МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Защита информации от утечки по техническим каналам» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000EAB102
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Цель дисциплины: Подготовка специалистов, способных эффективно организовывать и проводить мероприятия по защите информации от утечки по техническим каналам.

Задачи дисциплины:

- Освоение теоретических основ защиты информации.
- Овладение методами выявления и предотвращения утечек информации.
- Формирование навыков применения технических средств защиты.
- Изучение современных подходов и стандартов сертификации и аттестации защитных решений.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-13 : Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1к : понимает основные угрозы информационной безопасности предприятия (организации); методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации	РД1	Знание	Современные методы и технологии защиты информации
			РД2	Умение	Быстро восстанавливать работоспособность средств защиты информации при чрезвычайных ситуациях.
			РД3	Навык	Использование специализированных процедур и технологий для устранения сбоев в работе систем защиты.
	ОПК-6 : Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими	ОПК-6.2к : организовывает защиту в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной	РД4	Знание	Законодательные и нормативные требования в области информационной безопасности
			РД5	Умение	Грамотно разрабатывать планы и процедуры защиты информации в рамках действующего законодательства.
			РД6	Навык	Применение требований

	документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	службы по техническому и экспортному контролю			нормативных актов ФСБ и ФСТЭК при проектировании систем защиты

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Внимательность к деталям
Формирование духовно-нравственных ценностей		
Формирование ответственного отношения к труду	Созидательный труд	Дисциплинированность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Взаимопомощь и взаимоуважение	Дисциплинированность
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Высокие нравственные идеалы	Любовь к стране

2 Место дисциплины (модуля) в структуре ОПОП

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Технологии и методы программирования». На данную дисциплину опираются «Программно-аппаратные средства защиты информации»

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	7	4	70	18	36	0	1	15	74	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Методы обнаружения несанкционированных технических каналов утечки информации	РД1, РД2, РД3, РД5, РД6	6	12	0	15	практическое задание
2	Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН)	РД1, РД2, РД3, РД5, РД6	6	12	0	15	практическое задание
3	Организация комплексной защиты информационных ресурсов предприятия	РД1, РД2, РД3, РД5, РД6	6	12	0	15	практическое задание
Итого по таблице			**18**	**36**	**0**	**45**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Методы обнаружения несанкционированных технических каналов утечки информации.

Содержание темы: Понятие технического канала утечки информации и классификация таких каналов. Особенности идентификации и локализации пассивных и активных технических каналов утечки. Методы визуального осмотра помещений и техники для выявления закладных устройств. Специальные устройства и комплексы для детектирования скрытой записи и наблюдения (радиочастотные сканеры, индикаторы поля, нелинейные локаторы и др.). Проверка коммуникационных линий и инженерных коммуникаций на наличие технических каналов утечки. Порядок действий при обнаружении подозрительных технических средств и дальнейшие шаги по нейтрализации угрозы.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН).

Содержание темы: Механизм возникновения побочных электромагнитных излучений и возможности их использования злоумышленниками. Принципы экранирования помещений и электрооборудования для снижения уровня излучаемых сигналов. Использование специальных покрытий и материалов для поглощения и рассеивания электромагнитных волн. Выбор оптимальной частоты помехоподавляющих фильтров и устройств. Тестирование и сертификация технических средств защиты от ПЭМИН. Международные стандарты и нормы в области защиты от электромагнитных излучений. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Организация комплексной защиты информационных ресурсов предприятия.

