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

Информационные угрозы

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 "Информационные угрозы", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-5 - Способен определять оценки возможностей реализации угрозы внешних и внутренних нарушителей

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Определяет оценки возможностей внешних и внутренних нарушителей.

Результаты обучения по дисциплине:

Знать эталонную модель взаимодействия открытых систем. Знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах.

Уметь составлять перечень угроз.

Владеть методами обнаружения информационных угроз.

2 Место дисциплины "Информационные угрозы" в структуре ОПОП специалитета

Для освоения дисциплины необходимо владеть знаниями умениями, навыками, полученными в рамках среднего общего образования и (или) среднего специального и (или) дополнительного профессионального образования.

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 "Информационные угрозы" 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 "Информационные угрозы" составляет 5 зачетных единиц, 180 часов.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 1/Семестр 1			
Всего часов	180		
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		
Самостоятельная работа	80		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Информационные угрозы", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Источники и виды угроз информационной безопасности, их классификация.	1
2. Методы оценки уязвимости информации.	1
3. Криминалистическая характеристика компьютерных преступлений	1
4. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов	1
5. Основные элементы канала реализации угрозы безопасности информации.	1
6. Проблемы роста преступлений в электронной сфере.	1
7. Компьютерный терроризм.	1
8. Промышленный шпионаж.	1
9. Методика оценки угроз информационной безопасности.	1
10. Ошибки администрирования сетей.	1
11. Объекты и направления информационного нападения на проводные средства связи.	1
12. Уязвимость цифровых сетей предприятия.	1
13. Социальная инженерия – информационная угроза обществу.	1
14. Компьютерные вирусы	1
15. Результаты последних крупных кибератак и атак хакеров. Практика раскрытия и расследования компьютерных преступлений	1
16. Тренды и вероятные сценарии развития в сфере информационных угроз.	1
Итого	**16**

4.2. Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах
	ОФ
1. Составление перечня угроз для заданного предприятия в определенной предметной области	2
2. Расчет оценки уязвимости информации заданного типа	2
3. Составление классификация компьютерных преступлений по степени ущерба	2
4. Составление классификации дестабилизирующих факторов по степени ущерба нормальной работе предприятия	2

5. Составление перечня каналов реализации угрозы безопасности для заданного предприятия	2
6. Проблемы роста преступлений в электронной сфере	2
7. Компьютерный терроризм	2
8.Промышленный шпионаж	2
9. Расчет вероятности осуществления угроз ИБ для заданного предприятия	2
10. Составление перечня ошибок администрирования ИС, создающих потенциальную угрозу ИБ. Расположение в порядке возрастания ущерба.	2
11. Составление и классификация объектов и направлений информационного нападения на проводные средства связи для заданного предприятия	2
12. Оценка уязвимости цифровых сетей предприятия	2
13. Составление перечня психологического воздействия на человека методами социальной инженерии.	2
14. Классификация компьютерных вирусов и степень ущерба от них.	2
15. Результаты последних крупных кибератак и атак хакеров. Практика раскрытия и расследования компьютерных преступлений	2
16. Тренды и вероятные сценарии развития в сфере информационных угроз.	2
Итого	**32**

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

Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	40
Оформление отчетов по практическим и(или) лабораторным работам	34
Подготовка к промежуточной аттестации	6
Итого	**80**
Экзамен	**36**
Самостоятельная работа под руководством преподавателя	16

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Информационные угрозы"

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-5	Определяет оценки возможностей внешних и внутренних нарушителей	**Знать** эталонную модель взаимодействия открытых систем. Знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. **Уметь** составлять перечень угроз. **Владеть** методами обнаружения информационных угроз	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:

Тема 1. Источники и виды угроз информационной безопасности, их классификация.

1. Перечислите основные источники угроз ИБ
2. Перечислите основные виды угроз ИБ
3. Что является критерием для классификации источников угроз?
4. Что является критерием для классификации видов угроз?
5. Дайте определение угрозе ИБ

Тема 2. Методы оценки уязвимости информации.

1. Перечислите основные методы оценки уязвимости информации
2. Какая шкала используется для оценки уязвимости информации?
3. На чем основаны большинство методов оценки уязвимости информации?
4. Какие средства необходимы для оценки уязвимости информации?
5. Кто уполномочен проводить оценку уязвимости информации?

