ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля): **Защита информации от утечки по техническим каналам**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Умницын Ю. П., доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - является теоретическая и практическая подготовленность специалиста к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

Задачи дисциплины:

- ознакомление с техническими каналами утечки информации, обрабатывае-мой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) ин-формации;
- изучение способов и средств защиты информации, обрабатываемой технически-ми средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объек-тах информатизации и в выделенных помещениях

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части учебного плана.

Дисциплина изучается на 4 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов 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

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных; общие и специфические угрозы безопасности операционных систем и систем управления баз данных; основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Студент должен уметь:

решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Студент должен владеть навыками:

решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Седьмой семестр	Восьмой семестр
Контактная работа (всего)	**152**	**84**	**68**

Лабораторные	68	34	34
Лекции	68	34	34
Практические	16	16	
Самостоятельная работа (всего)	**64**	**60**	**4**
Виды промежуточной аттестации	**36**		**36**
Зачет с оценкой		+	
Экзамен	36		36
Общая трудоемкость часы	**252**	**144**	**108**
Общая трудоемкость зачетные единицы	**7**	**4**	**3**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (68 ч.)

Седьмой семестр. (34 ч.)

Тема 1. Основные понятия и определения. (2 ч.)

Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы.

Тема 2. Основные понятия и определения. (2 ч.)

Термины и определения в области технической защиты информации: утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получе-ния информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Тема 3. Место технической защиты информации в государственной системе защиты информации в Российской Федерации. (2 ч.)

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации).

Правовые аспекты защиты речевой информации.

Тема 4. Место технической защиты информации в государственной системе защиты информации в Российской Федерации. (2 ч.)

Законодательство в области защиты конфиденциальной речевой информации.

Действующие нормативные акты и инструкции.

Тема 5. Нормативные правовые акты Российской Федерации в области защиты информации. (2 ч.)

Руководящие и нормативно-методические документы ФСТЭК (Гостехкомиссии) России в области ТЗИ.

Ответственность за нарушение в сфере защиты информации.

Тема 6. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений.

Тема 7. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки инфор-мации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации, создаваемый путем вне-дрения в СВТ электронных устройств негласного получения информации.

Тема 8. Технические каналы утечки акустической (речевой) информации Характеристики речевого сигнала. (2 ч.)

Общая характери-стика и классификация технических каналов утечки акустической

информации.
Прямые акустические каналы утечки речевой информации.
Акустовибрационные каналы утечки речевой информации.
Акустооптический (оптикоэлектронный) канал утечки речевой информации.

Тема 9. Технические каналы утечки акустической (речевой) информации Характеристики речевого сигнала. (2 ч.)

Акустоэлектрические каналы утечки речевой информации.
Акустоэлектромагнитные каналы утечки речевой информации.
Средства акустической разведки и их технические характеристики.

Тема 10. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Показатели эффективности защиты речевой информации.
Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции.

Тема 11. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Методика расчета словесной разборчивости речи.
Методика оценки возможностей средств акустической разведки по перехвату речевой информации.
Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Тема 12. Планирование работ по ТЗИ (2 ч.)

Перечень организационно-распорядительных документов по ТЗИ.
Порядок разработки организационно-распорядительных документов по ТЗИ.
Контроль состояния защиты информации на предприятии.
Классификация угроз безопасности информации на предприятии (в организации, учреждении).

Тема 13. Планирование работ по ТЗИ (2 ч.)

Характеристика нарушителей.
Модели нарушителей, имеющих и не имеющих доступ в контролируемую зону предприятия (организации, учреждения).
Требования руководящих документов по размещению и оборудованию объектов информатизации.

Тема 14. Содержание и организация проведения специальных проверок технических средств передачи, обработки и хранения информации, ВТСС и выделенных помещений на наличие воз-можно внедренных закладочных устройств. (2 ч.)

Структура, содержание документов по результатам специальных проверок.
Содержание и организация проведения специальных исследований технических средств передачи, обработки и хранения информации, ВТСС.

Тема 15. Содержание и организация проведения специальных проверок технических средств передачи, обработки и хранения информации, ВТСС и выделенных помещений на наличие воз-можно внедренных закладочных устройств. (2 ч.)

Структура, содержание документов по результатам специальных исследований.
Лицензирование и сертификация в области технической защиты информации.

