МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Методы анализа защищенности информационных систем

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Методы анализа защищенности информационных систем", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-1 - Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.

Результаты обучения по дисциплине:

Знать технические средства контроля эффективности мер защиты информации.

Уметь контролировать безотказное функционирование технических средств защиты информации.

Владеть методами анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.

2 Место дисциплины "Методы анализа защищенности информационных систем" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Нормативные требования по защите информации, Классификация защищаемой информации и информационных систем, Методы и средства защиты информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Методы анализа защищенности информационных систем" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Методы анализа защищенности информационных систем" составляет 4 зачетных единицы, 144 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 3/Семестр 6			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	16		

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Самостоятельная работа	80		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Методы анализа защищенности информационных систем", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Методика анализа защищенности информационных систем	2
2. Понятие защищенности информационных систем, определение защищенной информационной системы	2
3. Последовательность мероприятий по анализу защищенности	2
4. Структура отчета по результатам анализа защищенности	2
5. Тестирование системы защиты по методу «черного» и «белого» ящика	2
6. Анализ защищенности внешнего периметра корпоративной сети и внутренней ИТ-инфраструктуры	2
7. Инструментальные средства анализа защищенности	2
8. Методы предотвращения сетевых атак на периметр сети	2
Итого	**16**

4.2. Практические занятия

Наименование работы Вид СРС	Трудоемкость в часах
	ОФ
1. Методика анализа защищенности информационных систем	4
2. Понятие защищенности информационных систем, определение защищенной информационной системы	4
3. Последовательность мероприятий по анализу защищенности	4
4. Структура отчета по результатам анализа защищенности	4
5. Тестирование системы защиты по методу «черного» и «белого» ящика	4
6. Анализ защищенности внешнего периметра корпоративной сети и внутренней ИТ-инфраструктуры	4
7. Инструментальные средства анализа защищенности	4
8. Методы предотвращения сетевых атак на периметр сети	4

Итого	**32**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	30
Оформление отчетов по практическим и(или) лабораторным работам	44
Подготовка к промежуточной аттестации	6
Итого	**80**
Самостоятельная работа под руководством преподавателя	16

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Методы анализа защищенности информационных систем"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ПК-1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	**Знать** технические средства контроля эффективности мер защиты информации. **Уметь** контролировать безотказное функционирование технических средств защиты информации. **Владеть** методами анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	Высокий или средний

Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено.
Средний уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено.
Низкий уровень достижения компетенции - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Критерии оценивания при ответе на вопросы:
- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Методика анализа защищенности информационных систем

1. Нормативные документы, описывающие методики анализа защищенности информационных систем
2. Принципы анализа ИС на предмет защищенности
3. Критерии и оценка уязвимостей компьютерной системы при проведении анализа.
4. Разновидности методик проверки и оценки уровня защищенности ИС
5. Выбор наиболее оптимальной методики оценки защищенности для конкретной ИС

2. Понятие защищенности информационных систем, определение защищенной информационной системы

1. Какие ключевые аспекты включает в себя понятие защищенности ИС?
2. Приведите пример одного из наиболее известных определений защищенной информационной системы

3. Измеряемые критерии защищенности ИС
4. Нормативные документы для оценки защищенности ИС
5. Относительность понятия «защищенная ИС»

3. Последовательность мероприятий по анализу защищенности

1. Основные этапы и методы работ по проведению анализа защищенности ИС. Программа анализа защищенности.
2. Методы сбора исходной информации для проведения анализа защищенности ИС
3. Анализ собранной исходной информации для проведения анализа защищенности ИС
4. Разновидности методов анализа (аудита) защищенности ИС
5. Формирование рабочей группы по проведению анализа защищенности ИС

4. Структура отчета по результатам анализа защищенности

1. Какие разделы включает в себя отчет по результатам анализа защищенности ИС?
2. Входят ли в состав отчета по анализу защищенности рекомендации по устранению недостатков и повышению уровня защищенности?
3. Для чего нужны и что содержится в опросных листах?
4. Какие отчеты программных и аппаратных средств приводятся в приложении к основному отчету по анализу защищенности?
5. Какие анализируемые объекты ИС описываются в специально выделенном для этого разделе?