Тема 3. Криминалистическая характеристика компьютерных преступлений

1. Перечислите основные виды компьютерных преступлений
2. Для чего дается криминалистическая характеристика компьютерных преступлений?
3. Какие параметры включаются в криминалистическую характеристику компьютерных преступлений?
4. Какая шкала используется в криминалистической характеристике компьютерных преступлений?
5. Какие меры наказаний существуют за совершение компьютерных преступлений?

Тема 4. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов

1. Перечислите виды факторов, которые могут воздействовать на защищаемую информацию.
2. Отчего зависит эффективность дестабилизирующего фактора по отношению к той или иной информации?
3. Какие существуют методы защиты от некоторых дестабилизирующих факторов?
4. Возможно ли одновременное влияние нескольких дестабилизирующих факторов?
5. Возможно ли в каких-то случаях восстановить информацию после воздействия дестабилизирующих факторов?

Тема 5. Основные элементы канала реализации угрозы безопасности информации.

1. Перечислите основные каналы реализации угрозы безопасности информации
2. Какие элементы каналов реализации угрозы безопасности информации наиболее уязвимы и требуют усиленной защиты?
3. Приведите пример каналов реализации угрозы безопасности информации, в которых вероятность реализации угрозы наименьшая
4. Какие существуют методы и принципы минимизации каналов угроз безопасности информации?
5. Каким образом выявляются каналы угроз безопасности информации?

Тема 6. Проблемы роста преступлений в электронной сфере.

1. Чем обусловлен рост преступлений в электронной сфере?
2. Что способно снизить рост преступлений в электронной сфере?
3. Приведите категории преступлений в электронной сфере.
4. Какие существуют категории борьбы с преступлениями в электронной сфере?
5. Что является мотивом для лиц, совершающих преступления в электронной сфере?

Тема 7. Компьютерный терроризм.

1. каковы цели компьютерного терроризма?
2. Кто и что является объектом компьютерного терроризма?
3. Каковы последствия компьютерного терроризма?
4. Каковы каналы и условия для осуществления компьютерного терроризма?

5. Какие существуют (если существуют) наказания за компьютерный терроризм согласно законам РФ?

Тема 8. Промышленный шпионаж.

1. Кто или что является объектом промышленного шпионажа?
2. Кто заинтересован в совершении промышленного шпионажа?
3. Каковы каналы и условия для осуществления промышленного шпионажа?
4. Какие средства могут использоваться для промышленного шпионажа?
5. Какие существуют (если существуют) наказания за компьютерный терроризм согласно законам РФ?

Тема 9. Методика оценки угроз информационной безопасности.

1. Перечислите основные методы оценки угроз информационной безопасности
2. Какая шкала используется для оценки угроз информационной безопасности?
3. На чем основаны большинство методов оценки угроз информационной безопасности?
4. Какие средства необходимы для оценки угроз информационной безопасности?
5. Кто уполномочен проводить оценку угроз информационной безопасности?

Тема 10. Ошибки администрирования сетей.

1. Какие типы ошибок администрирования сетей создают угрозу ИБ?
2. Какие типы угроз наиболее сильно зависят от ошибок администрирования сетей?
3. Какие программные инструменты позволяют минимизировать количество ошибок администрирования сетей?
4. Сети какого типа при ошибках администрирования сетей наиболее подвержены угрозам ИБ?
5. К каким последствиям могут привести ошибки администрирования сетей в случае осуществления угрозы (атаки)?

Тема 11. Объекты и направления информационного нападения на проводные средства связи.

1. Что является объектом информационного нападения посредством проводных средств связи?
2. Какие типы информационных нападений возможно реализовать посредством проводных средств связи?
3. Чем обусловлена возможность совершения некоторых типов нападения через проводные средства связи?
4. Какие признаки служат фактом совершения информационного нападения посредством проводных средств связи?
5. К каким последствиям могут привести информационные нападения посредством проводных средств связи?

Тема 12. Уязвимость цифровых сетей предприятия.

