**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 обнаружения угроз безопасности 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 обнаружения угроз безопасности информационных систем", соотнесенных с планируемыми результатами освоения образовательной программы**

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-3 - Способен выявлять основные угрозы безопасности информации в автоматизированных системах

**Результаты обучения по дисциплине определяются индикаторами достижения компетенций**

**Индикатор(ы) достижения:**

Выявляет основные угрозы безопасности информации в автоматизированных системах.

**Результаты обучения по дисциплине:**

Знать особенности защиты информации в автоматизированных системах управления технологическими процессами. Организационные меры по защите информации.

Уметь анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации.

Владеть методами выявления основные угрозы безопасности информации.

**2 Место дисциплины "Методы обнаружения угроз безопасности 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 обнаружения угроз безопасности 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 обнаружения угроз безопасности информационных систем" составляет 6 зачетных единиц, 216 часов.

| **Форма обучения** | **Количество часов** | | |
|---|---|---|---|
| | **ОФ** | **ЗФ** | **ОЗФ** |
| **Курс 4/Семестр 7** | | | |
| Всего часов | 216 | | |
| **Контактная работа обучающихся с преподавателем (по видам учебных занятий):** | | | |
| Аудиторная работа | | | |
| *Лекции* | 32 | | |
| *Лабораторные занятия* | | | |
| *Практические занятия* | 32 | | |
| Внеаудиторная работа | | | |
| *Индивидуальная работа с преподавателем:* | | | |
| *Консультация и иные виды учебной деятельности* | | | |
| *Самостоятельная работа под руководством преподавателя* | 16 | | |
| **Самостоятельная работа** | 100 | | |
| **Форма промежуточной аттестации** | экзамен /36 | | |

**4 Содержание дисциплины "Методы обнаружения угроз безопасности информационных систем", структурированное по разделам (темам)**

**4.1. Лекционные занятия**

| **Раздел дисциплины, темы лекций и их содержание** | **Трудоемкость в часах** |
|---|---|
| | **ОФ** |
| 1. История развития технологий обнаружения угроз безопасности информационных систем | 1 |
| 2. Современные решения для обнаружения угроз безопасности информационных систем | 1 |
| 3. Межсетевые экраны нового поколения | 1 |
| 4. Системы мониторинга событий безопасности | 1 |
| 5. Системы анализа сетевого трафика | 2 |
| 6. Средства обнаружения угроз безопасности информационных систем на конечных устройствах | 2 |
| 7. Система анализа сетевого трафика нового поколения | 2 |
| 8. Системы учета и обработки угроз безопасности информационных систем | 2 |
| 9. Поиск угроз | 1 |
| 10. Средства поведенческого анализа | 1 |
| 11. Приманки для хакеров | 1 |
| 12. Развитие технологий обнаружения компьютерных атак в России | 1 |
| **Итого** | **16** |

**4.2. Практические занятия**

| **Наименование работы** | **Трудоемкость в часах** |
|---|---|
| | **ОФ** |
| 1. История развития технологий обнаружения угроз безопасности информационных систем | 2 |
| 2. Современные решения для обнаружения угроз безопасности информационных систем | 2 |
| 3. Межсетевые экраны нового поколения | 2 |
| 4. Системы мониторинга событий безопасности | 2 |
| 5. Системы анализа сетевого трафика | 4 |
| 6. Средства обнаружения угроз безопасности информационных систем на конечных устройствах | 4 |

| | |
|---|---|
| 7. Система анализа сетевого трафика нового поколения | 4 |
| 8. Системы учета и обработки угроз безопасности информационных систем | 4 |
| 9. Поиск угроз | 2 |
| 10. Средства поведенческого анализа | 2 |
| 11. Приманки для хакеров | 2 |
| 12. Развитие технологий обнаружения компьютерных атак в России | 2 |
| **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 | 18 |
| Оформление отчетов по практическим и(или) лабораторным работам | 20 |
| Подготовка к промежуточной аттестации | 6 |
| **Итого** | **44** |
| Самостоятельная работа под руководством преподавателя | 16 |