5. Тестирование системы защиты по методу «черного» и «белого» ящика

1. Стратегия тестирования по методу черного ящика
2. Стратегия тестирования по методу белого ящика
3. На чем строится стратегия тестирования по методу черного ящика? Что является исходными данными?
4. Каким путем тестировщик получает тестовые данные по стратегии белого ящика?
5. На чем основан выбор стратегии белого или черного ящика?

6. Анализ защищенности внешнего периметра корпоративной сети и внутренней ИТ-инфраструктуры

1. На предмет каких атак и угроз выполняется анализ защищенности внешнего периметра корпоративной сети?
2. Примерные алгоритмы анализа защищенности для внешнего периметра корпоративной сети и внутренней ИТ-инфраструктуры
3. Какие объекты подлежат проверке в процессе анализа защищенности внешнего периметра?
4. Что проверяется и что не проверяется для веб-приложений в процессе анализа защищенности внешнего периметра?
5. Какие объекты подлежат проверке в процессе анализа защищенности Внутренней ИТ-инфраструктуры?

7. Инструментальные средства анализа защищенности

1. Программные средства анализа защищенности
2. Аппаратные средства анализа защищенности
3. Типовой набор инструментов анализа защищенности базового уровня
4. Типовой набор инструментов анализа защищенности повышенного уровня
5. Особенности анализа систем предотвращения вторжений (СПВ), основной объект анализа в СПВ.

8. Методы предотвращения сетевых атак на периметр сети

1. Методы защиты сетевого периметра от вирусных атак
2. Принцип работы систем IPS и IDS
3. Межсетевой экран как один из барьеров в предотвращении сетевых атак на периметр сети
4. Основной принцип защиты периметра сети
5. Алгоритм действий при обнаружении сетевых атак

Примерный перечень тестовых заданий:
1. Методика анализа защищенности информационных систем

1. Какая из перечисленных распространенных методик анализа защищенности ИС использует количественные методики оценки рисков?

FRAP
RiskWatch
CRAMM
Microsoft

2. Чем определяется ценность физических ресурсов в методике анализа защищенности CRAMM?

временем, необходимым на восстановление в случае разрушения
объемом финансовых активов организации
стоимостью их восстановления в случае разрушения

3. Что из перечисленного характерно для методики анализа защищенности OCTAVE?

весь процесс анализа автоматизирован, производится на основании параметрических функций
весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов
весь процесс анализа производится силами внешних консультантов, без привлечения сотрудников организации

2. Понятие защищенности информационных систем, определение защищенной информационной системы

1. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?

Информационная защита информации
Информационная безопасность
Зашита информации

2. Концепция "Защищенные информационные системы" включает ряд: выбрать все верные

законодательных инициатив,
научных решений
технических решений
технологических решений,

3. Укажите верные определения защищенной ИС: выбрать все верные

это система, которая для определенных условий эксплуатации обеспечивает конфиденциальность, целостность и доступность части информационного пространства, содержащего критичную информацию, и поддерживает работоспособность в условиях воздействия на неё множества угроз
это система, которая успешно и эффективно противостоит угрозам безопасности
это система, удовлетворяющая требованиям информационной безопасности использующих ее субъектов информационных отношений, в которой возможные риски сведены к допустимому минимуму

3. Последовательность мероприятий по анализу защищенности

1. Какие основные этапы работ включены в регламент мероприятий по анализу защищенности: выбрать все верные

Инициирование и планирование
Обследование, документирование и сбор информации
Анализ полученных данных и уязвимостей
Выработка рекомендаций
Подготовка отчетных документов
Поиск компетентного персонала

2. На каком этапе формируются модели угроз?

Инициирование и планирование
Обследование, документирование и сбор информации
Анализ полученных данных и уязвимостей

3. Какой вид анализа не проводится в рамках мероприятий по анализу защищенности ИС?