1. Какие типы цифровых сетей предприятия наиболее уязвимы с точки зрения ИБ?
2. В чем состоит уязвимость цифровых сетей предприятия?
3. Какие существуют методы и средства снижения уязвимости цифровых сетей предприятия?
4. Какие объекты цифровых сетей предприятия являются наиболее уязвимыми?
5. Зависит ли степень уязвимости цифровых сетей предприятия от конкретной сетевой технологии?

Тема 13. Социальная инженерия – информационная угроза обществу.

1. В чем заключаются основные цели социальной инженерии?
2. Какие методы и принципы использует социальная инженерия?
3. Что может являться защитой от угроз, сформированных методами социальной инженерии?
4. Является ли социальная инженерия противозаконным методом взаимодействия между людьми?
5. Приведите примеры преступлений, совершаемых с помощью социальной инженерии?

Тема 14. Компьютерные вирусы

1. Что представляет собой компьютерный вирус?
2. На какие типы / категории подразделяются компьютерные вирусы?
3. Какие типы вирусов наиболее опасны?
4. Какие меры необходимо предпринимать периодически для минимизации вирусного воздействия?
5. Всегда ли вирус может быть обнаружен антивирусной программой?

Тема 15. Результаты последних крупных кибератак и атак хакеров. Практика раскрытия и расследования компьютерных преступлений

1. Приведите примеры наиболее известных кибератак за последние 5 лет
2. Какие средства используются для расследования компьютерных преступлений?

3. Какими методами хакерам удавалось совершить компьютерные преступления?

4. Каков процент раскрытия компьютерных преступлений от общего числа?

5. К какому ущербу привели наиболее известные компьютерные преступления за последние 5 лет?

Тема 16. Тренды и вероятные сценарии развития в сфере информационных угроз.

1. Какие предполагаемые тренды в сфере информационных угроз можно ожидать в ближайшие 5 лет?

2. Какие сценарии развития в сфере информационных угроз наиболее вероятны в ближайшие 5 лет?

3. На какие методы защиты от угроз нужно делать акцент в ближайшие 5 лет?

4. Возможно ли создать систему защиты от угроз работающую на опережение киберпреступников?

5. Какова ожидаемая динамика роста киберпреступлений в ближайшие 5 лет?

Примерный перечень тестовых заданий:

Тема 1. Источники и виды угроз информационной безопасности, их классификация.

1. Основными источниками угроз информационной безопасности являются все указанное в списке:

Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

2. Наиболее распространены угрозы информационной безопасности корпоративной системы:

Покупка нелицензионного ПО
Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов

3. Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных

Тема 2. Методы оценки уязвимости информации.

1. Какая модель нарушителя используется для количественных оценок уязвимости объекта и эффективности охраны?

количественная
математическая
косвенная
содержательная

2. Обычно для оценки угроз и уязвимостей используются различные методы, в основе которых могут лежать: (выбрать все верные)

Экспертные оценки.
Статистические данные.
Учет факторов, влияющих на уровни угроз и уязвимостей
Математические
Физические
информационные

3. Уязвимости должны быть отсортированы:

В начале отчета сначала по степени важности, а затем по серверам/сервисам
В конце отчета сначала по серверам/сервисам, затем по степени важности
В начале отчета сначала по серверам/сервисам, затем по степени важности
В конце отчета сначала по степени важности, а затем по серверам/сервисам

Тема 3. Криминалистическая характеристика компьютерных преступлений

1. Согласно ст. 20 Закона “Об информации, информатизации и защиты информации” РФ,

информация как объект информационного преступления может быть подвержена: (выбрать все верные)

утечке,
хищению
утрате,
искажению,
подделке,
уничтожению,
модификации,
копированию,
блокированию.