**5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Методы обнаружения угроз безопасности 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-3 | Выявляет основные угрозы безопасности информации в автоматизированных системах | **Знать** особенности защиты информации в автоматизированных системах управления технологическими процессами. Организационные меры по защите информации. **Уметь** анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации. **Владеть** методами выявления основные угрозы безопасности информации. | 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. История развития технологий обнаружения угроз безопасности информационных систем***

1. Каким образом начала решаться и сейчас решается задача по поиску уязвимостей и предотвращения угроз для ОС в период бурного развития сети Интернет?
2. Как раньше чаще всего ловили хакеров?
3. Каков принцип работы первых антивирусных программ?
4. На чем основаны первые способы обнаружения компьютерных атак?
5. Что является драйвером развития технологий обнаружения компьютерных атак?

***2. Современные решения для обнаружения угроз безопасности информационных систем***

1. Классификация современных систем обнаружения угроз ИБ
2. Современные технологии построения систем обнаружения угроз
3. Недостатки современных систем обнаружения угроз
4. Современная концепция обнаружения компьютерных угроз, а не атак
5. Краткая характеристика новой методики оценки угроз от ФСТЭК (05.02.2021)

***3. Межсетевые экраны нового поколения***

1. В чем концептуальные преимущества межсетевого экрана нового поколения (NGFW)?
2. Какой производитель NGFW на основании тестов является лидером по эффективности защиты?
3. Каким основным функционалом должен обладать NGFW?
4. От чего зависит скорость любого NGFW ?
5. Основные критерии выбора NGFW

***4. Системы мониторинга событий безопасности***

1. Какие объекты могут являться источниками событий ИБ?
2. Классификация систем мониторинга событий ИБ
3. Основные возможности систем мониторинга событий ИБ
4. Основные компоненты систем мониторинга событий ИБ
5. Исходные данные для правильной настройки системы мониторинга событий ИБ

***5. Системы анализа сетевого трафика***

1. Назначение системы анализа сетевого трафика в современных условиях
2. Основные логические компоненты системы анализа сетевого трафика
3. Недостатки существующих систем анализа сетевого трафика
4. Основные требования к системе анализа трафика
5. Основные методы анализа и мониторинга сетевого трафика

***6. Средства обнаружения угроз безопасности информационных систем на конечных устройствах***

1. Основная задача решений класса Endpoint Detection and Response (EDR)
2. Какие технологии обнаружения угроз безопасности используются обычно в решениях EDR?
3. На какие типы угроз в основном ориентированы решения класса EDR?
4. Принцип работы EDR – агента
5. Варианты реализации средства обнаружения угроз ИБ на конечных устройствах, примеры.

***7. Система анализа сетевого трафика нового поколения***

1. Какие технологии включает в себя система анализа сетевого трафика нового поколения (NDR) ?
2. Что такое и чем характерны NTA-подсистемы с точки зрения анализа трафика, входящие в состав систем анализа сетевого трафика нового поколения (NDR) ?
3. Какие еще, кроме NTA-подсистем, входят в состав NDR?
4. Преимущество систем NDR по сравнению с традиционными системами анализа сетевого трафика

5. Варианты реализации систем NDR, примеры.

***8. Системы учета и обработки угроз безопасности информационных систем***

1. Назначение систем учета и обработки информационных угроз Threat Intelligence Platform (TIP)
2. С каким типом специальных данных работают системы TIP?
3. С какими системами / подсистемами может интегрироваться система TIP?
4. Чем полезны системы TIP для сетевых аналитиков?
5. Варианты реализации систем TIP, примеры.

***9. Поиск угроз***

1. Принцип действия и основная цель процесса поиска угроз (Threat hunting)
2. Основные элементы процесса threat hunting
3. За счет чего осуществляется проработка гипотез о вероятных угрозах при использовании процесса threat hunting?
4. Что является важным элементом для поиска угроз, полезным для сетевого аналитика / аналитика ИБ?
5. Что является источниками данных, необходимых для работы процесса threat hunting?

