ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины:

– изучение обучающимися особенностей применения технических каналов связи, предъявляемых к ним требования, технологии противодействия утечки по техническим каналам связи. В результате изучения дисциплины у обучающихся должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ защищенности технических каналов связи и защиты информации, обрабатываемой средствами вычислительной техники (СВТ) от несанкционированного использования технических каналов связи.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК – 13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

Задачи дисциплины:

- изучение новых образцов программных, технических средств защиты информации и информационных технологий;
- изучение тенденций развития методов и средств защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;
- получение знаний о технических каналах утечки информации и методах защиты информации от утечки.

2. Перечень планируемых результатов обучения дисциплины, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-13.1. Использует модели угроз и рисков информационной безопасности автоматизированных систем, методы оценки уязвимостей каналов передачи информации	**Знает** теоретические основы моделей угроз информационной безопасности автоматизированных систем и возможность их адаптации к возможным угрозам **Умеет** проводить оценку защищенности информации от утечки по техническим каналам; оформлять отчетные материалы по результатам контроля защищенности информации от утечки по техническим каналам
ОПК-13.2. Проводит тестирование информационной безопасности автоматизированных систем на основе оценки рисков реализации угроз безопасности	**Знает** способы перехвата информации в каналах утечки; методы защиты информации от утечки по техническим каналам; методы и методики контроля защищенности информации от утечки по техническим

	каналам **Умеет** применять средства контроля защищенности информации от утечки по техническим каналам
ОПК-13.3. Обладает навыками комплексного всестороннего анализа информационной безопасности автоматизированных информационных систем и их отдельных элементов	**Знает** правила эксплуатации проверки работоспособности средств защиты информации **Умеет** проверять работоспособность средств защиты информации утечки по техническим каналам, анализировать и оценивать технологический процесс обработки информации, с целью предотвращения ее утечки по техническим каналам

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части, образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация - **Анализ безопасности информационных систем**.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачётных единиц, 180 часов.

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			8
Общая трудоемкость дисциплины по учебному плану	**5**	**180**	**180**
Контактная работа		**74**	**74**
Лекции		30	30
Практические занятия		38	38
Лабораторные работы		4	4
Консультация		2	2
Самостоятельная работа		**70**	**70**
Экзамен		**36**	+

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов и тем	Всего часов	Количество часов по видам занятий						
		Лекции	Лаб. работы	Практические занятия	Практическая подготовка	Консультации	Контроль	Самостоятельная работа
8 семестр								
Раздел 1. Технические каналы утечки информации, обрабатываемой СВТ	28	6			8			14
Раздел 2. Технические каналы утечки акустической речевой информации	30	6		6	4			14
Раздел 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам	28	6	4	4				14
Раздел 4. Способы и средства защиты объектов информатизации от утечки информации, возникающей за счет наводок ПЭМИ	28	6		8				14
Раздел 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	28	6		8				14
Консультация	2					2		
Экзамен	36						36	
Итого за 8 семестр	**180**	**30**	**4**	**26**	**12**	**2**	**36**	**70**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Технические каналы утечки информации, обрабатываемой СВТ

Лекции. Классификация технических каналов утечки информации, обрабатываемой СВТ. Технические каналы утечки информации, возникающей за счет ПЭМИ СВТ. Технические каналы утечки информации, возникающей за счет наводок ПЭМИ СВТ.

Практическая подготовка. Исследование технических каналов утечки информации, возникающей за счет ПЭМИ СВТ.

Самостоятельная работа. Средства перехвата ПЭМИН СВТ. Специально создаваемые технические каналы утечки информации, обрабатываемой СВТ.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература: [1, 2, 3]

Раздел 2. Технические каналы утечки акустической речевой информации

Лекции. Классификация технических каналов утечки акустической речевой информации. Прямые акустические технические каналы утечки речевой акустической информации. Акустоэлектрические каналы утечки речевой информации.

