



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
«Б1.В.05 СИСТЕМЫ КОНТРОЛЯ УТЕЧКИ ДАННЫХ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Егорихин Д. Е.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-1 Способен администрировать средства защиты информации в компьютерных системах и сетях

ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах

Знать:

ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации

Уметь:

ПК-1.1/Ум1 анализировать и идентифицировать архитектуры подсистем защиты информации в различных операционных системах

Владеть:

ПК-1.1/Нв1 навыками администрирования и эксплуатации средств защиты информации, встроенных в операционные системы, включая осуществление настройки, тестирования и диагностики подсистем защиты

ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах

Знать:

ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности

Уметь:

ПК-1.2/Ум1 настраивать параметры сканирования, создавать правила и исключения для корректной работы систем и приложений

Владеть:

ПК-1.2/Нв1 навыками администрирования и конфигурирования антивирусных программ, обеспечивающих эффективную защиту систем

ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения

Знать:

ПК-1.3/Зн1 классификацию вредоносного программного обеспечения

ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях

Уметь:

ПК-1.3/Ум1 анализировать результаты сканирования и определять степень угрозы и характер вредоносного ПО

Владеть:

ПК-1.3/Нв1 навыками внедрения комплексных мер обнаружения вредоносного ПО, включая автоматизированные и ручные методы

ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования

Знать:

ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры

Уметь:

ПК-1.4/Ум1 применять антивирусные и антишпионские средства для удаления обнаруженного вредоносного ПО

ПК-1.4/Ум2 оценивать и устранять последствия функционирования вредоносного ПО, такие как изменения в настройках безопасности, повреждение данных и системных компонентов

Владеть:

ПК-1.4/Нв1 навыками применения специализированных инструментов и скриптов для очистки и восстановления систем

ПК-1.4/Нв2 навыками анализа безопасности системы после удаления вредоносного ПО и подтверждения полного устранения угрозы

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-1 Способен администрировать средства защиты информации в компьютерных системах и сетях	Повышенный	ИДК ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах Знать: ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации Уметь: ПК-1.1/Ум1 анализировать и идентифицировать архитектуры подсистем защиты информации в различных операционных системах Владеть: ПК-1.1/Нв1 навыками администрирования и эксплуатации средств защиты информации, встроенных в операционные системы, включая осуществление настройки, тестирования и диагностики подсистем защиты ИДК ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах Знать: ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности Уметь: ПК-1.2/Ум1 настраивать параметры сканирования, создавать правила и исключения для корректной работы систем и приложений Владеть: ПК-1.2/Нв1 навыками администрирования и конфигурирования антивирусных программ, обеспечивающих эффективную защиту систем ИДК ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения Знать: ПК-1.3/Зн1 классификацию вредоносного программного обеспечения

	ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях Уметь: ПК-1.3/Ум1 анализировать результаты сканирования и определять степень угрозы и характер вредоносного ПО Владеть: ПК-1.3/Нв1 навыками внедрения комплексных мер обнаружения вредоносного ПО, включая автоматизированные и ручные методы ИДК ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования Знать: ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры Уметь: ПК-1.4/Ум1 применять антивирусные и антишпионские средства для удаления обнаруженного вредоносного ПО ПК-1.4/Ум2 оценивать и устранять последствия функционирования вредоносного ПО, такие как изменения в настройках безопасности, повреждение данных и системных компонентов Владеть: ПК-1.4/Нв1 навыками применения специализированных инструментов и скриптов для очистки и восстановления систем ПК-1.4/Нв2 навыками анализа безопасности системы после удаления вредоносного ПО и подтверждения полного устранения угрозы
Базовый	ИДК ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах Знать: ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации Уметь: ПК-1.1/Ум1 анализировать и идентифицировать архитектуры подсистем защиты информации в различных операционных системах ИДК ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах Знать: ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности

	Уметь: ПК-1.2/Ум1 настраивать параметры сканирования, создавать правила и исключения для корректной работы систем и приложений ИДК ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения Знать: ПК-1.3/Зн1 классификацию вредоносного программного обеспечения ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях Уметь: ПК-1.3/Ум1 анализировать результаты сканирования и определять степень угрозы и характер вредоносного ПО ИДК ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования Знать: ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры Уметь: ПК-1.4/Ум1 применять антивирусные и антишпионские средства для удаления обнаруженного вредоносного ПО ПК-1.4/Ум2 оценивать и устранять последствия функционирования вредоносного ПО, такие как изменения в настройках безопасности, повреждение данных и системных компонентов
Пороговый	ИДК ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах Знать: ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации ИДК ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах Знать: ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности

		ИДК ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения Знать: ПК-1.3/Зн1 классификацию вредоносного программного обеспечения ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях ИДК ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования Знать: ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры
--	--	---

