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.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Рабочая программа дисциплины

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составители:
_____/к.т.н., доцент Солодянников А.В.
_____/ст. преподаватель Морозов С.К.

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 11
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 12
7.1. Методические указания для обучающегося по освоению дисциплины 12
7.2. Организация самостоятельной работы 12
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 13
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 13
9.1 Учебно-методическое и информационное обеспечение дисциплины 13
9.2. Материально-техническое обеспечение учебного процесса 14
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 14
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 15

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины – дать студентам необходимые знания в области инженерно-технической защиты информации, умения и навыки использования методов и средств инженерно-технической защиты информации на объектах информатизации, создаваемых и эксплуатируемых в различных сферах народного хозяйства.

Задачи дисциплины:

- приобретение теоретических знаний в области инженерно-технической защиты информации;
- формирование умения применять современные методы инженерно-технической защиты информации;
- выработка практических навыков использования средств инженерно-технической защиты информации;
- выработка практических навыков контроля эффективности средств инженерно-технической защиты информации;
- формирование умения организовывать работу по внедрению методов и средств инженерно-технической защиты информации на предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В «Инженерно-техническая защита информации» относится к вариативной части дисциплин Блока и 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)
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Первый уровень (пороговый) (ПК-1) –1	Знать: принципы построения и использования технических средств защиты информации: пассивных и активных средств защиты сетей электропитания, средств объемного зашумления. З1(ПК-1) Уметь: определять вариант размещения на объекте технических средств, предназначенных для защиты сетей электропитания и защиты от ПЭМИН. У1(ПК-1) Владеть: методами анализа угроз согласно требованиям руководящих документов В1(ПК1)
ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по	Первый уровень (пороговый) (ПК-5) –1	Знать основные нормативные правовые акты и нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в области инженерно-технической защиты информации. З1(ПК-5) Уметь: структурировать и систематизировать

требованиям безопасности информации		требования, изложенные в нормативных правовых актах и нормативных методических документов Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в области инженерно-технической защиты информации. У1(ПК-5) Владеть: методами использования нормативных правовых актов и нормативных методических документов Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в области инженерно-технической защиты информации для решения прикладных задач. В1(ПК-5)
ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	(ПК-6)	Знать: принципы организации контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации З(ПК-6) Уметь: на основе полученных знаний проводить контрольные проверки работоспособности и эффективности применяемых технических средств защиты информации У(ПК-6) Владеть: методами контроля работоспособности и эффективности применяемых технических средств защиты информации В(ПК-6)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов, из которых 36 часов самостоятельной работы обучающегося отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: зачет -5 семестр, экзамен - 6 семестр.

Распределение фонда времени по темам 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. Угрозы безопасности и способы добывания информации техническими средствами				
Введение	1			
1.1.Основные свойства информации как предмета инженерно-технической защиты.	1			3
1.2. Демаскирующие признаки объектов защиты.	1			3
1.3. Источники и носители информации, защищаемой техническими средствами	1			3
1.4 Источники опасных сигналов	1			3
1.5. Виды угроз безопасности информации, защищаемой техническими средствами.	1			3
1.6. Органы добывания информации.	1			3
1.7. Технология добывания информации.	1			3

1.8. Способы несанкционированного доступа к источникам информации.	1			3
1.9. Способы и средства добывания информации техническими средствами.	1			3
1.10. Классификация и структура технических каналов утечки информации.	1			3
1.11. Концепция инженерно-технической защиты информации.	1			4
Раздел 2. Способы и средства инженерно-технической защиты				
2.1. Способы и средства инженерной защиты и технической охраны.(12)	2	4	4	4
2.2. Способы и средства защиты информации от наблюдения.(13)	2	4	4	4
2.3. Способы и средства защиты информации от подслушивания.(14)	2	4	4	4
2.4. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки (15)	2	4	4	4
2.5. Способы предотвращения утечки информации по материально-вещественному каналу.(16)	2			4
Всего за 5 семестр	22	16	16	54
Раздел 3. Основные направления инженерно-технической защиты на объекте информатизации				
3.1. Общие положения по инженерно-технической защите информации в организации.(17)	2			9
3.2. Организационные и технические меры по инженерно-технической защите информации в организации.(18)	4	4	4	9
3.3. Системный подход к инженерно-технической защите информации(19)	4	4	4	9
3.4. Моделирование объекта защиты.(20)	4	4	4	9
3.5. Моделирование угроз информации.(21)	4	4	4	9
3.6. Методические рекомендации по разработке мер защиты.(22)	4			9
Всего за 6 семестр	22	16	16	54
Всего по дисциплине:	44	32	32	108