Практические занятия.

Исследование технических утечки акустической речевой информации. Акустовибрационные каналы утечки речевой информации.

Практическая подготовка. Средства акустической (речевой) разведки: Электронные стетоскопы, радио стетоскопы. Акустооптический канал утечки речевой информации.

Самостоятельная работа. Акустоэлектромагнитные каналы утечки речевой информации

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература:: [1, 2, 3]

Раздел 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам

Лекции. Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Требования к заземлению ОТСС (СВТ).

Практические занятия. Системы пространственного электромагнитного зашумления.

Лабораторная работы. Способы защиты объектов информатизации от утечки информации по техническим каналам

Самостоятельная работа. Экранированные помещения. Заземление технических средств.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература:: [1, 2, 3]

Раздел 4. Способы и средства защиты объектов информатизации от утечки информации, возникающей за счет наводок ПЭМИ

Лекции. Помехоподавляющие фильтры. Системы линейного зашумления.

Практические занятия. Использование средств защиты от утечки информации, возникающей за счет наводок ПЭМИ.

Самостоятельная работа. Защищенные ПЭВМ.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература:: [1, 2, 3]

Раздел 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Лекции. Классификация способов и средств защиты речевой информации в выделенных помещениях. Звуко - и виброизоляция выделенных помещений. Системы и средства виброакустической маскировки.

Практические занятия. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.

Самостоятельная работа. Способы и средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература:: [1, 2, 3]

5. Методические рекомендации по организации изучения дисциплины

При реализации программы учебной дисциплины используется традиционная образовательная технология, основой которой является системный принцип построения разделов и тем, используются лекционные и практические занятия.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– дать систематизированные научные знания по дисциплине, акцентировав внимание на наиболее сложных вопросах;

стимулировать активную познавательную деятельность обучающихся, способствовать формированию их творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цель практического занятия: углубить и закрепить знания, полученные на лекции, формирование навыков использования знаний для решения практических задач; выполнение тестовых заданий по проверке полученных знаний и умений.

Целью лабораторного занятия является усвоение теоретических основ дисциплины и получение практических навыков исследования путем постановки, проведения, обработки и представления результатов эксперимента на основе практического использования различных методов (наблюдения, измерения, сравнения и др.), приобретения навыков опыта творческой деятельности. В

заключительной части лабораторного занятия обучающиеся оформляют результаты экспериментов в форме отчета.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме типовых контрольных заданий.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов освоения дисциплины, проводится в форме экзамена.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Примерный перечень вопросов для тестов

1. Основные технические средства и системы – это 1) Технические средства и системы, непосредственно участвующие в обработке информации ограниченного доступа. 2) Технические средства и системы обработки открытой информации. 3) Технические средства и системы обработки информации. 4) Средства вычислительной техники и автоматизированные системы обработки информации. 5) Технические средства и системы, установленные на объекте информатизации

2. Вспомогательные технические средства и системы – это 1) Технические средства и системы, участвующие в обработке информации ограниченного доступа. 2) Технические средства и системы обработки открытой информации. 3) Технические средства и системы обработки информации. 4) Технические средства и системы, установленные на объекте информатизации. 5) Технические средства и системы, установленные на объектах информатизации или в выделенных (защищаемых) помещениях, непосредственно не участвующие в обработке (приеме, передачи, записи, хранения и и т.д.) информации ограниченного доступа

3. Применительно к области информационной безопасности информация – это 1) Сведения (сообщения, данные) независимо от формы их представления. 2) Факты, данные, характеризующие кого-л., что-л. 3) Отчет с цифровыми данными. 4) Сведения, предназначенные для передачи по каналу связи. 5) Сведения, представленные в форме, пригодной для постоянного хранения, передачи и (автоматизированной) обработки.