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации ПК-1.1/Ум1 анализировать и идентифицировать архитектуры подсистем защиты информации в различных операционных системах ПК-1.1/Нв1 навыками администрирования и эксплуатации средств защиты информации, встроенных в операционные системы, включая осуществление настройки, тестирования и диагностики подсистем защиты ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности ПК-1.2/Ум1 настраивать параметры сканирования, создавать правила и исключения для корректной работы систем и приложений ПК-1.2/Нв1 навыками администрирования и конфигурирования антивирусных программ, обеспечивающих эффективную защиту систем ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения ПК-1.3/Зн1 классификацию вредоносного программного обеспечения ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях ПК-1.3/Ум1 анализировать результаты сканирования и определять степень угрозы и характер вредоносного ПО ПК-1.3/Нв1 навыками внедрения комплексных мер обнаружения вредоносного ПО, включая автоматизированные и ручные методы

	ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры ПК-1.4/Ум1 применять антивирусные и антишпионские средства для удаления обнаруженного вредоносного ПО ПК-1.4/Ум2 оценивать и устранять последствия функционирования вредоносного ПО, такие как изменения в настройках безопасности, повреждение данных и системных компонентов ПК-1.4/Нв1 навыками применения специализированных инструментов и скриптов для очистки и восстановления систем ПК-1.4/Нв2 навыками анализа безопасности системы после удаления вредоносного ПО и подтверждения полного устранения угрозы
Хорошо	ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации ПК-1.1/Ум1 анализировать и идентифицировать архитектуры подсистем защиты информации в различных операционных системах ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности ПК-1.2/Ум1 настраивать параметры сканирования, создавать правила и исключения для корректной работы систем и приложений ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения ПК-1.3/Зн1 классификацию вредоносного программного обеспечения ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях ПК-1.3/Ум1 анализировать результаты сканирования и определять степень угрозы и характер вредоносного ПО ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры ПК-1.4/Ум1 применять антивирусные и антишпионские средства для удаления обнаруженного вредоносного ПО ПК-1.4/Ум2 оценивать и устранять последствия функционирования вредоносного ПО, такие как изменения в настройках безопасности, повреждение данных и системных компонентов
Удовлетворительно	ПК-1.1 Идентифицирует архитектуры подсистем защиты информации в операционных системах ПК-1.1/Зн1 основные принципы аппаратно-программной защиты информации ПК-1.2 Настраивает антивирусные средства защиты информации в операционных системах ПК-1.2/Зн1 рекомендации и методики обеспечения совместимости антивирусных программ с другими системными средствами безопасности

	ПК-1.3 Выполняет работы по обнаружению вредоносного программного обеспечения ПК-1.3/Зн1 классификацию вредоносного программного обеспечения ПК-1.3/Зн2 методы и средства обнаружения вредоносного ПО в операционных системах и сетях ПК-1.4 Выполняет работы по ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования ПК-1.4/Зн1 основные виды вредоносного программного обеспечения и характер их воздействия на операционные системы и сетевые инфраструктуры
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Зачет с оценкой

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Концепция инженерно-технической защиты информации	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4		Зачет с оценкой
2	Теоретические основы инженерно-технической защиты информации	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4		Зачет с оценкой
3	Физические основы технической защиты информации	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4		Зачет с оценкой
4	Системы защиты от утечки информации	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4		Зачет с оценкой
5	Применение и эксплуатация технических средств защиты информации	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4	Тестирование	Зачет с оценкой

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет с оценкой, 5 семестр.

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

6. Оценочные материалы текущего контроля

Раздел 5. Применение и эксплуатация технических средств защиты информации

Контролируемые ИДК: ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4

Тема 5.1. Применение и эксплуатация технических средств защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какое из приведённых определений наиболее полно характеризует понятие "документированная информация"?

- 1) Информация, представленная в устной форме и не зафиксированная на материальном носителе.
- 2) Информация, зафиксированная на материальном носителе и предназначенная для передачи, хранения или обработки.
- 3) Любая информация, доступная для публичного распространения.
- 4) Информация, содержащая государственную тайну и охраняемая законом.

2. Каково основное отличие государственной тайны от конфиденциальной информации?

- 1) Государственная тайна относится к сведениям, охраняемым государством, а конфиденциальная информация — к сведениям, охраняемым организацией.

- 2) Конфиденциальная информация всегда является государственной тайной.
- 3) Государственная тайна не подлежит защите, а конфиденциальная информация — подлежит.
- 4) Государственная тайна — это открытая информация, а конфиденциальная — закрытая.

3. Какие из перечисленных относятся к основным объектам защиты информации?