Тема 16. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Способы и средства защиты информации, обрабаты-ваемой средствами вычислительной техники и автоматизированными системами.
Классификация способов и средств защиты объектов информатизации.
Экранирование технических средств их соединительных линий.
Экранированные помещения. Заземление технических средств.

Тема 17. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Требования к системам электропитания и заземления основных технических средств и систем.

Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке).
Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).
Защищённые средства вычислительной техники.

Восьмой семестр. (34 ч.)

Тема 18. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
Звукоизоляция выделенных помещений. Звукопоглощающие материалы.

Тема 19. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке).
Способы и средства защиты вспомогательных технических средств и систем.
Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генера-торы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Тема 20. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений.

Тема 21. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники.

Тема 22. Методы и средства технической разведки. (2 ч.)

Классификация техничских средств разведки. Методы и средства технической разведки.

Тема 23. Методы и средства технической разведки. (2 ч.)

Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.

Тема 24. Методы и средства выявления электронных устройств негласного получения информации. (2 ч.)

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы.

Тема 25. Методы и средства выявления электронных устройств негласного получения информации. (2 ч.)

Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации. Способы и принципы работы средств защиты информации от перехвата. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей.

Тема 26. Организационные основы инженерно-технической защиты информации. (2 ч.)

Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации. Основные задачи, структура и характеристика

государственной системы противодействия технической разведке.

Тема 27. Организационные основы инженерно-технической защиты информации. (2 ч.)

Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств.

Тема 28. Способы и средства защиты информации от наблюдения. (2 ч.)

Способы и средства противодействия наблюдению в оптическом диапазоне волн.

Тема 29. Способы и средства защиты информации от наблюдения. (2 ч.)

Способы информационного скрытия объектов от радиолокационного наблюдения.

Тема 30. Средства инженерной защиты и технической охраны. (2 ч.)

Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства
управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.

Тема 31. Средства инженерной защиты и технической охраны. (2 ч.)

Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

Тема 32. Методическое обеспечение инженерно-технической защиты информации. (2 ч.)

Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты.
Моделирование угроз безопасности информации.

Тема 33. Методическое обеспечение инженерно-технической защиты информации. (2 ч.)

Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты.

Тема 34. Методическое обеспечение инженерно-технической защиты информации. (2 ч.)

Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов.

5.2. Содержание дисциплины: Лабораторные (68 ч.)

Седьмой семестр. (34 ч.)

Тема 1. Основные понятия и определения. (2 ч.)

Термины и определе-ния в области технической защиты информации: объект информа-
тизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получе-ния информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Тема 2. Основные понятия и определения. (2 ч.)

Термины и определе-ния в области технической защиты информации: объект информа-
тизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получе-ния информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Тема 3. Место технической защиты информации в государст-венной системе защиты информации в Российской Федерации. (2 ч.)

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации).
Правовые аспекты защиты речевой информации.

Тема 4. Место технической защиты информации в государственной системе защиты информации в Российской Федерации. (2 ч.)

Законодательство в области защиты конфиденциальной речевой информации.

Действующие нормативные акты и инструкции.

Тема 5. Нормативные правовые акты Российской Федерации в области защиты информации. (2 ч.)

Руководящие и нормативно-методические документы ФСТЭК (Гостехкомиссии) России в области ТЗИ.

Ответственность за нарушение в сфере защиты информации.

Тема 6. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений.

Тема 7. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки инфор-мации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации, создаваемый путем вне-дрения в СВТ электронных устройств негласного получения информации.

Тема 8. Технические каналы утечки акустической (речевой) информации. Характеристики речевого сигнала. (2 ч.)

Общая характери-стика и классификация технических каналов утечки акустической информации.

Прямые акустические каналы утечки речевой информации.

Акустовибрационные каналы утечки речевой информации.

Акустооптический (оптикоэлектронный) канал утечки речевой информации.

Тема 9. Технические каналы утечки акустической (речевой) информации. Характеристики речевого сигнала. (2 ч.)

Акустоэлектрические каналы утечки речевой информации.

Акустоэлектромагнитные каналы утечки речевой информации.

Средства акустической разведки и их технические характеристики.

Тема 10. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Показатели эффективности защиты речевой информации.

Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции.

Тема 11. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Методика расчета словесной разборчивости речи.

Методика оценки возможностей средств акустической разведки по перехвату речевой информации.

Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Тема 12. Планирование работ по ТЗИ (2 ч.)

Перечень организационно-распорядительных документов по ТЗИ.

Порядок разработки организационно-распорядительных документов по ТЗИ.