***10. Средства поведенческого анализа***

1. Как еще не официально называются средства поведенческого анализа?
2. Назначение средств поведенческого анализа
3. Что моделируют средства поведенческого анализа?
4. В каких случаях использование средств поведенческого анализа наиболее актуально?
5. Приведите пример реализации средств поведенческого анализа в составе какого-либо ПО или автономно

***11. Приманки для хакеров***

1. Для чего используется класс решений «Honeypot» (приманка для хакеров)
2. Что используется в качестве «приманки» в решениях «Honeypot»?
3. Что такое ханипот-ссылки и для чего они нужны?
4. Для кого могут быть особенно полезны решения «Honeypot»?
5. Дополнительные возможности ханипотов нового поколения, ориентированных для приманки более продвинутых злоумышленников

***12. Развитие технологий обнаружения компьютерных атак в России***

1. Что послужило стимулом для развития собственных (российских) решений в сфере обнаружения компьютерных атак?
2. Как учитываются и регистрируются новые отечественные разработки в области программного и аппаратного обеспечения для ИБ?
3. Какие льготы предоставляются ИТ-компаниям, производящим программное и аппаратное обеспечение для ИБ?
4. Проведение какой процедуры гарантирует отсутствие программных и аппаратных закладок для средств обеспечения ИБ?
5. Приведите примеры российских программных и аппаратных средств обеспечения ИБ

***Примерный перечень тестовых заданий:***

***1. История развития технологий обнаружения угроз безопасности информационных систем***

1. Каким образом в основном обнаруживали хакеров лет 30 назад?

с помощью завербованных информаторов
средствами интеллектуального обнаружения и автоматизированного анализа
вычисляли по IP-адресу
вычисляли по MAC-адресу

2. По какому принципу работали первые антивирусные программы?

на основе сигнатур (образцов вирусного кода)

эвристический анализ
поведенческий анализ.

3. Выберите все верные утверждения:

Развитие техник и тактик атакующих, появление новых угроз и уязвимостей является драйвером развития технологий обнаружения компьютерных атак
Развитие технологий обнаружения компьютерных атак является драйвером развития техник и тактик атакующих, появление новых угроз и уязвимостей

***2. Современные решения для обнаружения угроз безопасности информационных систем***

1. Современные системы обнаружения угроз ИБ разделяются на: выбрать все верные

Системы обнаружения аномального поведения
Системы обнаружения злоумышленного поведения
Системы наблюдения за нормальным поведением ИС и пользователей

2. Современные системы обнаружения вторжений ориентированы на поиск:

аномалий взаимодействия контролируемых объектов;
сигнатур всех узнаваемых атак;
искажения эталонной профильной информации
определенных моделей угроз
определенных портретов злоумышленников

3. Для систем обнаружения атак нового типа можно выделить следующие крупные уровни, на которых возможно осуществление доступа к обрабатываемой информации: выбрать все верные

Уровень прикладного ПО
Уровень СУБД
Уровень операционной системы
Уровень среды передачи
Уровень БД
Уровень драйверов

***3. Межсетевые экраны нового поколения***

1. В чем концептуальные отличия межсетевого экрана нового поколения (NGFW) в отличие от традиционного? выбрать все верные

фильтруют трафик на уровне портов
фильтруют трафик на уровне протоколов
фильтруют трафик на уровне протоколов приложений
фильтруют трафик на уровне функций приложений

2. Укажите лидеров на рынке NGFW по данным компании Gartnet на 2020 год

Palo Alto Networks
Fortinet
Check Point Software Technologies
Cisco
Huawei
Microsoft

3. Какие из перечисленных технологий добавлены в NGFW по сравнению с традиционными? выбрать все верные

пакетная фильтрация трафика
контроль сетевых соединений
функции межсетевого экрана прикладного уровня
сигнатурный анализ трафика для обнаружения угроз и их блокирования
полнотекстовый анализ (инспекция) трафика, зашифрованного протоколами различного уровня
поведенческий анализ файлов в изолированной среде

регулярные обогащения данными об актуальных угрозах

***4. Системы мониторинга событий безопасности***

1. Какие объекты могут являться источниками событий ИБ? выбрать все верные

журналы ОС
антивирусные приложения
ПО, анализирующее защищенность инфраструктуры
сетевое оборудование
аппаратные датчики
сотрудники организации