- 1) Только данные и документы.
- 2) Только программное обеспечение и данные.
- 3) Только аппаратные средства и каналы связи.
- 4) Аппаратные средства, программное обеспечение, данные, персонал.

4. Что такое демаскирующие признаки и для чего они используются?

- 1) Скрытые признаки, используемые для маскировки информации.
- 2) Признаки, позволяющие обнаружить наличие технических средств утечки информации.
- 3) Методы шифрования информации.
- 4) Признаки, используемые для классификации информации по уровню секретности.

5. Какое определение соответствует термину "Контролируемая зона"?

- 1) Зона, где отсутствует контроль за информационными потоками.
- 2) Зона, свободно доступная для всех сотрудников.
- 3) Зона, в которой осуществляется комплекс мер по предотвращению утечки информации.
- 4) Зона, где разрешено использование любых технических средств.

6. Какие компоненты входят в состав технического канала утечки информации?

- 1) Источник информации, передатчик, средство передачи, приёмник, приёмная сторона.
- 2) Только источник информации и приёмник.
- 3) Только передатчик и средство передачи.
- 4) Только приёмник и приёмная сторона.

7. К каким классам относится классификация технической разведки?

- 1) Активная и пассивная.
- 2) Внешняя и внутренняя.
- 3) Техническая и программная.
- 4) Открытая и скрытая.

8. Какие методы противодействия утечке информации по техническим каналам являются наиболее эффективными?

- 1) Использование открытых каналов связи.
- 2) Только использование антивирусного ПО.
- 3) Только обучение персонала.
- 4) Физическая изоляция, экранирование, фильтрация и маскировка сигналов.

9. Что из перечисленного является примером технического канала утечки речевой информации?

- 1) Печатные документы.
- 2) Электронная почта и мессенджеры.
- 3) Радиозакладки и акустические утечки через вентиляцию.
- 4) Видеонаблюдение.

10. Какое влияние оказывают паразитные емкостные, индуктивные и резистивные связи в каналах утечки информации?

- 1) Усиливают сигнал и облегчают его обнаружение.
- 2) Ослабляют сигнал и делают утечку невозможной.
- 3) Не оказывают никакого влияния на утечку информации.
- 4) Приводят к искажению информации без утечки.

11. Что из перечисленного относится к способам скрытого видеонаблюдения?

- 1) Открытое размещение камер на видных местах.
- 2) Использование миниатюрных камер, маскировка под бытовые предметы.
- 3) Использование только проводных систем видеонаблюдения.
- 4) Применение только звуковых датчиков.

12. Какой принцип действия лежит в основе работы металлодетекторов?

- 1) Излучение и приём электромагнитных волн, отражаемых металлическими объектами.
- 2) Анализ акустических сигналов.
- 3) Использование инфракрасного излучения.
- 4) Детекция радиоволн.

7. Оценочные материалы промежуточной аттестации

5 семестр, Зачет с оценкой

Контролируемые ИДК: ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4

Вопросы/Задания:

1. Дайте определение информации, документированной информации. Каково отличие государственной тайны, конфиденциальной информации и открытой информации?
2. Классификация технической разведки. Эффективность добывания информации технической разведкой.
3. Государственная система защиты информации. Эффективность защиты информации.
4. Основные объекты защиты информации.
5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры.
6. Дайте определение терминам Контролируемая зона, Опасная зона, Опасная зона 1, Опасная зона 2.
7. Состав технического канала утечки информации. 8. Классификация технических каналов утечки информации.
8. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры.
9. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры.
10. Перечислите каналы утечки речевой информации. Приведите примеры.
11. Перечислите каналы утечки видовой информации. Приведите примеры.
12. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах 59592?
13. Перечислите методы противодействия утечке информации по техническим каналам.
14. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения.
15. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок.

16. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».
17. Направленные микрофоны. Принцип действия.
18. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.
19. Датчики охранных систем. Принципы действия датчиков.
20. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.
21. Средства радиотехнической разведки. Состав. Характеристики.
22. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.
23. Периметровые средства охраны. Датчики периметровых систем охраны.
24. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.
25. Экранирование электромагнитных волн.
26. Экранирование акустических сигналов.
27. Фильтрация опасных сигналов. Приведите примеры.
28. Маскировка опасных сигналов зашумлением. Приведите примеры.
29. Металлодетекторы. Сферы применения. Принцип действия.
30. Локаторы нелинейностей. Сферы применения. Принцип действия.
31. Аттестация объектов информатизации по требованиям безопасности. Назначение. Порядок проведения аттестации.
32. Специальная проверка. Специальное обследование. Специальное исследование.
33. Проведение измерений акустических и виброакустических характеристик. Приведите примеры.
34. Проведение измерений побочных электромагнитных излучений. Приведите примеры.