Содержание темы: Определение критически важных информационных активов предприятия и оценка их значимости. Моделирование угроз информационной безопасности и разработка стратегии противодействия. Комплексные решения для защиты от физических проникновений и удалённых кибератак. Правильная организация сетевых периметров и межсетевого взаимодействия. Планирование физической защиты серверных комнат и зон обработки чувствительной информации. Мониторинг и аудит соблюдения регламента безопасности, периодические проверки соответствия установленным стандартам. Мероприятия по обучению сотрудников правилам безопасной работы с информацией и повышению осведомлённости персонала.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение

аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (Дата обращения - 22.10.2025)
2. Техническая защита информации : практикум / сост. А. С. Кравченко, В. А. Мельник, С. Л. Сахаров ; ФКОУ ВО Воронежский институт ФСИН России. - Иваново : Издательско-полиграфический комплекс «ПресСто», 2023. - 80 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2158325 (Дата обращения - 22.10.2025)

7.2 Дополнительная литература

1. Техническая защита информации: практикум : учебное пособие / Л. В. Аршинский, А. А. Бутин, Н. И. Глухов [и др.]. — Иркутск : ИрГУПС, 2022. — 76 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/342083 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Office 2013 Suites and Apps KMS
- Microsoft Windows 10 Home SL

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-13 : Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1к : понимает основные угрозы информационной безопасности предприятия (организации); методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации
	ОПК-6 : Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.2к : организовывает защиту в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-6.2к : организовывает защиту в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	РД 4	Знание	Законодательные и нормативные требования в области информационной безопасности	решение тестовых заданий
	РД 5	Умение	Грамотно разрабатывать планы и процедуры защиты информации в рамках действующего законодательства.	выполнение практических заданий
	РД 6	Навык	Применение требований нормативных актов ФСБ и ФСТЭК	выполнение практических заданий

			при проектировании систем з ащиты	

Компетенция ОПК-13 «Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-13.1к : понимает основные угрозы информационной безопасности предприятия (организации); методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации	РД 1	Знание	Современные методы и технологии защиты информации	решение тестовых заданий
	РД 2	Умение	Быстро восстанавливать работоспособность средств защиты информации при чрезвычайных ситуациях.	выполнение практических заданий
	РД 3	Навык	Использование специализированных процедур и технологий для устранения сбоев в работе систем защиты.	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : Современные методы и технологии защиты информации	1.1. Методы обнаружения несанкционированных технических каналов утечки информации	Тест	Экзамен в устной форме
		1.2. Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН)	Тест	Экзамен в устной форме
		1.3. Организация комплексной защиты информационных ресурсов предприятия	Тест	Экзамен в устной форме
РД2	Умение : Быстро восстанавливать работоспособность средств защиты и	1.1. Методы обнаружения несанкционированных технических каналов утечки информации	Практическая работа	Экзамен в устной форме

	нформации при чрезвычайных ситуациях.	1.2. Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН)	Практическая работа	Экзамен в устной форме
		1.3. Организация комплексной защиты информационных ресурсов предприятия	Практическая работа	Экзамен в устной форме
РД3	Навык : Использование специализированных процедур и технологий для устранения сбоев в работе систем защиты.	1.1. Методы обнаружения несанкционированных технических каналов утечки информации	Тест	Экзамен в устной форме
		1.2. Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН)	Тест	Экзамен в устной форме
		1.3. Организация комплексной защиты информационных ресурсов предприятия	Тест	Экзамен в устной форме
РД5	Умение : Грамотно разрабатывать планы и процедуры защиты информации в рамках действующего законодательства.	1.1. Методы обнаружения несанкционированных технических каналов утечки информации	Практическая работа	Экзамен в устной форме
		1.2. Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН)	Практическая работа	Экзамен в устной форме
		1.3. Организация комплексной защиты информационных ресурсов предприятия	Практическая работа	Экзамен в устной форме
РД6	Навык : Применение требований нормативных актов ФСБ и ФСТЭК при проектировании систем защиты	1.1. Методы обнаружения несанкционированных технических каналов утечки информации	Практическая работа	Экзамен в устной форме
		1.2. Современные подходы к защите от побочных электромагнитных излучений (ПЭМИН)	Практическая работа	Экзамен в устной форме
		1.3. Организация комплексной защиты информационных ресурсов предприятия	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест	Практические задания	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		60		60
Промежуточная аттестация			20	20
Итого2	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1. Что такое ПЭМИН?