*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. Угрозы безопасности и способы добывания информации техническими средствами

Введение

Предмет, цели, задачи и содержание курса инженерно-технической защиты информации (ИТЗИ). Роль и место курса в подготовке бакалавров в области информационной безопасности государственных и коммерческих структур. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

1.1. Основные свойства информации как предмета инженерно-технической защиты

Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты. Понятие о демаскирующих признаках объектов защиты. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта. Статистический и семантический подходы к оценке количества информации. Показатели качества информации. Старение информации. Полезность и цена информации. Копирование информации.

1.2. Демаскирующие признаки объектов защиты

Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Понятие о признаковых структурах. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазонах. Основные характеристики аналоговых и дискретных (импульсных) электрических сигналов, средств связи, радиолокационных станций, лазерных излучений и других. Основные признаки, характеризующие физические и химические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах.

1.3. Источники и носители информации, защищаемой техническими средствами

Понятие об источниках, носителях и получателях информации. Классификация источников информации. Источники технической и экономической информации при проведении научных исследований, разработке, производстве и эксплуатации продукции, на различных этапах и в различных видах коммерческой деятельности. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела). Способы записи информации на различные виды носителей. Виды модуляции (манипуляции) сигналов. Характеристики модулированных сигналов. Принципы съема информации путем демодуляции (детектирования). Искажения информации в результате воздействия на сигналы помех. Виды помех. Методы обеспечения безопасности информации в условиях воздействия помех.

1.4. Источники опасных сигналов

Понятие об опасных сигналах и их источниках. Основные и вспомогательные технические средства и системы. Побочные электромагнитные излучения и наводки. Акустоэлектрические преобразователи, их виды и принципы работы. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС). Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС. Паразитные наводки в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий.

1.5. Виды угроз безопасности информации, защищаемой техническими средствами

Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

1.6. Органы добывания информации

Роль разведки в деятельности государств и коммерческих структур. Структура органов разведки. Виды зарубежной разведки и разведки коммерческих структур. Классификация технической разведки по физической природе носителя. Носители технических средств разведки. Принципы ведения разведки.

1.7. Технология добывания информации

Основные принципы добывания и обработки информации техническими средствами. Структура органов управления, добывания и информационной работы. Видовая и комплексная обработка данных и сведений. Текущие и эталонные, первичные и вторичные признаковые структуры. Принципы идентификации и интерпретации, обнаружения и распознавания объектов, измерения характеристик демаскирующих признаков. Методы синтеза информации. Пути автоматизации процессов добывания и обработки информации.

1.8. Способы несанкционированного доступа к источникам информации

Понятие о разведывательном контакте и его условиях. Виды доступа к источникам информации (физический контакт и дистанционный доступ). Принципы доступа к источникам информации без физического проникновения в контролируемую зону. Классификация и характеристики наземных средств дистанционного съема информации с носителей. Принципы доступа к источникам информации без нарушения государственной

границы. Возможности зарубежной космической, воздушной и морской разведки в мирное время.

1.9. Способы и средства добывания информации техническими средствами

Способы и средства наблюдения. Факторы, влияющие на эффективность обнаружения и распознавания объектов наблюдения. Структура и основные характеристики средств наблюдения. Параметры зрительной системы человека. Классификация и основные характеристики объективов. Виды и технические характеристики визуально-оптических приборов. Принципы конструкции и работы, виды и характеристики фото- и киноаппаратов. Особенности цифровых фотоаппаратов. Технические эндоскопы. Структура средств телевизионного наблюдения. Принципы работы телевизионных камер на вакуумных трубках и приборах с зарядовой связью. Принципы видеозаписи. Характеристики телевизионных средств наблюдения и регистрации. Принципы работы и характеристики приборов ночного видения. Камуфлирование средств наблюдения. Принципы радиолокационного и радиотеплового наблюдения. Способы повышения разрешающей способности радиолокаторов.