Анализ и устранение уязвимостей информационной системы
Анализ установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации
Анализ работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
Анализ состава технических средств, программного обеспечения и средств защиты информации
Анализ правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
Анализ кадрового состава и его квалификации

4. Структура отчета по результатам анализа защищенности

1. Сколько основных разделов, включая Приложения, содержится в отчете по результатам анализа защищенности

7
8
9
10

2. Результаты каких анализов приводятся в отчете отдельными разделами? выбрать все верные

Результаты анализа организационных уязвимостей
Результаты анализа защищенности внешнего периметра сети
Результаты анализа защищенности внутренней ИТ-инфраструктуры
Результаты анализа защищенности рабочих помещений на предмет утечки информации по техническим каналам

3. К какому разделу отчета относится анализ топологии локальной вычислительной сети (ЛВС)?

Результаты анализа защищенности внешнего периметра сети
Результаты анализа защищенности внутренней ИТ-инфраструктуры
Структура и состав комплекса программно-технических средств

5. Тестирование системы защиты по методу «черного» и «белого» ящика

1. Основное средство тестирования по методу черного ящика это:

сетевые сканеры
программные агенты системного уровня

2. При каком методе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам?

метод черного ящика
метод белого ящика

3. При каком методе тестирования имитируют действия потенциальных злоумышленников, пытающихся взломать систему защиты?

метод черного ящика
метод белого ящика

6. Анализ защищенности внешнего периметра корпоративной сети и внутренней ИТ-инфраструктуры

1. Для анализа защищенности чего проверочные мероприятия включают в себя проверку межсетевых экранов на наличие уязвимостей?

внешнего периметра
внутренней ИТ-инфраструктуры

2. Анализ защищенности внутренней ИТ-инфраструктуры организации предполагает проведение

полного комплекса мероприятий по техническому аудиту, включая: выбрать все верные

Анализ конфигурационных файлов маршрутизаторов, межсетевых экранов, почтовых серверов, DNS серверов и других критичных элементов сетевой инфраструктуры
Проверка межсетевых экранов на наличие уязвимостей
Обследование Web и Почтового серверов

3. Анализ защищенности чего предполагает большее количество мероприятий:

внутренней ИТ-инфраструктуры
внешнего периметра сети

7. Инструментальные средства анализа защищенности

1. Среди перечисленного актуальными перечнями уязвимостей являются: выбрать все верные

SANS top 20
CVE
OSSTMM

2. К категориям программно-аппаратных средств защиты, используемых для анализа защищенности относятся: выбрать все верные

Сетевые сканеры безопасности
Сетевые взломщики паролей
Сетевые снифферы и анализаторы протоколов
Сетевые спуферы
Сетевые фишеры

3. К какому виду средств относятся средства Brutus, Hydra, LC5?

Сетевые взломщики паролей
Сетевые сканеры безопасности
Хостовые средства анализа параметров защиты
Средства инвентаризации и сканеры ресурсов сети

8. Методы предотвращения сетевых атак на периметр сети

1. Лучшими методами для предотвращения рисков сетевых атак на периметр сети являются: выбрать все верные

Конфигурирование систем и использование автоматизированных средств для предотвращения инсталляции/деинсталляции программного обеспечения пользователями
Использование прокси-серверов на периметре вашей сети
Использование автоматизированных средств повышения осведомленности и применение санкций к тем, кто не соблюдает допустимую политику использования средств обработки информации
Устранение недостатков безопасности в веб-приложениях, посредством проверки знаний программистов в области безопасности и поиска дефектов программного обеспечения

2. Какие сценарии используются при моделировании сетевых атак для улучшения методов защиты периметра сети? выбрать все верные

подбор учетных данных
социальная инженерия
открытые данные
групповые политики
атаки на протоколы сетевого и канального уровней

3. Каким образом можно уменьшить площадь атаки? Выбрать все верные

Ограничить разрешенные порты на уровне файерволла;
Ограничить используемые приложения в корпоративной сети;
Ограничить доступ к вредоносным ресурсам;
Запретить нежелательный тип контента (исполняемые файлы и т.д.);
Включить SSL-инспекцию, чтобы видеть всю картину
Запретить использование почтовых вложений