4. Контролируемая зона – это 1) Охраняемая территория. 2) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц. В) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц или транспортных средств. 3) Пространство (территория, здание, часть здания), в котором исключено пребывание лиц, не имеющих постоянного или разового допуска. 4) Пространство (территория, здание, часть здания), в котором исключено пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

5. Утечка информации – это 1) Неконтролируемое распространение защищаемой информации в результате ее разглашения. 2) Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней или получения защищаемой информации иностранными разведками и другими заинтересованными субъектами. 3) Неконтролируемое распространение защищаемой информации в результате несанкционированного доступа к ней. 4) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками и другими заинтересованными субъектами. 5) Неправомерное разглашение или распространение сведений ограниченного доступа.

6. Неправомерный доступ к информации может быть осуществлен путем: 1) Перехвата информации с использованием технических средств. 2) Хищения носителя информации. 3) Несанкционированного доступа к информации. 4) Передачи носителя информации, содержащего сведения ограниченного доступа, постороннему лицу. 5) Передачи информации ограниченного доступа по незащищенным каналам связи.

7. К специально создаваемым техническим каналам утечки информации (ТКУИ), обрабатываемой техническими средствами (ТСПИ), относятся: 1) Электромагнитные технические каналы утечки информации. 2) Электрические технические каналы утечки информации. 3) Акустоэлектромагнитные технические каналы утечки информации. 4) Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ТСПИ. 5) Технические каналы утечки информации, создаваемые путем внедрения в ТСПИ электронных устройств перехвата информации (закладных устройств).

8. Техническая защита информации – 1) Защита информации с помощью ее криптографического преобразования. 2) Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. 3) Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. 4) Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых

документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. 5) Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации путем проведения организационных мероприятий и применения технических, программных и программно-аппаратных средств.

9. Случайной антенной являются: 1) Вспомогательные технические средства и системы (ВТСС), соединительные линии которых выходят за пределы контролируемой зоны. 2) Вспомогательные технические средства и системы (ВТСС), соединительные линии которых не выходят за пределы контролируемой зоны. 3) Соединительные линии ВТСС, посторонние проводники, линии электропитания и цепи заземления, выходящие за пределы контролируемой зоны. 4) Соединительные линии ВТСС и посторонние проводники, не выходящие за пределы контролируемой зоны. 5) Цепи заземления, не выходящие за пределы контролируемой зоны.

10. Зона r1 – это 1) Пространство вокруг ТСПИ, на границе и за пределами которого уровень наведенного от ТСПИ информативного сигнала в сосредоточенных антеннах, имеющих выход за пределы контролируемой зоны объекта, не превышает нормированного значения. 2) Пространство вокруг ТСПИ, на границе и за пределами которого напряженность электрической или магнитной составляющей электромагнитного поля информативного сигнала не превышает допустимого (нормированного) значения. 3) Пространство вокруг ТСПИ, на границе и за пределами которого уровень наведенного от ТСПИ информативного сигнала в распределенных антеннах, имеющих выход за пределы контролируемой зоны объекта, не превышает нормированного значения. 4) Пространство вокруг ТСПИ, в пределах которого уровень наведенного от ТСПИ информативного сигнала в сосредоточенных антеннах, имеющих выход за пределы контролируемой зоны объекта, превышает нормированное значение. 5) Минимальное расстояние от ТСПИ до случайной антенны.

11. Основными причинами возникновения электрических каналов утечки информации являются: 1) Наводки информативных сигналов в электрических цепях ТСПИ, вызванные информативными побочными и (или) паразитными электромагнитными излучениями (ПЭМИ) ТСПИ. 2) Наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными побочными и (или) паразитными электромагнитными излучениями (ПЭМИ) ТСПИ. 3) Наводки информативных сигналов в электрических цепях ТСПИ, вызванные внутренними емкостными и (или) индуктивными связями («просачивание» информативных сигналов в цели электропитания через блоки питания ТСПИ). 4) Наводки информативных сигналов в цепях заземления, вызванные информативными ПЭМИ ТСПИ, а также гальванической связью схемной (рабочей) земли и блоков ТСПИ. Д) Наличие акустоэлектрических преобразователей в элементах ВТСС.