Способы и средства перехвата сигналов. Задачи, решаемые при перехвате сигналов. Структура средств перехвата и их функции. Классификация и характеристики антенн. Структура радиоприемника и его характеристики. Особенности и основные характеристики сканирующих радиоприемников. Принципы определения координат источников радиоизлучений и анализа сигналов.

Способы и средства подслушивания акустических сигналов. Параметры слуховой системы человека. Структура и характеристики технических средств подслушивания. Классификация и характеристики микрофонов. Виды и принципы работы остронаправленных микрофонов. Стетоскопы. Принципы работы и характеристики диктофонов для скрытной записи. Классификация и характеристики закладных устройств. Варианты камуфлирования закладных устройств. Способы и средства лазерного подслушивания и ВЧ-навязывания.

Способы и средства добывания информации о демаскирующих признаках веществ. Способы и возможности определения демаскирующих признаков веществ. Принципы дистанционного анализа веществ. Виды и показатели радиоактивных излучений. Структура и принципы работы средств радиационной разведки.

1.10. Классификация и структура технических каналов утечки информации

Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

Оптические каналы утечки информации. Структура оптического канала утечки информации. Условия освещенности объектов наблюдения в видимом и ИК-диапазонах в различные периоды времени. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации. Варианты оптических каналов утечки информации для типовых контролируемых зон организации.

Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации. Направляющие линии связи, их характеристики. Классификация радиоволн. Особенности распространения радиоволн различных диапазонов частот. Способы повышения дальности передачи информации в ультракоротком диапазоне радиоволн. Ослабления радиоволн при распространении через различные среды. Классификация и характеристики помех в радиоэлектронных каналах утечки информации.

Акустические каналы утечки информации. Структура акустического канала утечки информации. Отражение и поглощение акустических волн в среде распространения. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации.

Материально-вещественные каналы утечки информации. Структура материально-вещественного канала утечки информации и характеристики ее элементов. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде. Особенности утечки информации о радиоактивных веществах. Принципы физического и химического анализа веществ.

1.11. Концепция инженерно-технической защиты информации

Цели и задачи инженерно-технической защиты информации. Принципы инженерно-технической защиты информации. Уровни безопасности информации. Методы защиты информации. Сущность инженерной защиты и технической охраны источников информации. Понятие об информационном портрете объекта защиты. Способы изменения информационного портрета при маскировке и дезинформировании. Зависимость качества информации от соотношения мощностей носителя информации и помехи. Сущность энергетического скрытия. Показатели эффективности инженерно-технической защиты информации.

Раздел 2. Способы и средства инженерно-технической защиты

2.1. Способы и средства инженерной защиты и технической охраны

Роль и место технических средств в организации режима охраны. Современная концепция защиты объектов. Категорирование объектов охраны. Демаскирующие признаки злоумышленника и стихийных сил (пожара, воды). Модели злоумышленников. Уровни физической безопасности объектов охраны. Типовая структура системы охраны режимных помещений. Системы автономной и централизованной охраны. Основные показатели системы охраны. Показатели эффективности инженерно-технической охраны объектов.

Способы и средства инженерной защиты объектов. Типовые инженерные конструкции. Естественные и искусственные преграды. Двери и ворота. Виды замков. Способы и средства защиты окон. Виды стекол, используемых для укрепления окон. Контрольно-пропускные пункты пропуска людей и автотранспорта. Способы и средства идентификации людей. Металлические шкафы, сейфы и хранилища. Показатели стойкости сейфов и хранилищ.

Способы и средства обнаружения злоумышленников и пожара. Структура комплекса технических средств охраны. Классификация датчиков (извещателей). Принципы работы и основные характеристики контактных извещателей. Акустические извещатели. Оптико-электронные извещатели. Микроволновые (радиоволновые) извещатели. Вибрационные извещатели. Емкостные извещатели. Тепловые и ионизационные извещатели. Комбинированные извещатели. Помехи работе извещателей. Рекомендации по установке извещателей. Приемно-контрольные приборы, их назначение, классификация и основные характеристики. Пульты централизованного наблюдения. Системы сбора и обработки тревожной информации.

