Аннотация к рабочей программе дисциплины «Защита информации от утечки по техническим каналам»

Цель преподавания дисциплины

Целью преподавания дисциплины "Защита информации от утечки по техническим каналам" является ознакомление студентов с основными способами, методами, принципами работы технических средств защиты информации, передаваемой по техническим каналам от технических средств обнаружения.

Задачи изучения дисциплины

- изучение основных способов защиты информации от утечки по техническим каналам, а также основных принципов, используемых при организации и проведении мероприятий по защите информации на объектах защиты;

- изучение основных методов защиты информации от утечки по техническим каналам;

- изучение методов и способов оценки угроз информационной безопасности объектов информатизации;

- изучение основных требований и рекомендаций по защите информации от утечки по техническим каналам;

- изучение основных юридических законов в области защиты информации от утечки по техническим каналам;

- овладение навыками по разработке и проектированию систем защиты помещений на объектах с повышенными требованиями.

- изучение принципов работы и основных технических характеристик средств защиты информации от утечки по техническим каналам;

- изучение принципов работы и основных технических характеристик средств контроля эффективности защиты информации;

- изучение эксплуатационной документации и овладение навыками применения средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

- анализ показателей качества и критериев оценки систем и отдельных методов и средств защиты информации;

- изучение методов и способов оценки информационных рисков в автоматизированных системах.

Компетенции, формируемые в результате освоения дисциплины

Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности (ОПК-9);

Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений (ОПК-12).

Разделы дисциплины

Технические средства разведки. Общие сведения. Радиоэлектронная разведка. Оптическая разведка. Акустическая разведка. Компьютерная разведка. Средства технической разведки. Противодействие техническим разведкам. Радиоэлектронное противодействие и радиомаскировка. Противодействие акустической разведке. Противодействие видовой разведке. Защита от внедряемых на объекты разведывательных устройств. Технические средства защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«_31_» ___августа___ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам
(наименование дисциплины)

ОПОП ВО 10.03.01Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
наименование направленности (профиля, специализации)

форма обучения _____очная_____
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Защита информации от утечки по техническим каналам составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 10.03.01Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета (протокол №6 «26» 02 2021 г.).

Рабочая программа дисциплины Защита информации от утечки по техническим каналам обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, на заседании кафедры информационной безопасности Протокол № 1 «30» 08 2021г.

Зав. кафедрой Таныгин М.О.
Разработчик программы
к.воен.н., доцент Ханис А.Л.
Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Защита информации от утечки по техническим каналам пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета Протокол № «6» 26.02 2021г., на заседании кафедры ИБ Протокол №11 от 30.06.2022 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа дисциплины Защита информации от утечки по техническим каналам пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета Протокол № « » _____ 20 г., на заседании кафедры_____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Защита информации от утечки по техническим каналам» является ознакомление студентов с основными способами, методами, принципами работы технических средств защиты информации передаваемой по техническим каналам от технических средств обнаружения.

1.2 Задачи дисциплины

- изучение основных способов защиты информации от утечки по техническим каналам, а также основных принципов, используемых при организации и проведении мероприятий по защите информации на объектах защиты;
- изучение основных методов защиты информации от утечки по техническим каналам;
- изучение методов и способов оценки угроз информационной безопасности объектов информатизации;
- изучение основных требований и рекомендаций по защите информации от утечки по техническим каналам;
- изучение основных юридических законов в области защиты информации от утечки по техническим каналам;
- овладение навыками по разработке и проектированию систем защиты помещений на объектах с повышенными требованиями.
- изучение принципов работы и основных технических характеристик средств защиты информации от утечки по техническим каналам;
- изучение принципов работы и основных технических характеристиксредств контроля эффективности защиты информации;
- изучение эксплуатационной документации и овладение навыками применения средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- анализ показателей качества и критериев оценки систем и отдельных методов и средств защиты информации;
- изучение методов и способов оценки информационных рисков в автоматизированных системах.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	ОПК-9.3 Организует защиту информации от утечки по техническим каналам на объектах информатизации.	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения радиоволн, принципы и способы организации системы защиты информации на объектах информатизации. Порядок и алгоритм проведения организационных мероприятий на объектах информатизации. Функциональные обязанности по организации мероприятий по защите информации. ***Уметь:*** Выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Разрабатывать нормативную документацию по выполнению требований защиты информации на объектах информатизации. Осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации объектов информатизации. Осуществлять