12. Основными причинами возникновения электромагнитных каналов утечки информации являются: 1) Побочные электромагнитные излучения (ПЭМИ), возникающие вследствие протекания переменного электрического тока (информативных сигналов) по элементам ТСПИ. 2) Наводки информативных сигналов, вызванных побочными и (или) паразитными электромагнитными излучениями ТСПИ. 3) Модуляция информативным сигналом ПЭМИ высокочастотных генераторов ТСПИ (на частотах работы высокочастотных генераторов). 4) Модуляция информативным сигналом паразитного электромагнитного излучения ТСПИ (например возникающего вследствие самовозбуждения усилителей низкой частоты). 5) Модуляция акустическим сигналом побочных электромагнитных излучений высокочастотных генераторов ВТСС (на частотах работы высокочастотных генераторов ВТСС).

13. Зона R2– это 1) Пространство вокруг ТСПИ, на границе и за пределами которого уровень наведенного от ТСПИ информативного сигнала в сосредоточенных антеннах, имеющих выход за пределы контролируемой зоны объекта, не превышает нормированного значения. 2) Пространство вокруг ТСПИ, на границе и за пределами которого напряженность электрической или магнитной составляющей электромагнитного поля информативного сигнала не превышает допустимого (нормированного) значения. 3) Пространство вокруг ТСПИ, в пределах которого напряженность электрической или магнитной составляющей электромагнитного поля информативного сигнала превышает допустимое (нормированное) значение. 4) Пространство вокруг ТСПИ, на границе и за пределами которого напряженность электрической или магнитной составляющей электромагнитного поля информативного сигнала превышает допустимое (нормированное) значение. 5) Минимальное расстояние от ТСПИ до границы контролируемой зоны объекта.

14. Выделенное (защищаемое) помещение – это 1) Помещение, предназначенное для установки технических средств обработки информации. 2) Помещение, предназначенное для установки вспомогательных технических средств и систем. 3) Служебный кабинет, актовый зал, конференц-зал. 4) Специальное помещение (служебный кабинет, актовый, конференц-зал и т.д.), предназначенное для регулярного проведения совещаний, обсуждений, конференций, переговоров, бесед и других мероприятий секретного (конфиденциального) характера. 5) Помещение, в котором размещены средства вычислительной техники и автоматизированные системы обработки информации.

15. Основные задачи защиты информации от утечки по техническим каналам 1) Предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических обработки информации. 2) Предотвращение утечки речевой информации по техническим каналам из выделенных (защищаемых) помещений. 3) Выявление электронных устройств перехвата информации, внедренных в технические средства и выделенные (защищаемые) помещения. 4) Исключение несанкционированного доступа к

обрабатываемой или хранящейся в технических средствах информации. 5) Предотвращение хищения носителей информации и несанкционированного снятия копий с носителей информации.

16. К естественным техническим каналам утечки информации (ТКУИ), обрабатываемой техническими средствами (ТСПИ), относятся: 1) Электромагнитные технические каналы утечки информации. 2) Электрические технические каналы утечки информации. 3) Акустоэлектромагнитные технические каналы утечки информации. 4) Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ТСПИ. 5) Технические каналы утечки информации, создаваемые путем внедрения в ТСПИ электронных устройств перехвата информации (закладных устройств)

17. Защищаемый объект информатизации – это 1) Совокупность информационных ресурсов, содержащих сведения ограниченного доступа, и технических средств, и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией. 2) Совокупность информационных ресурсов, содержащих сведения ограниченного доступа, технических средств и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией, и технических средств обеспечения объекта информатизации. 3) Совокупность информационных ресурсов, содержащих сведения ограниченного доступа, технических средств и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией, технических средств обеспечения объекта информатизации (вспомогательных технических средств и систем), а также помещений или объектов (зданий, сооружений, технических средств), в которых они установлены. 4) Совокупность технических средств и систем обработки информации ограниченного доступа, технических средств обеспечения объекта информатизации, а также помещений или объектов (зданий, сооружений, технических средств), в которых они установлены. 5) Д) Совокупность технических средств и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией, и технических средств обеспечения объекта информатизации.