Способы и средства визуального наблюдения. Структура системы видеоконтроля. Телевизионные камеры, их классификация, принципы работы и основные характеристики. Мониторы, коммутаторы, квадраторы, мультиплексоры, видеомагнитофоны. Детекторы движения. Способы повышения времени видеозаписи. Дежурное освещение. Виды и основные характеристики источников света.

Способы и средства нейтрализации угроз. Виды способов и средств нейтрализации угроз. Подразделение охраны. Средства тревожной сигнализации. Средства пожаротушения, тенденция развития средств пожаротушения. Резервное и аварийное

электропитание. Основные характеристики источников резервного электропитания (батарей, аккумуляторов).

Средства управления системой охраны. Способы и средства передачи извещений. Автоматизированные интегрированные системы охраны объектов, их структура и тенденция развития. Типовой проект охраны объектов

2.2. Способы и средства защиты информации от наблюдения

Способы и средства противодействия наблюдению в оптическом диапазоне волн.

Виды маскировки и их сущность. Особенности маскировки в видимом и ИК-диапазонах света. Виды и принципы применения искусственных масок, аэрозолей и воздушной пены.

Способы и средства противодействия радиолокационному и гидроакустическому наблюдению. Способы информационного скрытия объектов от радиолокационного наблюдения. Средства дезинформирования и пассивного зашумления изображения на экране радиолокатора. Способы уменьшения эффективной площади рассеяния объекта наблюдения. Виды радиопоглощающих покрытий. Способы активного подавления сигналов радиолокаторов.

2.3. Способы и средства защиты информации от подслушивания

Способы и средства информационного скрытия акустических сигналов и речевой информации. Способы и средства информационного скрытия информации от подслушивания. Виды информационного скрытия речевой информации. Классификация способов технического закрытия. Сущность способов технического закрытия, их сравнительный анализ. Типы и параметры скремблеров. Принципы работы и параметры вокодеров.

Способы и средства энергетического скрытия акустических сигналов. Методы энергетического скрытия акустических сигналов: звукоизоляция и звукопоглощение. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы повышения звукоизоляции окон и дверей. Основные звукопоглощающие материалы и способы их применения. Типы и способы применения генераторов акустического и вибрационного зашумления. Способы оценки энергетических и информационных показателей безопасности речевой информации.

Способы и средства предотвращения утечки информации с помощью закладных устройств. Основные демаскирующие признаки проводных и радиозакладных устройств, качественная оценка их информативности. Классификация средств обнаружения, локализации и подавления закладных устройств. Принципы работы и основные характеристики обнаружителей электромагнитного поля, их достоинства и недостатки, способы применения. Возможности бытовых приемников и селективных вольтметров. Особенности специальных радиоприемников. Типы и параметры сканирующих приемников. Состав, принципы работы, возможности и параметры автоматизированных комплексов радиоконтроля помещений. Способы контроля телефонных линий и цепей электропитания. Способы подавления сигналов закладных устройств. Типы генераторов радиопомех. Средства подавления сигналов закладных устройств в телефонных линиях и цепях электропитания. Принципы работы нелинейных локаторов. Типы и характеристики отечественных и зарубежных локаторов. Физические принципы работы и способы применения обнаружителей пустот для выявления закладных устройств. Принципы работы и характеристики металлодетекторов. Виды рентгеновских установок. Типы, возможности и способы применения для выявления закладных устройств флюороскопов и рентгенотелевизионных установок. Виды "чисток" помещения. Способы и средства визуального осмотра помещения. Способы и средства контроля помещения перед совещаниями и в ходе их проведения. Виды проверки отдельных предметов. Варианты наборов средств для "чистки" помещений.

2.4. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки

Требования к средствам подавления сигналов побочных электромагнитных излучений и наводок. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных и электромагнитных полей. Экранирование проводов и кабелей. Материалы для экранирования. Требования к заземлению и конструкция заземлителей. Развязка и фильтрация цепей электропитания. Средства активного линейного и пространственного зашумления.

2.5. Способы предотвращения утечки информации по материально-вещественному каналу

Классификация способов предотвращения утечки информации по материально-вещественному каналу. Способы и средства уничтожения информации, содержащейся в отходах делопроизводства и промышленного производства. Способы и средства стирания информации на магнитных носителях. Способы защиты демаскирующих веществ.