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками применения технических средств защиты информации, разработки нормативных и технических документов по организации защиты объекта информатизации, проведения организационных мероприятий по вскрытию уязвимых мест систем обеспечения защиты информации объекта информатизации.
		ОПК-9.4 Оценивает угрозы информационной безопасности объек-та информатизации.	***Знать:*** этапы построения системы информационной безопасности на объекте информатизации, условия и факторы, приводящие к нарушению целостности, доступности и конфиденциальности информации, классификацию угроз, основные направления защиты информации на объекте, последствия и виды несанкционированных действий с информацией, классификацию нарушителей, методы и способы оценки ущерба от различных рисков потери информации, анализа уровня информационной безопасности объекта, оценки состояния степени защищённости информации, методы и методики оценки рисков информационной безопасности при использовании программных средств и информационных систем управления, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Уметь: применять известные методики оценки угроз, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать угрозы, применять типовые методики для получения характеристик рисков и угроз, использовать основные модели оценки рисков для получения количественных и качественных оценок рисков, использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками. ***Владеть:*** навыками анализа защищенности объекта информатизации, методами проведения анализа угроз информационной безопасности; навыками разделения рисков на приемлемые и неприемлемые, навыками оценки рисков информационной безопасности, навыками оценки рисков информационной безопасности, навыками оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками.
		ОПК-9.5 Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.	***Знать:*** классификацию, принципы, способы и порядок функционирования средств защиты информации, принципы организации проверок технических СЗИ, инструментальные средства проведения проверок технических СЗИ, основные угрозы, предотвращаемые, СЗИ; виды, методы и средства контроля защиты информации, нормативные документы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			регламентирующие порядок проведения контроля защиты информации, комплекс мероприятий, проводимых в ходе контроля эффективности защиты информации. ***Уметь:*** применять средства защиты информации и средства контроля защиты информации в соответствии с эксплуатационной документацией, анализировать нормативную документацию, регламентирующую порядок проведения контроля защиты информации, организовать комплекс мероприятий контроля эффективности защиты информации, в соответствии регламентирующими документами. ***Владеть:*** навыками организации контрольных проверок технических СЗИ, эксплуатации средств защиты информации и средств контроля защиты информации в соответствии с эксплуатационной документацией, требованиями нормативной документации, регламентирующей порядок проведения контроля защиты информации, комплексом мероприятий контроля эффективности защиты информации.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.	ОПК-12.2 Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им. ***Уметь:*** правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
		ОПК-12.3 Оценивает информационные риски в автоматизированных системах.	***Знать:*** классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования объекта информатизации; основные компоненты автоматизированных систем объекта информатизации, состав, структуры и принципы функционирования современных автоматизированных систем, требования основных законов и нормативных документов в области безопасности автоматизированных систем; методы, способы и методики анализа рисков безопасности автоматизированных систем; классификацию основных источников угроз, комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности автоматизированных систем; основные принципы построения комплексной системы защиты автоматизированных систем. ***Уметь:*** определять угрозы безопасности автоматизированных систем, определять возможные риски нарушения безопасности