A) Путевые электрические измерения наводок напряжения

B) Побочные электромагнитные излучения и наводки

C) Параметры эксплуатационного мониторинга инфраструктурных сетей

D) Первичные элементы механического интерфейса настольных приборов

2. Какой способ наиболее эффективен для защиты информации от утечки по акустическим каналам?

A) Установка звукопоглощающих панелей

B) Шифрование передаваемого звука

C) Повышение громкости фонового шума

D) Полностью изолированные помещения

Какие приборы используются для выявления прослушивающих устройств?

3. A) Инфракрасные камеры

B) Магнитометры

C) Радиосканеры и нелинейные локаторы

D) Термоскопы

4. Как называется процесс систематического контроля правильности функционирования средств защиты информации?

A) Аттестация

B) Сертификация

C) Аккредитация

D) Лицензирование

5. Какой термин обозначает защиту информации путём физического ограничения доступа посторонних лиц к источникам информации?

A) Организационные меры защиты

B) Физическая защита

C) Техническая защита

D) Логическая защита

6. Какая мера применяется для уменьшения риска утечки информации по кабельным линиям питания?

A) Замена обычных проводов экранированными

B) Частота шифрования кабеля

C) Увеличение количества витых пар

D) Монтаж дополнительного оборудования для усиления сигнала

7. Какой документ регламентирует порядок обязательной сертификации средств защиты информации в России?

A) ГОСТ Р 50922-2006

B) Федеральный закон №152-ФЗ

C) Постановление Правительства РФ №1119

D) Приказ ФСБ России №378

8. Какой канал утечки является результатом нежелательных электромагнитных излучений электронного оборудования?

A) Прямой акустический канал

B) Электромагнитный канал

C) Проводной канал

D) Визуальный канал

9. Чем отличаются технические каналы утечки от организационных?

A) Только техническими каналами пользуются хакеры

B) Организационные каналы зависят исключительно от человеческого фактора

C) Технические каналы связаны исключительно с физическими устройствами

D) Все перечисленные утверждения неверны

10. Какие меры относятся к организационным мерам защиты информации?

A) Установление режима секретности и ограничение допуска сотрудников

B) Использование антивирусных программ

C) Установка охранных сигнализаций

D) Применение криптографических алгоритмов

11. Что означает аббревиатура СПЗИ?

A) Система профилактики защиты информации

B) Совокупность правовых норм защиты информации

C) Средство противодействия злонамеренным инцидентам

D) Система предупреждения и защиты информации

12. Какой уровень классификации соответствует самой строгой степени защиты информации согласно российскому законодательству?

A) Конфиденциальная информация

B) Информация ограниченного распространения

C) Государственная тайна

D) Открытая информация

13. Какой прибор используется для проверки целостности и качества изоляции электрических сетей?

A) Мегомметр

B) Микроскоп

C) Линейный индикатор

D) Индикатор влажности воздуха

14. Что называют демаскирующими признаками объекта?

A) Внешне заметные особенности, позволяющие выявить объект наблюдению

B) Неправильно настроенная система сигнализации

C) Отсутствие должного освещения территории вокруг объекта

D) Повреждение ограждений охраняемой зоны

15. Что относится к основным методам повышения стойкости системы защиты информации против взлома?

A) Использование сложных паролей и многоуровневой аутентификации

B) Постоянное обновление операционной системы и приложений

C) Периодическое обучение сотрудников принципам информационной безопасности

D) Всё вышеперечисленное верно

Краткие методические указания

Перед решением тестов внимательно следует ознакомься с каждым вопросом и предлагаемыми вариантами ответов. Затем необходимо опираясь на теоретический материал, связанный с темой вопроса сопоставить его с приведёнными вариантами. Выбирается тот ответ, который точно отражает изложенные факты.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Вопросы к экзамену