Отказаться от использования протокола Http

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации является зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Методы качественного анализа защищенных ИС
2. Принцип анализа уровня ИБ в защищенной ИС
3. Анализ рисков для защищаемой ИС
4. Принципы тестирования защищенных ИС

1774292599

5. Методы количественного анализа защищенных ИС
6. Метод экспертных оценок при анализе защищенных ИС
7. Метод информационных потоков при анализе защищенных ИС
8. Графовый метод при анализе защищенных ИС
9. Метод весовых коэффициентов при анализе защищенных ИС
10. Методы и средства анализа защищенности ИС
11. Анализ защищенности внешнего периметра корпоративной сети
12. Анализ защищенности внутренней ИТ-инфраструктуры
13. Нормативные документы, описывающие методики анализа защищенности информационных систем
14. Выбор наиболее оптимальной методики оценки защищенности для конкретной ИС
15. Методы сбора и анализа исходной информации для проведения анализа защищенности ИС
16. Формирование рабочей группы по проведению анализа защищенности ИС
17. Структура отчета по результатам анализа защищенности
18. Стратегия тестирования по методу черного ящика
19. Стратегия тестирования по методу белого ящика
20. Программные средства анализа защищенности
21. Аппаратные средства анализа защищенности
22. Типовой набор инструментов анализа защищенности базового уровня
23. Типовой набор инструментов анализа защищенности повышенного уровня
24. Особенности анализа систем предотвращения вторжений (СПВ), основной объект анализа в СПВ.
25. Методы анализа защиты внешнего сетевого периметра от угроз вирусных атак
26. Принцип работы систем IPS и IDS
27. Межсетевой экран как один из барьеров в предотвращении сетевых атак на периметр сети
28. Основной принцип защиты периметра сети
29. Алгоритм действий при обнаружении сетевых атак
30. Понятие и определение защищенности ИС
31. Концепция "Защищенные информационные системы"
32. Последовательность мероприятий по анализу защищенности

Примерный перечень тестовых заданий на экзамен:

1. Какая из перечисленных распространенных методик анализа защищенности ИС использует количественные методики оценки рисков?

FRAP
RiskWatch
CRAMM
Microsoft

2. Чем определяется ценность физических ресурсов в методике анализа защищенности CRAMM?

временем, необходимым на восстановление в случае разрушения
объемом финансовых активов организации
стоимостью их восстановления в случае разрушения

3. Концепция "Защищенные информационные системы" включает ряд: выбрать все верные

законодательных инициатив,
научных решений
технических решений
технологических решений,

4. Укажите верные определения защищенной ИС: выбрать все верные

это система, которая для определенных условий эксплуатации обеспечивает конфиденциальность, целостность и доступность части информационного пространства, содержащего критичную информацию, и поддерживает работоспособность в условиях воздействия на неё множества угроз
это система, которая успешно и эффективно противостоит угрозам безопасности
это система, удовлетворяющая требованиям информационной безопасности использующих ее субъектов информационных отношений, в которой возможные риски сведены к допустимому минимуму

5. Какие основные этапы работ включены в регламент мероприятий по анализу защищенности: выбрать все верные

Инициирование и планирование
Обследование, документирование и сбор информации
Анализ полученных данных и уязвимостей
Выработка рекомендаций
Подготовка отчетных документов
Поиск компетентного персонала

6. Какой вид анализа не проводится в рамках мероприятий по анализу защищенности ИС?

Анализ и устранение уязвимостей информационной системы
Анализ установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации
Анализ работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
Анализ состава технических средств, программного обеспечения и средств защиты информации
Анализ правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
Анализ кадрового состава и его квалификации

7. Результаты каких анализов приводятся в отчете отдельными разделами? выбрать все верные

Результаты анализа организационных уязвимостей
Результаты анализа защищенности внешнего периметра сети
Результаты анализа защищенности внутренней ИТ-инфраструктуры
Результаты анализа защищенности рабочих помещений на предмет утечки информации по техническим каналам

8. К какому разделу отчета относится анализ топологии локальной вычислительной сети (ЛВС)?