2. Основные компоненты систем мониторинга событий ИБ: выбрать все верные

программные агенты
сервер
хранилища информации
консоль
персонал, работающий с системой
регламенты работы по мониторингу
подсистема IPS

3. Какая информация необходима для правильной настройки системы мониторинга событий ИБ? выбрать все верные

что должно рассматриваться в качестве инцидента ИБ
какие виды инцидентов присущи или могут быть присущи данной компании
какие события могут предварять каждый тип инцидента
какие источники могут производить инциденты
к каким рискам ведет каждый вид инцидента, и каков взаимный приоритет данных рисков
квалификация пользователей
тип и вид компьютерного оборудования

***5. Системы анализа сетевого трафика***

1. Системы анализа сетевого трафика (NTA) анализируют трафик:

на периметре
в ИТ-инфраструктуре
в обоих случаях

2. Системы анализа сетевого трафика (NTA) предназначены: выбрать все верные

выявление сетевых атак
перехвата и анализа сетевого трафика
отражения сетевых атак

3. В каких типах систем анализа сетевого трафика, мониторинг подразделяется на активный / пассивный / комбинированный?

маршрутизаторо-ориентированные
не маршрутизаторо-ориентированные
коммутаторо-ориентированные
объектно-ориентированые

***6. Средства обнаружения угроз безопасности информационных систем на конечных устройствах***

1. Основные задачи решений класса Endpoint Detection and Response (EDR): выбрать все верные

обнаружение компьютерных атак на конечных устройствах
отражение компьютерных атак на конечных устройствах
предоставить необходимые метрики для реагирования специалистам по ИБ
оценить размер возможного ущерба от атаки
предоставить информацию об атакующем специалистам по ИБ

обнаружение компьютерных атак, исходящих от конечных устройств во внешнюю сеть или периметр

2. Какие технологии обнаружения угроз безопасности могут обычно использоваться в решениях EDR?: выбрать все верные

агента для сбора и анализа данных
средство антивирусной защиты с поведенческим анализом
анализ индикаторов компрометации
автоматическое взаимодействие с SIEM- и Threat Intelligence- системами для обогащения данными об угрозах
средство антивирусной защиты с сигнатурным анализом
межсетевой экран

3. Принцип работы EDR – агента:

отслеживает открываемые вредоносной программой порты и передает это событие в систему управления событиями и информацией о безопасности (SIEM)
отслеживает открываемые вредоносной программой порты, закрывает порты и передает это событие в систему управления событиями и информацией о безопасности (SIEM)

***7. Система анализа сетевого трафика нового поколения***

1. Какие технологии включает в себя система анализа сетевого трафика нового поколения (NDR) ?

анализ сетевого трафика
поведенческая аналитика
эвристический анализ угроз

2. Укажите все верные утверждения относительно подсистем NTA, входящих в состав системы анализа сетевого трафика нового поколения:

NTA работает с трафиком как на периметре, так и в ИТ-инфраструктуре
хранят информацию о сетевых взаимодействиях

3. С какими средствами управления ИТ и ИБ могут интегрироваться системы анализа сетевого трафика нового поколения (NDR) ? выбрать все верные

межсетевые экраны
средства управления доступом к сети

***8. Системы учета и обработки угроз безопасности информационных систем***

1. Назначение систем учета и обработки информационных угроз Threat Intelligence Platform (TIP)

для обогащения, обнаружения, распространения и корреляции данных об угрозах
для анализа угроз в режиме реального времени
для анализа угроз на основе зафиксированных ранее событий

2. С каким типом специальных данных работают системы TIP?

фиды
сиды
пиры

3. Чем полезны системы  TIP для сетевых аналитиков?

помогают аналитикам находить следы компрометации в сети и системах
помогают аналитикам находить узкие места в сети ИТ-инфраструктуры
помогают аналитикам оптимизировать таблицы маршрутизации для оптимизации трафика

***9. Поиск угроз***

1. Принцип действия и основная цель процесса поиска угроз (Threat hunting)

поиск угроз происходит автоматически перед срабатыванием средства обнаружения или защиты и не зависит от работы аналитика
поиск угроз происходит перед срабатыванием средства обнаружения или защиты во время работы

аналитика
поиск угроз происходит после срабатыванием средства обнаружения или защиты во время работы аналитика
поиск угроз происходит автоматически после срабатыванием средства обнаружения или защиты и не зависит от работы аналитика

2. Основные элементы процесса threat hunting: выбрать все верные

Сбор данных
Аналитика
Исследование полученных данных
Нейтрализация атаки и разработка сценария реагирования на атаки

3. За счет чего осуществляется проработка гипотез о вероятных угрозах при использовании процесса threat hunting?