1. Назовите основные виды технических каналов утечки информации.
2. Объясните механизм образования побочных электромагнитных излучений (ПЭМИН) и пути их предотвращения.
3. Охарактеризуйте разницу между активной и пассивной защитой информации от утечки по техническим каналам.
4. Приведите классификацию технических средств выявления несанкционированных устройств съёма информации.
5. Раскройте понятие «аттестация объекта информатизации» и этапы проведения данной процедуры.
6. Расскажите о существующих стандартах и правилах сертификации средств защиты информации.
7. Определите понятия «демаскирующий признак объекта» и поясните, каким образом они влияют на безопасность.
8. Опишите принципы построения системы защиты информации от утечки по акустическим каналам.
9. Назовите и охарактеризуйте известные вам методики и оборудование для поиска закладочных устройств.
10. Поясните значение термина «нормативно-правовая база защиты информации» и приведите примеры важнейших законодательных актов.
11. Перечислите возможные причины появления утечек информации по проводным каналам и назовите меры по их предотвращению.
12. Рассмотрите проблемы защиты информации от несанкционированного видеонаблюдения и укажите эффективные контрмеры.
13. В чём заключается суть принципа «глубокой обороны» применительно к защите информации?
14. Какую роль играет проверка на предмет наличия закладки («закладка») в обеспечении информационной безопасности?
15. Назовите различия между технической и организационной защитой информации и оцените значимость каждой составляющей в общей системе защиты.

Краткие методические указания

Для ответы на представленные вопросы необходимо изучать как теоретический, так и практический материал

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.

5.3 Примеры заданий для выполнения практических работ

Задание 1

Описание : Студенты проводят экспериментальное исследование влияния различных факторов на интенсивность побочных электромагнитных излучений. Необходимо измерить уровни излучения различных офисных приборов (компьютеров, принтеров, роутеров) и предложить оптимальные защитные меры.

Порядок выполнения :

1. Подготовьте помещение для измерений.
2. Используйте специальный инструмент (анализатор спектра) для замеров интенсивности излучения.
3. Запишите полученные значения и сравните их с установленными стандартами.
4. Разработайте перечень рекомендаций по снижению уровня излучения.

Задание 2. Проект по созданию схемы защиты офиса от утечки информации

Описание : Создать проект комплексного защитного комплекса для офисного помещения среднего размера. Задача — разработать схему, включающую меры физической и технической защиты, учитывая требования к оборудованию и помещениям.

Порядок выполнения :

1. Выберите гипотетический офис (размер, количество работников, оборудование).
2. Составьте список угроз и потенциальных каналов утечки информации.
3. Предложите защитные меры: экранирование, установку датчиков движения, видеонаблюдение, фильтрацию сигналов.
4. Представьте итоговую схему и расчеты стоимости реализации проекта.

Задание 3. Практическое задание по поиску закладных устройств

Описание : Участники получают набор виртуальных ситуаций (описание интерьера, подозреваемое устройство) и специальное программное обеспечение для моделирования процесса поиска. Нужно определить возможное размещение и конфигурацию закладки, выбрать подходящее средство для её обнаружения и представить отчет о проведенном поиске.

Порядок выполнения :

1. Ознакомьтесь с заданием (местоположение, характеристики подозреваемого устройства).
2. Выберите оптимальный инструмент для поиска (радиосканер, нелинейный локатор, металлодетектор).
3. Проверьте эффективность выбранного инструмента в условиях виртуальной среды.
4. Предоставьте отчёт с описанием хода поиска и найденных результатов.

Краткие методические указания

Отчетом является файл с подробным отчётом, где описаны этапы работы при выполнении работы в программе. Отчёт оформляется в соответствии с требованиями ВВГУ СТО. Структурными элементами отчета являются: титульный лист; содержание; основная часть; заключение; список использованных источников.

Шкала оценки

Оценка	Баллы	Описание
5	45-60	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	30-44	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	14-29	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-13	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/или неверно применил методы необходимые его выполнения.