2. Основные криминалистические особенности компьютерной информации заключаются в следующем: (выбрать все верные)

она достаточно просто и быстро преобразуется из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств электросвязи;
при изъятии компьютерной информации, в отличие от изъятия материального предмета (вещи), она сохраняется в первоисточнике, т.к. доступ к ней могут одновременно иметь несколько лиц, например, при работе с информацией, содержащейся в одном файле, доступ к которому одновременно имеют несколько пользователей сети ЭВМ.
для нее невозможно определить первоисточник (владельца)

3. Компьютерные преступления -это

предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства
представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных
процесс внедрения вредоносной программы с целью нарушения работы ПК.
Создание множества аккаунтов в соцсетях
Использование торрентов

Тема 4. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов

1. К условиям, создающим возможность для дестабилизирующего воздействия на информацию, можно отнести: (выбрать все верные)

недостаточность мер, принимаемых для защиты информации, в том числе из-за недостатка ресурсов;
недостаточное внимание и контроль со стороны администрации вопросам защиты информации;
принятие решений по производственным вопросам без учета требований по защите информации;
плохие отношения между сотрудниками и сотрудников с администрацией.
пиратское ПО или некачественное сетевое оборудование или его настройка

2. источники дестабилизирующего воздействия на информацию. К ним относятся: выбрать все верные

Люди;
Технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи;
Системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации;
Технологические процессы отдельных категорий промышленных объектов;
Природные явления.
Экономические ситуация и явления

3. Способами непосредственного воздействия на носители защищаемой информации могут быть: выбрать все верные

физическое разрушение носителя (поломка, разрушение и др.);

создание аварийных ситуаций для носителей (поджог, искусственное затопление, взрыв и т. д.);
удаление информации с носителей;
создание искусственных магнитных полей для размагничивания носителей;
внесение фальсифицированной информации в носители.

Тема 5. Основные элементы канала реализации угрозы безопасности информации.

1. Каналы проникновения в систему и утечки информации, которые могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов, принято называть …

пассивными
активными
прямыми
косвенными

2. Бесконтактный несанкционированный доступ реализуется посредством

программно-математических каналов проникновения и утечки
физических каналов проникновения и утечки
электромагнитных каналов проникновения и утечки

3. Какие сетевые каналы являются наиболее доступными для реализации угрозы безопасности информации (выбрать все верные)

Сеть Wi-Fi
Проводная локальная сеть
Сотовая сеть
Спутниковая сеть

Тема 6. Проблемы роста преступлений в электронной сфере.

1. Какие факторы создают почву для совершения преступлений в электронной сфере? Выбрать все верные

большая уверенность в ненаказуемости за данный вид преступления из-за отсутствия эффективных методов борьбы с ними со стороны правоохранительных органов
доступность средств, методов и знаний для совершения данных преступлений
низкий уровень защиты закрытых ведомственных и банковских сетей
низкий уровень информационной культуры у большинства граждан
развитие социальной инженерии

2. Какие факторы снижают эффективность раскрытия киберпреступлений со стороны правоохранительных органов? Выбрать все верные

не хватает подготовленных в ИТ сотрудников
отсутствуют методики расследования инновационных преступлений
нет надежных и эффективных информационно-аналитических решений
отсутствует принципиально новая система криминалистического учета и идентификации в киберпространстве
коррумпированность правоохранительных органов
слишком низкая зарплата правоохранительных органов и нежелание расследовать данный вид преступлений

3. Во сколько раз увеличилось в мире количество киберпреступлений за период 2013 по 2019 год?

в 5 раз
в 10 раз
в 25 раз
в 35 раз

Тема 7. Компьютерный терроризм.

1. Цели кибертерроризма выбрать все верные

- взлом компьютерных систем и получение доступа к личной и банковской информации, военным и государственным конфиденциальным данным;

вывод из строя оборудования и программного обеспечения, создание помех, нарушение работы сетей электропитания;
кража данных с помощью взлома компьютерных систем, вирусных атак, программных закладок;
утечка секретной информации в открытый доступ;
распространение дезинформации с помощью захваченных каналов СМИ;
нарушение работы каналов связи;
проверка информационных систем на предмет ИБ

2. компьютерный терроризм это:

Преступные действия, связанные с использованием или угрозами использования локальных и глобальных компьютерных сетей в террористических целях.
Особая форма насилия, представляющая собой сознательное и целенаправленное информационное воздействие для принуждения правительства к реализации политических, экономических, религиозных и иных целей террористов.

3. Источники и признаки информационного терроризма определены в:

Конвенции ООН о защите прав человека
Совместном всеобъемлющем плане действий» (СВПД) Ирана и группы государств «51» (России, США, Великобритании, Франции, КНР и Германии)
Соглашении между Правительствами государствами-членами Шанхайской организации сотрудничества

Тема 8. Промышленный шпионаж.