Результаты анализа защищенности внешнего периметра сети
Результаты анализа защищенности внутренней ИТ-инфраструктуры
Структура и состав комплекса программно-технических средств

9. При каком методе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам?

метод черного ящика
метод белого ящика

10. Анализ защищенности чего предполагает большее количество мероприятий:

внутренней ИТ-инфраструктуры
внешнего периметра сети

11. К какому виду средств относятся средства Brutus, Hydra, LC5?

Сетевые взломщики паролей
Сетевые сканеры безопасности
Хостовые средства анализа параметров защиты
Средства инвентаризации и сканеры ресурсов сети

12. Какие сценарии используются при моделировании сетевых атак для улучшения методов защиты периметра сети? выбрать все верные

подбор учетных данных
социальная инженерия
открытые данные
групповые политики
атаки на протоколы сетевого и канального уровней

13. Каким образом можно уменьшить площадь атаки? Выбрать все верные

Ограничить разрешенные порты на уровне файерволла;
Ограничить используемые приложения в корпоративной сети;
Ограничить доступ к вредоносным ресурсам;
Запретить нежелательный тип контента (исполняемые файлы и т.д.);
Включить SSL-инспекцию, чтобы видеть всю картину
Запретить использование почтовых вложений
Отказаться от использования протокола Http

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса,

выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Котов, Ю. А. Криптографические методы защиты информации : стандартные шифры. Шифры с открытым ключом : учебное пособие : [16+] / Ю. А. Котов. – Новосибирск : Новосибирский государственный технический университет, 2017. – 67 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574782 (дата обращения: 10.04.2026). – Библиогр. с 46. – ISBN 978-5-7782-3411-6. – Текст : электронный.

2. Дураковский, А. П. Оценка защищенности речевой информации : учебно-методическое пособие / А. П. Дураковский, И. В. Куницын. — Москва : НИЯУ МИФИ, [б. г.]. — Часть 1 : Выявление акустических и вибрационных каналов утечки речевой информации — 2015. — 52 с. — ISBN 978-5-7262-2173-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126657 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Дураковский, А. П. Оценка защищенности речевой информации : учебно-методическое пособие / А. П. Дураковский, И. В. Куницын. — Москва : НИЯУ МИФИ, [б. г.]. — Часть 2 : Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования — 2015. — 44 с. — ISBN 978-5-7262-2174-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126658 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Дураковский, А. П. Оценка защищенности речевой информации : учебно-методическое пособие / А. П. Дураковский, И. В. Куницын. — Москва : НИЯУ МИФИ, [б. г.]. — Часть 3 : Проведение инструментального контроля в канале высокочастотного акустоэлектрического преобразования — 2015. — 44 с. — ISBN 978-5-7262-2175-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126659 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

5. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133924 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие : [16+] / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=467139 (дата обращения: 16.04.2026). – Библиогр. в кн. – Текст : электронный.

2. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 09.04.2026). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

3. Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Прохорова, О. В. Информационная безопасность и защита информации : Учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7970-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169817 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Криптографические методы защиты информации : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 21 с. – URL: http://library.kuzstu.ru/meto.php?n=9123 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. База данных zbMath https://zbmath.org/
2. Универсальная полнотекстовая база данных электронных периодических изданий «ИВИС» https://eivis.ru/
3. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
4. Электронная библиотечная система «Лань» http://e.lanbook.com
5. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
6. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
7. Образовательная платформа «Юрайт» https://urait.ru/
8. Электронная библиотечная система «Znanium» https://new.znanium.com/my/documents
9. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
10. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
11. Национальная электронная библиотека https://rusneb.ru/
12. Электронная библиотека http://library.gorobr.ru/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646
2. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т.

Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Методы анализа защищенности информационных систем"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Методы анализа защищенности информационных систем", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Ubuntu
2. Libre Office
3. Mozilla Firefox
4. Google Chrome
5. 7-zip
6. Open Office
7. Microsoft Windows
8. ESET NOD32 Smart Security Business Edition
9. Kaspersky Endpoint Security

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Методы анализа защищенности информационных систем"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.