опыта специалистов центра реагирования, а также за счет получаемой информации из различных сетевых систем и устройств
автоматически подсистемой нейтрализация атаки
автоматически самим процессом threat hunting

***10. Средства поведенческого анализа***

1. Назначение средств поведенческого анализа: выбрать все верные

для анализа файлов на предмет наличия ВПО
для запуска подозрительного кода
для реализации виртуальной машины

2. Что моделируют средства поведенческого анализа?

экспериментальные средства обнаружения угроз безопасности ИС
виртуальную машину
изолированную среду для безопасного запуска исполняемых файлов

3. В каких случаях использование средств поведенческого анализа наиболее актуально?

для своевременного выявления потенциальных угроз
для отладки и испытания новых экспериментальных средств обнаружения угроз безопасности ИС
для отладки и испытания любого ПО

***11. Приманки для хакеров***

1. Для чего используется класс решений «Honeypot» (приманка для хакеров)? выбрать все верные

для обнаружения попыток взлома и изучения применяемых методов
для прогнозирования атак и принятия мер противодействия
для разоблачения хакера и получения информации о нем

2. Что используется в качестве «приманки» в решениях «Honeypot»?

изолированные от промышленных систем среды со специально открытыми портами, уязвимостями и другими явными недостатками
публичная информация об организации, размещенная в открытом доступе
сотрудники, имеющие доступ к секретной информации

3. Для кого могут быть особенно полезны решения «Honeypot»?

для пользователей, работающих в информационной системе
для системных администраторов и сетевых аналитиков
для специалистов, занимающихся поиском киберпреступников

***12. Развитие технологий обнаружения компьютерных атак в России***

1. Что послужило стимулом для развития собственных (российских) решений в сфере обнаружения компьютерных атак?

инициатива правительства по внедрению отечественного ПО в органах государственной власти и госкорпорациях с целью исключения кибершпионажа в пользу иностранных государств
программа по импортозамещению
резких скачок отечественных высоких и наукоемких технологий
налоговые льготы для разработчиков и производителей отечественных решений в сфере защиты информации

2. Как учитываются и регистрируются новые отечественные разработки в области программного и аппаратного обеспечения для ИБ?

в базе данных ФСТЭК
в базе данных ФСБ
в едином реестре российских программ для ЭВМ и баз данных

3. Проведение какой процедуры гарантирует отсутствие программных и аппаратных закладок для средств обеспечения ИБ?