1. В защите от промышленного шпионажа нуждаются…

Только руководители фирмы
Только помещения фирмы (компании, организации)
Планы на будущее, информация, работники, идеи (интеллектуальная собственность), объекты и оборудование
Только носители информации

2. Смысл шпионажа — информация. Это означает, что…

В демократическом обществе все должны знать все и обо всех
Информация делает нас умнее других
Чем больше мы имеем информации о конкурентах, тем более правильные решения можем принимать
Чем больше у нас информации — тем мы сильнее

3. Защитно-оборонная сторона шпионажа — это…

Средства, используемые организацией для самозащиты от утечки
Создание системы ограниченного доступа к документам
Информации и нанесения ей ущерба конкурентами/врагами
Защита компьютерных сетей от внешнего проникновения

Тема 9. Методика оценки угроз информационной безопасности.

1. Что является наилучшей методикой оценки угроз ИБ на основе описания количественного анализа рисков?

Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
Метод, основанный на суждениях и интуиции

2. Какая формула в методике оценки угроз ИБ на основе расчета остаточного риска является верной?

Угрозы х Риски х Ценность актива
(Угрозы х Ценность актива х Уязвимости) х Риски
SLE х Частоту = ALE
(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

3. В методике оценки угроз ИБ на основе качественного подхода степень угрозы измеряется в терминах

денежных потерь
заданных с помощью шкалы или ранжирования
оценок экспертов
объема информации

Тема 10. Ошибки администрирования сетей.

1. При какой ошибке администрирования злоумышленник может исправить одну из запускаемых программ?

не запрет записи в один из каталогов, используемых в файле начальной загрузки (loginscript)
наличие у пользователя права на чтение SYS:SYSTEM

2. Для администратора баз данных недопустимо забывать и игнорировать: выбрать все верные

тестировании резервных копий
не принимать меры по ограничению доступа в целях обеспечения безопасности
пренебрегать плановыми мероприятиями по обслуживанию баз данных
откладывать мониторинг использования сервера

3. К чему может привести привычка администратора выполнять все административные действия на ОС Linux, работающей в качестве сервера под учетной записью Root? выбрать все верные

к удалению любого каталога, в т.ч. и системного
к повышенной уязвимости ОС и всей сети, которой она управляет
к удалению / изменению любой информации на сервере, указанной администратором

Тема 11. Объекты и направления информационного нападения на проводные средства связи.

1. Основными направлениями информационного нападения через проводные средства связи извне являются: выбрать все верные

доступ в локальную сеть со стороны штатного персонального компьютера
доступ в локальную сеть со стороны кабельных линий связи

2. Несанкционированный доступ в локальных сетях со стороны кабельных линий может произойти по следующим каналам: выбрать все верные

со стороны штатного пользователя-нарушителя одного персонального компьютера при обращении к информации другого, в том числе файл-серверу;
при подключении постороннего персонального компьютера и другой посторонней аппаратуры;
при побочных электромагнитных излучениях и наводках информации.
со стороны оператора связи через внешнюю сеть и входной шлюз организации

3. Какие элементы проводных средств связи (сетей) могут являться объектами атак и информационных нападений выбрать все верные

Активное коммуникационное оборудование
Пассивное коммуникационное оборудование
Офисные АТС
Сетевые адаптеры серверов и рабочих станций
Сетевое периферийное оборудование
Сеть и оборудование пожарно-охранной сигнализации

Тема 12. Уязвимость цифровых сетей предприятия.

1. Ключевыми механизмами ИС, от которых зависит уязвимость цифровых сетей предприятия являются: выбрать все верные

идентификация и аутентификация;
управление доступом;
протоколирование и регистрация;
криптография и сетевая защита;
экранирование

архивация данных

2. Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют: выбрать все верные

увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации;
сосредоточение в базах данных информации различного уровня важности и конфиденциальности;
расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети;
увеличение числа удаленных рабочих мест;
широкое использование глобальной сети Internet и различных каналов связи;
автоматизация обмена информацией между компьютерами пользователей.
Низкая информационная культура пользователей
Ненадежность Интернет-провайдера

3. по статистике от компании Trustwave в 2013 году в первую тройку уязвимостей попали: выбрать все верные

Недостаточная сложность пароля системного администратора
Передача критичных данных в незашифрованном виде
Недостаточная сложность пароля доступа к БД
Использование слабого механизма аутентификации в ОС Windows
Ошибки настройки межсетевого экрана, защищающего периметр
Доступ к системам/хранилищам, содержащим критичные данные

Тема 13. Социальная инженерия – информационная угроза обществу.