Контроль состояния защиты информации на предприятии.

Классификация угроз безопасности информации на предприятии (в организации, учреждении).

Тема 13. Планирование работ по ТЗИ (2 ч.)

Структура, содержание документов по результатам специальных исследований.

Лицензирование и сертификация в области технической защиты информации.

Тема 14. Содержание и организация проведения специальных проверок технических средств передачи, обработки и хранения информации, ВТСС и выделенных помещений на наличие воз-можно внедренных закладочных устройств. (2 ч.)

Структура, содержание документов по результатам специальных проверок.

Содержание и организация проведения специальных исследований технических средств передачи, обработки и хранения информации, ВТСС.

Тема 15. Содержание и организация проведения специальных проверок технических средств передачи, обработки и хранения информации, ВТСС и выделенных помещений на наличие воз-можно внедренных закладочных устройств. (2 ч.)

Структура, содержание документов по результатам специальных проверок. Содержание и организация проведения специальных исследований технических средств передачи, обработки и хранения информации, ВТСС. Структура, содержание документов по результатам специальных исследований. Лицензирование и сертификация в области техни-ческой защиты информации.

Тема 16. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Способы и средства защиты информации, обрабаты-ваемой средствами вычислительной техники и автоматизированными системами.

Классификация способов и средств защиты объектов информатизации.

Экранирование технических средств их соединительных линий.

Экранированные помещения. Заземление технических средств.

Тема 17. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Требования к системам электропитания и заземления основных технических средств и систем.

Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке).

Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).

Защищённые средства вычислительной техники.

Восьмой семестр. (34 ч.)

Тема 18. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

Звукоизоляция выделенных помещений. Звукопоглощающие материалы.

Тема 19. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 ч.)

Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке).

Способы и средства защиты вспомогательных технических средств и систем.

Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генера-торы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Тема 20. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений.

Тема 21. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. (2 ч.)

Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники.

Тема 22. Методы и средства технической разведки. (2 ч.)

Классификация техничских средств разведки. Методы и средства технической разведки.

Тема 23. Методы и средства технической разведки. (2 ч.)

Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.

Тема 24. Методы и средства выявления электронных устройств негласного получения информации. (2 ч.)

Тема 25. Методы и средства выявления электронных устройств негласного получения информации. (2 ч.)

Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации. Способы и принципы работы средств защиты информации от перехвата. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей.

Тема 26. Организационные основы инженерно-технической защиты информации. (2 ч.)

Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической разведке.

Тема 27. Организационные основы инженерно-технической защиты информации. (2 ч.)

Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств.

Тема 28. Способы и средства защиты информации от наблюдения. (2 ч.)

Способы и средства противодействия наблюдению в оптическом диапазоне волн.

Тема 29. Способы и средства защиты информации от наблюдения. (2 ч.)

Способы информационного скрытия объектов от радиолокационного наблюдения.

Тема 30. Средства инженерной защиты и технической охраны. (2 ч.)

Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства
управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.

Тема 31. Средства инженерной защиты и технической охраны. (2 ч.)

Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

Тема 32. Методическое обеспечение инженерно-технической защиты информации. (2 ч.)

Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты.
Моделирование угроз безопасности информации.

Тема 33. Методическое обеспечение инженерно-технической защиты информации. (2 ч.)

Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты.

Тема 34. Методическое обеспечение инженерно-технической защиты информации. (2 ч.)

Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов.

5.3. Содержание дисциплины: Практические (16 ч.)

Седьмой семестр. (16 ч.)

Тема 1. Концепция технической защиты информации (2 ч.)

Что собой представляет техническая защита информации? Каковы принципиальные отличия технической защиты информации от прочих методов обеспечения информационной безопасности? Каковы цели и задачи технической защиты информации? На каком структурном уровне организации
информационных систем работает техническая защита информации (согласно модели OSI)? Что представляет собой информация и носитель защищаемой информа

Тема 2. Концепция технической защиты информации (2 ч.)

Что собой представляет инженерно-техническое добывание информации? Какие виды инженерно-технического добывания информации известны? Что собой представляет системный подход к защите информации? Какие характеристики и показатели эффективности инженерно-технической защиты информации вам известны? Какие существуют основные параметры системы технической защиты информации? Какие существуют основные направления инженерно-технической защиты информации?

Тема 3. Утечка информации по техническим каналам. (2 ч.)