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			функционирования объекта информатизации; определять состав, структуру и принципы функционирования современных автоматизированных систем, анализировать требования основных законов и нормативных документов в области безопасности автоматизированных систем; применять методики анализа рисков безопасности автоматизированных систем; определять основные источники угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности автоматизированных систем. ***Владеть:*** навыками анализа защищенности автоматизированных систем; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности автоматизированных систем, выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности автоматизированных систем; методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведения и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты автоматизированных систем объекта информатизации.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам», входит в обязательную часть блока 1 «Дисциплины (модули») основной профессиональной образовательной программы – программы бакалавриата 10.03.01Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий». Дисциплина изучается на 3 курсе в 6 семестре.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 6 зачетных единиц (з.е.), 216академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	64
в том числе:	
лекции	32
лабораторные занятия	32
практические занятия	0
Самостоятельная работа обучающихся (всего)	123,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
1	2	3
1	Технические средства разведки. Общие сведения.	Демаскирующие признаки и каналы утечки информации. Виды технических разведок. Классификация технических разведок по видам носителей аппаратуры разведки. Классификация технических разведок по способу добывания информации и типу аппаратуры разведки.
2	Радиоэлектронная разведка.	Общие сведения о радиоэлектронной разведке. Выбор стратегий разведки и маскировки. Схема конфликтного взаимодействия средств разведки и маскировки. Сложная сигнальная обстановка. Радио и радиотехническая разведки. Способы определения частоты сигналов РЭС. Пеленгация радиоэлектронных средств. Принцип работы доплеровского пеленгатора. Радиолокационная разведка. Радиотепловая разведка. Разведка побочных электромагнитных излучений и наводок.
3	Оптическая разведка.	Общие сведения об оптической разведке. Визуально-оптическая разведка. Фотографическая и фототелевизионная разведки. Тепловидение. Оптическая (лазерная) локация: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.
4	Акустическая разведка.	Инструментарий акустической разведки. Обработка речевых сигналов. Акустические закладные устройства.
5	Компьютерная разведка.	Методы взлома компьютерных систем. Программы шпионы. Парольные взломщики. Криптоаналитические атаки.
6	Средства технической разведки.	Средства космической разведки. Средства воздушной разведки. Средства морской разведки. Автоматические устройства технической разведки кабельных линий связи. Портативная техника для развед-служб
7	Противодействие техническим разведкам.	Общие сведения о противодействии техническим разведкам. Меры противодействия. Пути противодействия распознаванию типа объекта.
8	Радиоэлектронное противодействие и радиомаскировка.	Радиомаскировка. Экранирование. Фильтрация сигналов. Требования к заземлению технических средств. Специальные помещения. Специальные кабельные системы. Маскировка от средств РЛР. Активная радиомаскировка. Активное подавление РЛС.

9	Противодействие акустической разведке.	Характеристики октавных полос частотного диапазона речи. Пассивные методы акустической защиты. Звукоизоляция. Оценка звукоизоляции объекта. Активные методы акустической защиты.
10	Противодействие видовой разведке.	Защита от видовой РЛР. Защита от оптической и оптико-электронной разведок.
11	Защита от внедряемых на объекты разведывательных устройств.	Оценка степени угрозы объекту от возможного агентурного проникновения на охраняемую территорию Контроль радио-эфира. Проверка на наличие металл**а.** Рентгеноскопия. Поисковые приборы. Краткие сравнительные характеристики.
12	Технические средства защиты информации.	Электромагнитные материалы, используемые для экранирования, и их характеристики. Помехоподавляющие фильтры. Поисковая техника Линейные помехоподавляющие фильтры.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Технические средства разведки. Общие сведения.	2	-	-	У-1, У-2, У-3-У-10	УО - 2	ОПК-9, ОПК-12
2	Радиоэлектронная разведка.	2	-	-	У-1, У-2, У-3-У-10	УО - 3	ОПК-9
3	Оптическая разведка.	2	1	-	У-1, У-2, У-3-У-10 МУ-1, 3	УО -4, ЗЛР - 4	ОПК-9
4	Акустическая разведка.	2	-	-	У-1, У-2, У-3-У-10	УО – 5	ОПК-9
5	Компьютерная разведка.	2	-	-	У-1, У-2, У-3-У-10	УО -6	ОПК-9
6	Средства технической разведки.	2	-	-	У-1, У-2, У-3-У-10	УО -7	ОПК-9

7	Противодействие техническим разведкам.	2	-	-	У-1, У-2, У-3-У-10	УО - 8	ОПК-9, ОПК-12
8	Радиоэлектронное противодействие и радиомаскировка.	2	2,3	-	У-1, У-2, У-3-У-10 МУ-2,3	УО – 10 ЗЛР – 10,12	ОПК-9, ОПК-12
9	Противодействие акустической разведке.	4	-	-	У-1, У-2, У-3-У-10	УО - 12	ОПК-9, ОПК-12
10	Противодействие видовой разведке.	4	-	-	У-1, У-2, У-3-У-10	УО - 14	ОПК-9, ОПК-12
11	Защита от внедряемых на объекты разведывательных устройств.	4	4,5	-	У-1, У-2, У-3-У-10 МУ-4	УО – 16 ЗЛР – 14,16	ОПК-9, ОПК-12
12	Технические средства защиты информации.	4	6,7	-	У-1, У-2, У-3-У-10 МУ-5,6	УО – 18 ЗЛР – 16,18	ОПК-9, ОПК-12
	Всего	32					