6.1.2. Промежуточной аттестации

Примерный перечень вопросов, выносимых на экзамен

1) Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации.
2) Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.
3) Основные организационные и технические меры по защите информации.
4) Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.
5) Способы оценки безопасности речевой информации в помещении.
6) Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения.
7) Требования по защите информации от утечки по техническим каналам. Виды технического контроля.
8) Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля.
9) Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.
10) Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.
11) Принципы защиты информации техническими средствами.
12) Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
13) Распространение оптических сигналов в атмосфере и в светопроводах.
14) Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.
15) Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.
16) Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение
17) Комплекс технических средств охраны
18) Инженерные конструкции. Автономные и централизованные системы охраны
19) Энергетическое скрытие радио и электрических сигналов
20) Классификация способов и средств защиты речевой информации в выделенных помещениях

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
Экзамен	правильность и полнота ответа	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа	Отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя	Хорошо
		дан недостаточно правильный и полный ответ, логика и последовательность изложения имеют нарушения, в ответе отсутствуют выводы	Удовлетворительно
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствуют фрагментарность, нелогичность изложения, дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос	Неудовлетворительно

7. Ресурсное обеспечение дисциплины.

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Лицензия №217800111-ore-2.12-client-6196

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Common Edition релиз Орел

Срок действия: бессрочно

2. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14545

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Special Edition

Срок действия: бессрочно

3. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14544

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования Astra Linux Special Edition

Срок действия: бессрочно

4. ПО «Р7-Офис. Профессиональный»

Выдана: «ФГБОУ ВО Санкт-Петербургский университет МЧС России»

Срок действия: бессрочно

7.2. Профессиональные базы данных и информационные справочные системы

1. Сервер органов государственной власти Российской Федерации http://россия.рф/ (свободный доступ);
2. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ);
3. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ);
4. Система официального опубликования правовых актов в электронном виде http://publication.pravo.gov.ru (свободный доступ);
5. Федеральный портал «Совершенствование государственного управления» https://ar.gov.ru (свободный доступ);
6. Электронная библиотека университета http://elib.igps.ru (авторизованный доступ);
7. Электронно-библиотечная система «ЭБС IPR BOOKS» http://www.iprbookshop.ru (авторизованный доступ).
8. Электроно-библиотечная система "Лань" https://e.lanbook.com (авторизованный доступ).

7.3. Литература

Основная литература:

1. Киренберг А.Г. Защита информации от утечки по техническим каналам: учебное пособие / А.Г. Киренберг, В.О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. — 221 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/135100.html .

2. Голиков А.М. Защита информации от утечки по техническим каналам: учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. — 256 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/72090.html.

Дополнительная литература:

1. Газизов А.Р. Техническая защита информации : учебное пособие / А.Р. Газизов, Д.В. Фатхи. — Ростов-на-Дону : Донской государственный

технический университет, 2022. — 108 с. — ISBN 978-5-7890-2053-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/130429.html.

2. Скрипник Д.А. Общие вопросы технической защиты информации : учебное пособие / Д.А. Скрипник. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 424 с. — ISBN 978-5-4497-2415-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/133955.html.

3. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А.А. Евстифеев, В.И. Ерошев, А.П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 с. — ISBN 978-5-9515-0426-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/101929.html.

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Лабораторное занятие на 4 курсе обучения (8 семестр) проводится в лаборатории технической защиты информации.

Помещения для практических занятий и самостоятельной работы обучающихся оснащены компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: доктор технических наук, профессор Буйневич Михаил Викторович.