Что собой представляет утечка информации? Что собой представляет технический канал утечки информации? Основные классификации технических каналов утечки информации? Какие разновидности технических каналов утечки речевой информации вам известны? В чём состоит принципиальное отличие технических каналов утечки?

Тема 4. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов. (2 ч.)

На чём основана обобщённая методика оценки протяжённости технического канала утечки информации? Что такое "разборчивость речи"? Какие показатели разборчивости речи вам известны? Какова методика расчёта показателей разборчивости речи? Какова методика субъективной оценки разборчивости речи? Какие существуют методы подавления опасных акустических сигналов? Каковы основные закономерности ослабления радиосигналов при их распространении?

Тема 5. Методы противодействия утечке и добыванию информации. (2 ч.)

Какие существуют методы противодействия радиоэлектронным каналам утечки вам известны? Какие методы противодействия акустоэлектрическим каналам утечки вам известны? Какие методы противодействия виброакустическим каналам утечки вам известны и в чём состоит их особенность? Какие методы противодействия оптикоэлектронным каналам утечки вам известны? Какие методы противодействия электрическим каналам утечки вам известны? Какие существуют методы противодействия перехвату телефонных переговоров?

Тема 6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок. (2 ч.)

Что собой представляют "побочные электромагнитные излучения" (ПЭМИ) и какова их физическая природа? В чём состоит принципиальное отличие ПЭМИ от радиоканалов передачи информации? Что такое "наводки" и какова их физическая природа? Что такое радиусы R1 и R2? Как выглядит профиль стандартной функции ослабления ПЭМИ и что собой представляют ближняя, промежуточная и дальняя зоны ЭМИ? Какой объект является элементарным излучателем побочных электрических полей? Какой объект является элементарным излучателем побочных магнитных полей?

Тема 7. Моделирование процессов технической защиты информации (2 ч.)

Каковы основные этапы проектирования системы защиты информации? Каковы основные принципы оптимизации
системы технической защиты информации? Каковы основные принципы моделирования объектов технической защиты? Каковы основные принципы моделирования технических каналов утечки информации? Каковы основные принципы моделирования каналов технического добывания информации?

Тема 8. Технические средства добывания информации (2 ч.)

Что собой представляет "закладное устройство"? Какие различают способы классификации закладных устройства? Какие существуют виды закладных устройств, различающихся по типу технического канала утечки информации? Какие бывают типы закладных устройств,

различающихся по типу источника питания? Какие различают типы закладных устройств, различающихся по регулярности режима работы? С какими техническими ограничениями сталкивается злоумышленник при разработке закладного устройства?

6. Виды самостоятельной работы студентов по дисциплине

Седьмой семестр (60 ч.)

Вид СРС: Подготовка рефератов (60 ч.)

Тематика заданий СРС:

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.

Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.

Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.

Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.

Структура реферата.

1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.

При проверке реферата оцениваются:

- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;

Темы рефератов:

1. Контроль эффективности защиты информации. рекомендации по выбору средств защиты.
2. Способы и принципы работы средств защиты информации от перехвата.
3. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.
4. Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).
5. Основные средства средств выявления электронных устройств негласного получения информации.

Восьмой семестр (4 ч.)

Вид СРС: Конспектирование текста (4 ч.)

Тематика заданий СРС:

Представляет собой вид внеаудиторной самостоятельной работы студента по созданию обзора информации, содержащейся в объекте конспектирования, в более краткой форме. В конспекте должны быть отражены основные принципиальные положения источника, то новое, что внес его автор, основные методологические положения работы, аргументы, этапы доказательства и выводы. Ценность конспекта значительно повышается, если студент излагает мысли своими словами, в лаконичной форме. Конспект должен начинаться с указания реквизитов источника (фамилии автора, полного наименования работы, места и года издания).
Критерии оценки:
содержательность конспекта, соответствие плану;
отражение основных положений, результатов работы автора, выводов;
ясность, лаконичность изложения мыслей студента;
наличие схем, графическое выделение особо значимой информации;
соответствие оформления требованиям;
грамотность изложения;
конспект сдан в срок.

Литература для конспектирования:
1. Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам. - М.: НПЦ "Нелк", 1998. - 200 с.
2. Баранов В.М., Вальков Г.В., Еремеев М.А. и др. Защита информации в системах и средствах связи. Учебное пособие. - Санкт- Петербург: ВИККА имени А.Ф. Можайского, 1994. - 113с.
3. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности: Учебное пособие для вузов. Ч. 1 : Технические каналы утечки информации. - Томск : ТМЦДО , 2004. - 199 с.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС

компетенции	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.
Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов 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

Студент должен знать:

основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных; общие и специфические угрозы безопасности операционных систем и систем управления баз данных; основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Вопросы, задания:

1. Виды, источники и носители защищаемой информации.
2. Концепция инженерно-технической защиты информации.
3. Основные принципы организации и методы реализации технической защиты информации.