УО – устный опрос, ЗЛР – лабораторная работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№п/п	Наименование лабораторной работы	Объем, час.
1	Анализ технических средств перехвата информации в оптическом диапазоне	4
2	Анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах	4
3	Анализ технических средств перехвата информации в акустическом диапазоне	4
4	Анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники	4
5	Анализ технических средств перехвата информации в материально-вещественном канале утечки	4
6	Моделирование объекта защиты	6
7	Моделирование технических каналов утечки информации	6
Итого		32

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Технические средства разведки. Общие сведения.	2 неделя	10
2	Радиоэлектронная разведка.	3 неделя	10
3	Оптическая разведка.	4 неделя	10
4	Акустическая разведка.	5 неделя	10
5	Компьютерная разведка.	6 неделя	10,85
6	Средства технической разведки.	7 неделя	10
7	Противодействие техническим разведкам.	8 неделя	11
8	Радиоэлектронное противодействие и радиомаскировка.	10 неделя	10
9	Противодействие акустической разведке.	12 неделя	10
10	Противодействие видовой разведке.	14 неделя	11
11	Защита от внедряемых на объекты разведывательных устройств.	16 неделя	11
12	Технические средства защиты информации.	18 неделя	10
Итого			123,85

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно- методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к экзамену;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 - Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
5	Лабораторная работа№6	Анализ конкретных ситуаций	3
6	Лабораторная работа№7	Анализ конкретных ситуаций	3
Итого			6

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на

формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю, специализации) программы бакалавриата.

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, представителями работодателей (командная работа, разбор конкретных ситуаций, и др.)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	Основы информационной безопасности.	Защита информации от утечки по техническим каналам. Методы и средства криптографической защиты информации. Сети и системы передачи информации. Безопасность сетей ЭВМ. Учебно-лабораторная практика.	Методы и средства криптографической защиты информации. Сети и системы передачи информации.
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.	Защита информации от утечки по техническим каналам. Экономическое обоснование проектных решений. Основы управления информационной безопасностью. Производственная эксплуатационная практика.		Программно-аппаратные средства защиты информации. Основы управления информационной безопасностью.

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ОПК-9, основной	ОПК-9.3 Организует защиту информации от утечки по техническим каналам на объектах информатизации.	Знать: виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам. Уметь: выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Владеть: навыками разработки нормативных и технических документов по организации защиты объекта информатизации.	Знать: основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения радиоволн, принципы и способы организации системы защиты информации на объектах информатизации. Уметь: разрабатывать нормативную документацию по выполнению требований защиты информации на объектах информатизации. Владеть: навыками применения технических средств	Знать: порядок и алгоритм проведения организационных мероприятий на объектах информатизации. Функциональные обязанности по организации мероприятий по защите информации. Уметь: осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации объектов информатизации. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. Владеть:

			защиты информации.	навыками проведения организационных мероприятий по вскрытию уязвимых мест систем обеспечения защиты информации объекта информатизации.
	ОПК-9.4 Оценивает угрозы информационной безопасности объекта информатизации.	Знать: этапы построения системы информационной безопасности на объекте информатизации, условия и факторы, приводящие к нарушению целостности, доступности и конфиденциальности информации. Уметь: применять известные методики оценки угроз, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать угрозы. Владеть: навыками анализа защищенности объекта информатизации, методами проведения анализа угроз информационной безопасности.	Знать: классификацию угроз, основные направления защиты информации на объекте, последствия и виды несанкционированных действий с информацией, классификацию нарушителей, методы и способы оценки ущерба от различных рисков потери информации, анализа уровня информационной безопасности объекта, оценки состояния степени защищённости информации. Уметь: применять типовые методики для получения характеристик рисков и угроз.	Знать: методы и методики оценки рисков информационной безопасности при использовании программных средств и информационных систем управления, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз. Уметь: использовать основные модели оценки рисков для получения количественных и качественных оценок рисков, использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками.
			Владеть: навыками разделения рисков на приемлемые и неприемлемые, навыками оценки рисков информационной безопасности.	Владеть: навыками оценки рисков информационной безопасности, навыками оценки рисков информационной безопасности и проектирования систем управления корпо-