сертификация
аттестация
аккредитация

***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. Каким образом начала решаться и сейчас решается задача по поиску уязвимостей и предотвращения угроз для ОС в период бурного развития сети Интернет?
2. Как раньше чаще всего ловили хакеров?
3. Каков принцип работы первых антивирусных программ?
4. На чем основаны первые способы обнаружения компьютерных атак?
5. Что является драйвером развития технологий обнаружения компьютерных атак?
6. Классификация современных систем обнаружения угроз ИБ
7. Современные технологии построения систем обнаружения угроз
8. Недостатки современных систем обнаружения угроз
9. Современная концепция обнаружения компьютерных угроз, а не атак
10. Краткая характеристика новой методики оценки угроз от ФСТЭК (05.02.2021)
11. В чем концептуальные преимущества межсетевого экрана нового поколения (NGFW)?
12. Какой производитель NGFW на основании тестов является лидером по эффективности защиты?
13. Каким основным функционалом должен обладать NGFW?
14. От чего зависит скорость любого NGFW ?
15. Основные критерии выбора NGFW
16. Какие объекты могут являться источниками событий ИБ?
17. Классификация систем мониторинга событий ИБ
18. Основные возможности систем мониторинга событий ИБ
19. Основные компоненты систем мониторинга событий ИБ
20. Исходные данные для правильной настройки системы мониторинга событий ИБ
21. Назначение системы анализа сетевого трафика в современных условиях
22. Основные логические компоненты системы анализа сетевого трафика
23. Недостатки существующих систем анализа сетевого трафика
24. Основные требования к системе анализа трафика
25. Основные методы анализа и мониторинга сетевого трафика
26. Основная задача решений класса Endpoint Detection and Response (EDR)
27. Какие технологии обнаружения угроз безопасности используются обычно в решениях EDR?
28. На какие типы угроз в основном ориентированы решения класса EDR?
29. Принцип работы EDR – агента
30. Варианты реализации средства обнаружения угроз ИБ на конечных устройствах, примеры.
31. Какие технологии включает в себя система анализа сетевого трафика нового поколения (NDR) ?
32. Что такое и чем характерны NTA-подсистемы с точки зрения анализа трафика, входящие в состав систем анализа сетевого трафика нового поколения (NDR) ?
33. Какие еще, кроме NTA-подсистем, входят в состав NDR?
34. Преимущество систем NDR по сравнению с традиционными системами анализа сетевого трафика
35. Варианты реализации систем NDR, примеры
36. Назначение систем учета и обработки информационных угроз Threat Intelligence Platform (TIP)
37. С каким типом специальных данных работают системы TIP?
38. С какими системами / подсистемами может интегрироваться система TIP?
39. Чем полезны системы  TIP для сетевых аналитиков?
40. Варианты реализации систем TIP, примеры.
41. Принцип действия и основная цель процесса поиска угроз (Threat hunting)
42. Основные элементы процесса threat hunting
43. За счет чего осуществляется проработка гипотез о вероятных угрозах при использовании процесса

threat hunting?
44. Что является важным элементом для поиска угроз, полезным для сетевого аналитика / аналитика ИБ?
45. Что является источниками данных, необходимых для работы процесса threat hunting?
46. Как еще не официально называются средства поведенческого анализа?
47. Назначение средств поведенческого анализа
48. Что моделируют средства поведенческого анализа?
49. В каких случаях использование средств поведенческого анализа наиболее актуально?
50. Для чего используется класс решений «Honeypot» (приманка для хакеров)
51. Что используется в качестве «приманки» в решениях «Honeypot»?
52. Что такое ханипот-ссылки и для чего они нужны?
53. Для кого могут быть особенно полезны решения «Honeypot»?
54. Дополнительные возможности ханипотов нового поколения, ориентированных для приманки более продвинутых злоумышленников
55. Что послужило стимулом для развития собственных (российских) решений в сфере обнаружения компьютерных атак?
56. Как учитываются и регистрируются новые отечественные разработки в области программного и аппаратного обеспечения для ИБ?
57. Какие льготы предоставляются ИТ-компаниям, производящим программное и аппаратное обеспечение для ИБ?
58. Проведение какой процедуры гарантирует отсутствие программных и аппаратных закладок для средств обеспечения ИБ?

*Примерный перечень тестовых заданий на экзамен:*

1. Выберите все верные утверждения:

Развитие техник и тактик атакующих, появление новых угроз и уязвимостей является драйвером развития технологий обнаружения компьютерных атак
Развитие технологий обнаружения компьютерных атак является драйвером развития техник и тактик атакующих, появление новых угроз и уязвимостей

2. Для систем обнаружения атак нового типа можно выделить следующие крупные уровни, на которых возможно осуществление доступа к обрабатываемой информации: выбрать все верные

Уровень прикладного ПО
Уровень СУБД
Уровень операционной системы
Уровень среды передачи
Уровень БД
Уровень драйверов

3. Какие из перечисленных технологий добавлены в NGFW по сравнению с традиционными? выбрать все верные

пакетная фильтрация трафика
контроль сетевых соединений
функции межсетевого экрана прикладного уровня
сигнатурный анализ трафика для обнаружения угроз и их блокирования
полнотекстовый анализ (инспекция) трафика, зашифрованного протоколами различного уровня +
поведенческий анализ файлов в изолированной среде
регулярные обогащения данными об актуальных угрозах