Раздел 3. Основные направления инженерно-технической защиты на объекте информатизации

3.1. Общие положения по инженерно-технической защите информации в организации

Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации инженерно-технической защиты информации в организации, их сущность. Функции сотрудников службы безопасности, обеспечивающих инженерно-техническую защиту информации.

3.2. Организационные и технические меры по инженерно-технической защите информации в организации

Основные направления инженерно-технической защиты информации в организации. Сущность организационных и технических мер по защите информации в организации. Задачи и виды контроля эффективности защиты информации. Сущность технического контроля эффективности защиты информации.

3.3. Системный подход к инженерно-технической защите информации

Сущность системного подхода и системного анализа. Характеристики системы защиты информации. Сущность характеристик системы защиты информации. Частные и глобальные критерии эффективности системы защиты. Алгоритм проектирования системы. Основные этапы и алгоритм проектирования системы защиты информации техническими средствами или разработки предложений по ее модернизации. Понятие о моделировании как основном процессе системного анализа. Виды моделей и их возможности при исследовании проблем защиты информации.

3.4. Моделирование объекта защиты

Сущность и методические рекомендации по структурированию защищаемой информации. Выявление и описание источников информации. Формы представления моделей объектов информационной безопасности.

3.5. Моделирование угроз информации

Виды моделей угроз информации: путей физического проникновения злоумышленника к источнику и каналов утечки. Методические рекомендации по определению путей проникновения злоумышленника к источнику информации, формы моделей. Типовые индикаторы каналов утечки. Методические рекомендации по моделированию каналов утечки. Формы представления результатов моделирования. Рекомендации по оценке угроз безопасности информации.

3.6. Методические рекомендации по разработке мер защиты

Основные способы и средства защиты информации от типовых вариантов угроз. Рекомендации по оценке угроз безопасности информации и расходов на техническую защиту. Комплексирование мер защиты. Оптимизация проекта системы (предложений) защиты информации. Требования к оформлению проекта системы (предложений) при

представлении на согласование и утверждение. Тенденции развития методического обеспечения защиты информации.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	*2*	
2.1	Изучение способов и средств обнаружения злоумышленников и пожара. Изучение комплекса технических средств охраны	ПЗ/Решение практических задач
	Изучение способов и средств обнаружения злоумышленников и пожара. Изучение комплекса технических средств охраны	ЛР/Решение практических задач
2.2	Изучение способов и средств защиты информации от наблюдения	ПЗ/Решение практических задач
	Изучение способов и средств защиты информации от наблюдения	ЛР/Решение практических задач
2.3	Изучение способов и средств защиты информации от подслушивания.	ПЗ/Решение практических задач
	Изучение способов и средств защиты информации от по	ЛР/Решение практических задач
2.4	Изучение способов и средств предотвращения утечки информации через побочные электромагнитные излучения и наводки	ПЗ/Решение практических задач
	Изучение способов и средств предотвращения утечки информации через побочные электромагнитные излучения и наводки	ЛР/Решение практических задач/ Отчет. Индивидуальное задание 2
3.2	Изучение способов и средств уничтожения информации	ПЗ/Решение практических задач
	Изучение способов и средств уничтожения информации	ЛР/Решение практических задач/ Отчет. Индивидуальное задание 3
3.3	Основные этапы и алгоритм проектирования системы защиты информации техническими средствами или разработки предложений по ее модернизации	ПЗ/Решение практических задач
	Основные этапы и алгоритм проектирования системы защиты информации техническими средствами или разработки предложений по ее модернизации	ЛР/ешение практических задач
3.4	Моделирование объекта защиты	ПЗ/Решение практических задач
	Моделирование объекта защиты	ЛР/Решение практических задач
3.5	Моделирование угроз информации	ПЗ/Решение практических задач
	Моделирование угроз информации	ЛР/Решение практических задач/ Отчет. Индивидуальное задание 4

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*
8	Подготовка к выполнению и защите контрольной точки 1.
15	Подготовка к выполнению и защите контрольной точки 2.
18	Подготовка к выполнению и защите контрольной точки 3.
21	Подготовка к выполнению и защите контрольной точки 4.
1-22	Подготовка к экзамену

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины 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 2.1, 2.2, 2.3, 2.4, 3.2, 3.3, 3.4., 3.5.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по изучению пакетов прикладных программ, языков программирования, информационно-коммуникационных технологий (как правило, организационной формой таких занятий являются лабораторные работы).