				ративными рисками.
	ОПК-9.5 Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.	Знать: классификацию, принципы, способы и порядок функционирования средств защиты информации, принципы организации проверок технических СЗИ, инструментальные средства проведения проверок технических СЗИ. Уметь: анализировать нормативную документацию, регламентирующую порядок проведения контроля защиты информации. Владеть: навыками организации контрольных проверок технических СЗИ, эксплуатациисредств защиты информации и средств контроля защиты информации в соответствии с эксплуатационной документацией.	Знать: основные угрозы, предотвращаемые, СЗИ; виды, методы и средства контроля защиты информации. Уметь: организовать комплекс мероприятий контроля эффективности защиты информации, в соответствии регламентирующими документами. Владеть: требованиями нормативной документации, регламентирующей порядок проведения контроля защиты информации.	Знать: нормативные документы регламентирующие порядок проведения контроля защиты информации, комплекс мероприятий, проводимых в ходе контроля эффективности защиты информации.Уметь: применятьсредства защиты информации и средства контроля защиты информации в соответствии с эксплуатационной документацией. Владеть: навыками применения комплекса мероприятий контроля эффективности защиты информации.
ОПК-12, основной	ОПК-12.2 Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.	Знать: виды угроз и возможные каналы утечки конфиденциальной информации. Уметь: эксплуатировать антивирусные программные комплексы. Владеть: навыками применения программных средств защиты ин-	Знать: основные принципы построения политики информационной безопасности. Уметь: снижать вероятность отрицательных последствий сетевых атак путем правильной настрой-	Знать: основные виды сетевых атак и методы противодействия им. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности.

		формации.	ки операционной системы. Владеть: навыками разработки защищенных сайтов.	Владеть: разработки архитектуры сетевой защиты.
	ОПК-12.3 Оценивает информационные риски в автоматизированных системах.	Знать: классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования объекта информатизации. Уметь: определять угрозы безопасности автоматизированных систем, определять возможные риски нарушения безопасности функционирования объекта информатизации. Владеть: навыками анализа защищенности автоматизированных систем; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности автоматизированных систем.	Знать: основные компоненты автоматизированных систем объекта информатизации, состав, структуры и принципы функционирования современных автоматизированных систем, требования основных законов и нормативных документов в области безопасности автоматизированных систем. Уметь: определять состав, структуру и принципы функционирования современных автоматизированных систем, анализировать требования основных законов и нормативных документов в области безопасности автоматизированных систем Владеть: навыками выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности авто-	Знать: методы, способы и методики анализа рисков безопасности автоматизированных систем; классификацию основных источников угроз, комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности автоматизированных систем; основные принципы построения комплексной системы защиты автоматизированных систем. Уметь: применять методики анализа рисков безопасности автоматизированных систем; определять основные источники угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности автоматизированных систем. Владеть: методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведе-

			матизированных систем.	ния и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты автоматизированных систем объекта информатизации.

7.3Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Технические средства разведки. Общие сведения	ОПК-9, ОПК-12	Лекция, СРС	Вопросы для устного опроса	1-8	Согласно таблице 7.2
2	Радиоэлектронная разведка	ОПК-9	Лекция, СРС	Вопросы для устного опроса	1-8	Согласно таблице 7.2
3	Оптическая разведка	ОПК-9	Лекция, СРС	Вопросы для устного опроса КВЗЛР №1	1-7 1-6	Согласно таблице 7.2
4	Акустическая разведка	ОПК-9	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2