1. Какие каналы для воздействия на человека методом социальной инженерии используются чаще всего: выбрать все верные

Телефон
Почтовые спам-рассылки
Смс-сообщения
Личный контакт
Реклама
СМИ

2. Социальная инженерия это:

Совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним.
Психологическое манипулирование человека, с помощью которого заставляют делать то, что он делать не должен или не собирался.
Все ответы верны.
Метод управления действиями человека, основанный на использовании слабостей человеческого фактора для получения закрытой информации, или информации, которая представляет большую ценность.

3. Объектом воздействия в методах социальной инженерии являются: выбрать все верные

человек
человек или его домашнее животное
компьютерная техника
коммуникационное оборудование

Тема 14. Компьютерные вирусы

1. Основные типы компьютерных вирусов:

Аппаратные, программные, загрузочные.
Программные, загрузочные, макровирусы.
Файловые, программные, макровирусы.

2. Этапы действия программного вируса:

Размножение, вирусная атака.
Запись в файл, размножение.
Запись в файл, размножение, уничтожение программы.

3. Что называется вирусной атакой?

Неоднократное копирование кода вируса в код программы.
Отключение компьютера в результате попадания вируса.
Нарушение работы программы, уничтожение данных, форматирование жесткого диска.

Тема 15. Результаты последних крупных кибератак и атак хакеров. Практика раскрытия и расследования компьютерных преступлений

1. При расследовании преступлений в сфере компьютерной информации подлежат выявлению следующие обстоятельства

все ответы правильные
характер и размер причиненного вреда
способ совершения преступлений
кто имеет доступ к информации, содержащейся в ЭВМ

2. Какое из перечисленных следственных действий не является типичным для расследования преступлений в сфере компьютерной информации

назначение судебных экспертиз
проверка показаний на месте
выемка и осмотр предметов и документов
обыск
допрос свидетелей

3. какой из перечисленных случаев кибератак оказался самым масштабным?

Maroochy Water System
Светофоры в Лос-Анджелесе
Трамвайная сеть в Лодзе
Stuxnet

Тема 16. Тренды и вероятные сценарии развития в сфере информационных угроз.

1. По прогнозам исследователей, развитие каких технологий приведет к возникновению абсолютно безопасной коммуникации?

Системы прокси-серверов
Квантовый компьютер
Облачные вычисления
Темные паттерны

2. Какие угрозы ИБ попадают в ТОП-3 в ближайшие несколько лет с наибольшей вероятностью? Выбрать все верные

атаки шифровальщиков;
атаки на удалённых сотрудников и переснальный фишинг
атак на инфраструктуру интернета вещей
телефонное мошенничество
атаки сетей 5G

3. Какие меры противодействия киберугрозам наиболее вероятно попадают в ТОП-3 в ближайшие несколько лет? Выбрать все верные

Сети кибербезопасности
Повышение внимания руководителей предприятий к вопросам ИБ и увеличение бюджета на эти цели
Поддержка безопасности удаленной работы
Киберпространственный совет директоров
Объединение поставщиков средств безопасности
Вычисления, повышающие конфиденциальность

Моделирование взлома и атаки
Управление идентификационными данными машин

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

Формой промежуточной аттестации является экзамен, 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 зачете 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	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 2 0вопросов;
- 85…99 баллов – при правильном ответе на 17-19 вопросов;
- 75…84 баллов – при правильном ответе на 13-16 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	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень вопросов на экзамен:

1. Понятие уязвимости и угрозы информации.
2. Источники утраты конфиденциальности и искажения информации.
3. Классификация противоправных способов получения конфиденциальной информации. Понятие шпионажа и его виды.
4. Понятие преступления в информационной сфере. Характеристика основных составов преступлений, связанных с информационными отношениями.
5. Анализ и оценка угроз информационной безопасности объекта.