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**
Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2021. - 256 с.	Основная		https://znanium.com/catalog/product/1178151
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с.	Основная	–	https://znanium.com/catalog/document?id=358722
Морозов С.К. Инженерно-техническая защита информации : лабораторный практикум : направление подготовки 10.03.01 «Информационная безопасность» : направленность «Безопасность компьютерных систем (в экономике и управлении)» / Минобрнауки России, Санкт-Петербургский государственный экономический университет, Кафедра вычислительных систем и программирования ; [сост.]: С.К. Морозов Санкт-Петербург : [б. и.], 2020	дополнительная		ЭБ OPAC.UNECON.RU
Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Электрон. дан. — Москва : ИНФРА-М, 2020. — 327 с.	дополнительная	–	ЭБС ZNANIUM
Жук А.П. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. — Электрон. дан. - М. : РИОР : ИНФРА-М, 2018. - 392 с.	дополнительная	–	ЭБС ZNANIUM

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.

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№ п/п	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)

Лабораторные работы по дисциплине проводятся в лаборатории «Инженерно-технической защиты, лаборатория Программно-аппаратной защиты».

Таблица 9.2.2 – Лаборатория «Инженерно-технической защиты, лаборатория Программно-аппаратной защиты»

Вид учебных занятий	**Адрес, № аудитории**	**Лабораторное оборудование**
1	*2*	*3*
Лабораторные работы	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р», Ауд. 2057	Лаборатория Инженерно-технической защиты, лаборатория Программно-аппаратной защиты. Специализированная мебель и оборудование: Учебная мебель на 30 посадочных мест (Парта двухместная – 11 шт., стол – 8 шт., стулья- 30 шт.); 2 рабочих места преподавателя (2 стола, 2 стула); стол – 1 шт.; трибуна для выступлений –

		1 шт.; шкаф для документов – 1 шт.; стенды настенные пробковые – 2 шт.; шкаф настенный со стеклянными створками – 4 шт.; доска для маркеров двухсторонняя – 1 шт.; персональный компьютер IBM PC-совместимый (i5-3470/RAM 8Gb/HDD 500Gb/Win7pro) – 7 шт.; персональный компьютер IBM PC-совместимый (i3-2100/RAM 8Gb/HDD 500Gb/Win7pro) – 8 шт.; коммутатор Cisco для организации локальной сети лаборатории с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации – 1 шт.; шкаф серверный 42U – 1 шт.; шкаф телекоммуникационный 20U – 1 шт.; проектор NEC ME-401X – 1 шт.; экран для проектора Screen Media Goldview 244*244MW настенный – 1шт.; акустическая система марка Microlab модель Pro2– 1 шт.; коммутатор консольный Trend Net TK-803R – 1 шт.; разветвитель видеосигнала Aten VS-92A – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЭ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЦТ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ФОЭ-НР» – 1 комплект; комплект плакатов НПП «Учтех-Профи» – 1 шт.; генератор акустического шума ЛГШ-301 АО «Лаборатория ППШ» – 1 шт.; виброгенератор ЛГШ-403 в комплекте с вибропреобразователями ЛВП-2о, ЛВП-2Т АО «Лаборатория ППШ» – 1 шт.; фильтр сетевой однофазный ЛФС-10-1Ф АО «Лаборатория ППШ» – 1 шт.; генератор шума по цепям электропит., заземл. и ПЭМИ ЛГШ-503 АО «Лаборатория ППШ» – 1 шт.; устройство защиты телефонных линий Гранит-8 абонентское АО «Лаборатория ППШ» – 1 шт.; сервер HP-DL – 5 шт.; Коммутатор Cisco Small Business SF302-08 – 4 шт.; Коммутатор Cisco 2950 – 3 шт.; Коммутатор Cisco 3560 – 1 шт.; Беспроводной маршрутизатор TP-Link TL -WR941 ND; Электронные ключи Guardant – 16 шт.; огнетушитель ОУ-5 – 1 шт.; огнетушитель ОП-4(3)-ВСЕ – 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).