Студент должен уметь:

решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Задания:

1. Различать виды защищаемой информации, идентифицировать её источники и носители.
2. Выявлять основные угрозы безопасности информации и оценивать их степень.

3. Использовать основные руководящие и нормативные документы в сфере инженерно-технической защиты информации.

Студент должен владеть навыками:

решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий

Задания:

1. Методы аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем передачи, хранения и обработки информации.

2. Методами инженерного расчета размеров контролируемой зоны.

3. Навыки работы с профессиональными аппаратными средствами инженерно-технической защиты информации.

8.3. Вопросы промежуточной аттестации

Седьмой семестр (Зачет с оценкой)

1. Классификация и краткая характеристика технических каналов утечки информации.
2. Структура канала утечки информации.
3. Технические средства приема, обработки, хранения и передачи информации.
4. Пассивные и активные методы защиты информации.
5. Способы и средства предотвращения утечки информации по техническим каналам.

Восьмой семестр (Экзамен)

1. Организация работ по технической защите конфиденциальной информации.
2. Классификация каналов утечки информации по виду информативного сигнала и среде распространения.
3. Общая классификация технических каналов утечки по источнику информации.
4. Перехват побочных электромагнитных излучений.
5. Способы перехвата информации, обрабатываемой техническими средствами.

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Зачет с оценкой

зачет с оценкой служит формой проверки усвоения учебного материала по дисциплине (модулю), практики, готовности к практической деятельности.

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Седьмой семестр

1. Контрольная работа - от 0 до 0 баллов
2. Устный опрос, собеседование - от 0 до 0 баллов
3. Письменные задания или лабораторные работы - от 0 до 0 баллов
4. Зачет с оценкой - Аттестация по дисциплине в форме зачета (зачета с оценкой) проводится по сумме результатов модульных контрольных работ и текущей успеваемости обучающегося.

Восьмой семестр

1. Контрольная работа - от 0 до 0 баллов
2. Устный опрос, собеседование - от 0 до 0 баллов
3. Письменные задания или лабораторные работы - от 0 до 0 баллов
4. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Жук Александр Павлович Защита информации [Электронный ресурс]: учебное - Издание 2 - РИОР, 2018. - 392 с. - Режим доступа: http://new.znanium.com/go.php?id=937469

2. Щеглов Андрей Юрьевич Защита информации: основы теории [Электронный ресурс]: - Юрайт, 2019. - 309 с. - Режим доступа: https://urait.ru/bcode/433715

3. Казарин Олег Викторович Программно-аппаратные средства защиты информации. Защита программного обеспечения [Электронный ресурс]: - Юрайт, 2019. - 312 с. - Режим доступа: https://urait.ru/bcode/437163

9.2 Дополнительная литература

1. Хорев Павел Борисович Программно-аппаратная защита информации [Электронный ресурс]: учебное - ФОРУМ, 2009. - 352 с. - Режим доступа: http://new.znanium.com/go.php?id=169345

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru - Научная электронная библиотека
2. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю
3. http://www.consultant.ru/ - КонсультантПлюс
4. http://www.garant.ru/ - Гарант
5. http://www.scopus.com/ - Scopus

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых

лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:
- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения (обновление производится по мере появления новых версий программы)

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы (обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/
Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/

КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
Специализированная мебель:
1. парта со скамьей – 40 шт.
2. учебные места – 80 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, меловая)
2. Мультимедийное оборудование
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной
аттестации.
Специализированная мебель:
1. столы – 8 шт.
2. стулья – 16 шт.
3. учебные места – 16 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Учебно-лабораторные стенды:
1. типовые схемотические решения
Средства для измерения и визуализации частотных и
временных характеристик сигналов:
1. осциллограф С1-65
2. осциллограф С1-77
3. осциллограф С1-93
Средства для измерения параметров электрических цепей:
1. селективный вольтметр В6-9
2. микровольтметр устройство В6-10
3. частотомер электрич. Ч3-63
Средства генерирования сигналов:
1. генератор Г4-102
2. генератор Г3-106
3. генератор Г3-118
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)