5	Компьютерная разведка	ОПК-9	Лекция, СРС	Вопросы для устного опроса	1-8	Согласно таблице 7.2
6	Средства технической разведки	ОПК-9	Лекция, СРС	Вопросы для устного опроса	1-7	Согласно таблице 7.2
7	Противодействие техническим разведкам	ОПК-9, ОПК-12	Лекция, СРС	Вопросы для устного опроса	1-5	Согласно таблице 7.2
8	Радиоэлектронное противодействие и радиомаскировка	ОПК-9, ОПК-12	Лекция, лабораторные работы №2 3, СРС	Вопросы для устного опроса КВЗЛР №2 КВЗЛР №3	1-10 1-6 1-5	Согласно таблице 7.2
9	Противодействие акустической разведке	ОПК-9, ОПК-12	Лекция,СРС	Вопросы для устного опроса	1-7	Согласно таблице 7.2
10	Противодействие видовой разведке	ОПК-9, ОПК-12	Лекция,СРС	Вопросы для устного опроса	1-4	Согласно таблице 7.2
11	Защита от внедряемых на объекты разведывательных устройств	ОПК-9, ОПК-12	Лекция, лабораторные работы №4,5, СРС	Вопросы для устного опроса КВЗЛР №4 КВЗЛР №5	1-6 1-6 1-5	Согласно таблице 7.2
12	Технические средства защиты информации	ОПК-9, ОПК-12	Лекция, лабораторные работы №6,7, СРС	Вопросы для устного опроса КВЗЛР №6 КВЗЛР №7	1-5 1-5 1-10	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗЛР – контрольные вопросы для защиты лабораторных работ.

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 12. «Технические средства защиты информации».

1. Область применения нелинейных локаторов.
2. Какие существуют методы защиты информации от утечки по электромагнитному каналу?
3. Предназначение отсекающего линейного фильтра.

Контрольные вопросы для защиты лабораторной работы №3 «Анализ технических средств перехвата информации в акустическом диапазоне»:

1. Чем описывается область слухового восприятия человека?
2. Основные величины и их соотношения, характеризующие разборчивость речи.
3. Очерёдность проведения инструментальной проверки.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,

– на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Какой средний радиус подавления диктофонов способен обеспечить генератор шума дециметрового диапазона:

А) 1метр.

Б) 5 метров.

В) 0,5 метров.

Г) 10 метров.

Задание в открытой форме:

1. Перехват акустических сигналов по виброакустическим техническим каналам осуществляется …….

2. Оптико-электронный технический канал утечки информации образуется путем……..

3. Техническими средствами приёма, обработки и хранения информации являются……...

4. Дальняя зона электромагнитного поля располагается в границах……

Задание на установление правильной последовательности.

Установить в правильном порядке этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

Задание на установление соответствия:
между элементами и функциями

1	Подавлениеемкостных паразитныхсвязей	А	Средства выявления каналов утечки информации
2	Телевизионныесистемы	Б	Защита информации от утечки по техническим каналам
3	Нелинейныелокаторы	В	Аттестация объектов информатизации
4	Специальныепроверки	Г	Средства инженерной защиты объектов

Компетентностно-ориентированная задача:

Определить уровень потерь распространения сигнала, если высота передатчика и приёмника составляют 15 и 1,5 метров соответственно, несущая частота сигнала 450 МГц, расстояние от передатчика - 500 метров.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по темам 1-4	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 5-8	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 9-12	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Лабораторная работа № 1-2	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил,доля правильных ответов более 90%
Лабораторная работа № 3	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №5	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №6	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №7	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме –2 балла,
– задание в открытой форме – 2 балла,
– задание на установление правильной последовательности – 2 балла,

– задание на установление соответствия – 2 балла,
– решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Котенко В. В. Теория информации: учебное пособие / В.В. Котенко. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 240 с. // Режим доступа - https://biblioclub.ru/index.php?page=book&id=561095. – Текст: электронный.

2. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие : [16+] / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. :– URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 20.08.2021). Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

3. Зайцев А.П. Технические средства и методы защиты информации [Текст]: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

4. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=208567

5. Меньшаков Ю.К. Основы защиты от технических разведок[Текст]: учебное пособие / Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2011. – 478 с.

6. Меньшаков Ю.К. Виды и средства иностранных технических средств разведок[Текст]: учебное пособие Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2009. – 656 с.

7. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=90753

8. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=429070

9. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

10. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

8.3 Перечень методических указаний

1. Защита информации от утечки по техническим каналам: Методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун- т; сост.: Е.А. Кулешова. Курск, 2023. 53 с. – Текст: электронный.

2. Защита информации от утечки по техническим каналам: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 23 с.. – Текст: электронный.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.»- http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Защита информации от утечки по техническим каналам» являются лекциии лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, устного опроса, защиты отчетов по лабораторным и работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информации от утечки по техническим каналам»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Защита информации от утечки по техническим каналам» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Защита информации от утечки по техническим каналам» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной

форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14.Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Измененных	Заменённых	Аннулированных	новых			