4. Основные компоненты систем мониторинга событий ИБ: выбрать все верные

программные агенты
сервер
хранилища информации
консоль
персонал, работающий с системой
регламенты работы по мониторингу
подсистема IPS

5. Системы анализа сетевого трафика (NTA) анализируют трафик:

на периметре
в ИТ-инфраструктуре
в обоих случаях

6. Какие технологии обнаружения угроз безопасности могут обычно использоваться в решениях EDR?: выбрать все верные

агента для сбора и анализа данных
средство антивирусной защиты с поведенческим анализом
анализ индикаторов компрометации
автоматическое взаимодействие с SIEM- и Threat Intelligence- системами для обогащения данными об угрозах
средство антивирусной защиты с сигнатурным анализом
межсетевой экран

7. Укажите все верные утверждения относительно подсистем NTA, входящих в состав системы анализа сетевого трафика нового поколения:

NTA работает с трафиком как на периметре, так и в ИТ-инфраструктуре
хранят информацию о сетевых взаимодействиях

8. Назначение систем учета и обработки информационных угроз Threat Intelligence Platform (TIP)

для обогащения, обнаружения, распространения и корреляции данных об угрозах
для анализа угроз в режиме реального времени
для анализа угроз на основе зафиксированных ранее событий

9. Основные элементы процесса threat hunting: выбрать все верные

Сбор данных
Аналитика
Исследование полученных данных
Нейтрализация атаки и разработка сценария реагирования на атаки

10. В каких случаях использование средств поведенческого анализа наиболее актуально?

для своевременного выявления потенциальных угроз
для отладки и испытания новых экспериментальных средств  обнаружения угроз безопасности ИС
для отладки и испытания любого ПО

11. Для кого могут быть особенно полезны решения «Honeypot»?

для пользователей, работающих в информационной системе
для системных администраторов и сетевых аналитиков
для специалистов, занимающихся поиском киберпреступников

12. Проведение какой процедуры гарантирует отсутствие программных и аппаратных закладок для средств обеспечения ИБ?

сертификация
аттестация
аккредитация

**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. Рочев, К. В. Информационные технологии. Анализ и проектирование информационных систем : учебное пособие / К. В. Рочев. — 2-е изд., испр. — Санкт-Петербург : Лань, 2019. — 128 с. — ISBN 978-5-8114-3801-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/122181 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Компьютерная криминалистика : лабораторный практикум : [16+] / авт.-сост. И. А. Калмыков, В. С. Пелешенко. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 84 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=466995 (дата обращения: 16.04.2026). – Библиогр. в кн. – Текст : электронный.

3. Компьютерная криминалистика : учебное пособие / составители И. А. Калмыков, В. С. Пелешенко. — Ставрополь : СКФУ, 2017. — 84 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155227 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

### 6.2 Дополнительная литература

1. Введение в защиту информации от внутренних ИТ-угроз : курс : учебное пособие : [16+] / Национальный открытый университет «ИНТУИТ». – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2007. – 32 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=234901 (дата обращения: 15.04.2026). – Текст : электронный.

2. Кияев, В. Безопасность информационных систем : курс : учебное пособие : [16+] / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429032 (дата обращения: 16.04.2026). – Текст : электронный.

### 6.3 Методическая литература

1. Методические рекомендации по организации учебной деятельности обучающихся КузГТУ / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. приклад. информ. технологий ; сост. Л. И. Михалева. – Кемерово : КузГТУ, 2017. – 32 с. – URL: http://library.kuzstu.ru/meto.php?n=553 (дата обращения: 23.03.2026). – Текст : электронный.

### 6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
3. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
4. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
5. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
6. Национальная электронная библиотека https://rusneb.ru/
7. Электронная библиотека http://library.gorobr.ru/

### 6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646
2. Защита информации. Инсайд: информационно-методический журнал https://eivis.ru/browse/publication/122426
3. 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 обнаружения угроз безопасности 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 обнаружения угроз безопасности информационных систем", включая перечень программного обеспечения и информационных справочных систем**

Для изучения дисциплины может использоваться следующее программное обеспечение:

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

**10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Методы обнаружения угроз безопасности**

**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.