопасности	1			3
Раздел 2. Методы и средства обеспечения информационной безопасности				
2.1. Классификация методов и средств защиты информации	1			3
2.2. Антивирусная защита	2			3
2.3. Системы идентификации и аутентификации	2			3
2.4 Системы разграничения доступа	2			3
2.5. Стеганографические методы	2	4		3
2.6. Криптографические методы	2	4		3
2.7. Технология электронной подписи	2	4		3
2.8. Методы защиты в операционных системах	1	4		3
2.9. Сетевые технологии защиты	2			3
2.10. Правовое обеспечение информационной безопасности	2			3
Всего по дисциплине:	**20**	**16**		**36**

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

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Раздел 1. Основы информационной безопасности

Тема 1.1. 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. Системы обеспечения информационной безопасности.

Тема 1.2. Риски и угрозы 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.

Раздел 2. Методы и средства обеспечения информационной безопасности

Тема 2.1. Классификация методов и средств 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.

Тема 2.2. 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 2.3. 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.

Тема 2.4. Системы разграничения доступа

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

Тема 2.5. Стеганографические методы

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

Тема 2.6 Криптографические методы

Основы современной криптографии. Понятия и определения современной криптографии. Стойкость шифра. Стойкость алгоритмов шифрования. Классификация криптоаналитических атак. Классификация криптографических алгоритмов. Исторические шифры. Требования, предъявляемые к современным алгоритмам шифрования. Симметричные алгоритмы шифрования. Алгоритмы шифрования с открытым ключом.

Тема 2.7. Технология электронной цифровой подписи

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

Тема 2.8. Методы защиты в операционных системах

Защищенные информационные 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 2.9. 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. **Безопасность работы** в сети Интернет. Безопасная доставка e-mail сообщений.

Тема 2.10. 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.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	2	3
2.5	Сокрытие сообщения методом знаков одинакового начертания Стеганография в ASCII-логотипах	ПЗ/ Решение прикладных задач
2.6	Анализ шифра табличной перестановки Криптоанализ шифра простой замены Изучение шифра RSA	ПЗ/ Решение прикладных задач
2.7	Использование цифровой подписи проектов VBA Изучение электронной цифровой подписи Эль-Гамаля	ПЗ/ Решение прикладных задач.
2.8	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/Решение прикладных задач.

* ПЗ – практические занятия, СЗ – семинарские занятия, ЛР – лабораторные работы

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 установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратится 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*
1.1	Подготовка к текущему контролю.
1.2	Подготовка к текущему контролю.
2.1	Подготовка к текущему контролю.
2.2	Подготовка к текущему контролю.
2.3	Подготовка к текущему контролю.

№ темы	Вид самостоятельной работы
2.4	Подготовка к выполнению практического задания.
2.5	Подготовка к выполнению и защите индивидуального задания 1.
2.6	Подготовка к выполнению и защите индивидуального задания 2.
2.7	Подготовка к выполнению практического задания.
2.8	Подготовка к выполнению практического задания.
2.9	Подготовка к текущему контролю.
2.10	Подготовка к текущему контролю.

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании 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 2.5 2.6, 2.7, 2.8.

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. Васильева, Е.В. Стельмашонок.— Санкт-Петербург: СПбГИЭУ, 2011.— 271 с. – Сведения доступны также по Интернету: opac.unecon.ru.	Основная	71	opac.unecon.ru Полный текст
Нестеров С.А. Информационная безопасность : учебник и практикум. — Электрон. дан. — Москва : Издательство Юрайт, 2019. — 321 с.	Основная		ЭБС Юрайт
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2019. — 592 с.	Дополнительная		ЭБС ZNANIUM

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
1	Электронная библиотека СПбГЭУ– opac.unecon.ru
2	Научная электронная библиотека eLIBRARRY – http://elibrary.ru/defaultx.asp

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Электронная библиотечная система BOOK.ru - http://www.book.ru
2	Электронная библиотечная система ЭБС ЮРАЙТ - https://urait.ru
3	Электронная библиотечная система IPR BOOKS - http://www.iprbookshop.ru/
4	Электронная библиотечная система ЗНАНИУМ (ZNANIUM) - https://new.znanium.com

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, 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)

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).