6. Виды угроз информационной безопасности, исходящих по техническим каналам.
7. Угрозы безопасности информации в процессе использования компьютеров, локальных сетей и средств связи.
8. Расчёт остаточного риска при реализации информационной угрозы
9. Естественные угрозы безопасности информации
10. Искусственные угрозы безопасности информации
11. Непреднамеренные искусственные угрозы безопасности информации
12. Принцип работы фишинга
13. Принцип работы фарминга
14. Активный перехват информации
15. DoS атака
16. Классификация угроз информационной безопасности
17. Информационные угрозы, их виды и причины возникновения.
18. Информационные угрозы для государства.
19. Информационные угрозы для компании.
20. Информационные угрозы для личности (физического лица).
21. Действия и события, нарушающие информационную безопасность.
22. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
23. Способы воздействия информационных угроз на объекты.
24. Внешние и внутренние субъекты информационных угроз.
25. Компьютерные преступления и их классификация
26. Вредоносные программы, их виды.
27. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
28. Классификация кибератак
29. Анализ угроз информационной безопасности. Виды «нарушителей»
30. Виды угроз информационной безопасности Российской Федерации

Примерный перечень тестовых заданий на экзамен:

1. Какие элементы проводных средств связи (сетей) могут являться объектами атак и информационных нападений выбрать все верные

Активное коммуникационное оборудование
Пассивное коммуникационное оборудование
Офисные АТС
Сетевые адаптеры серверов и рабочих станций
Сетевое периферийное оборудование
Сеть и оборудование пожарно-охранной сигнализации

2. Социальная инженерия это:

Совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним.
Психологическое манипулирование человека, с помощью которого заставляют делать то, что он делать не должен или не собирался.
Все ответы верны.
Метод управления действиями человека, основанный на использовании слабостей человеческого фактора для получения закрытой информации, или информации, которая представляет большую ценность.

3. Основные типы компьютерных вирусов:

Аппаратные, программные, загрузочные.
Программные, загрузочные, макровирусы.

4. При расследовании преступлений в сфере компьютерной информации подлежат выявлению следующие обстоятельства

все ответы правильные

характер и размер причиненного вреда
способ совершения преступлений
кто имеет доступ к информации, содержащейся в ЭВМ

5. Какое из перечисленных следственных действий не является типичным для расследования преступлений в сфере компьютерной информации

назначение судебных экспертиз
проверка показаний на месте
выемка и осмотр предметов и документов
обыск
допрос свидетелей

6. Какие угрозы ИБ попадают в ТОП-3 в ближайшие несколько лет с наибольшей вероятностью? Выбрать все верные

атаки шифровальщиков;
атаки на удалённых сотрудников и персональный фишинг
атак на инфраструктуру интернета вещей
телефонное мошенничество
атаки сетей 5G

7. Какие меры противодействия киберугрозам наиболее вероятно попадают в ТОП-3 в ближайшие несколько лет? Выбрать все верные

Сети кибербезопасности
Повышение внимания руководителей предприятий к вопросам ИБ и увеличение бюджета на эти цели
Поддержка безопасности удаленной работы
Киберпространственный совет директоров
Объединение поставщиков средств безопасности
Вычисления, повышающие конфиденциальность
Моделирование взлома и атаки
Управление идентификационными данными машин

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. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.

2. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628 (дата обращения: 27.03.2026). – Режим доступа: по подписке.

3. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / Зенков А. В.. – 2-е изд., пер. и доп. – Москва : Юрайт, 2025. – 107 с. – ISBN 978-5-534-16388-9. – URL: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-567915 (дата обращения: 23.03.2026). – Текст : электронный.

4. Щербак, А. В. Информационная безопасность: учебник для вузов / Щербак А. В.. – 2-е изд. –

Москва : Юрайт, 2025. – 252 с. – ISBN 978-5-9916-4299-6. – URL: https://urait.ru/book/informacionnaya-bezopasnost-569267 (дата обращения: 23.03.2026). – Текст : электронный.

5. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2025. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2178344 (дата обращения: 27.03.2026). – Режим доступа: по подписке.

6.2 Дополнительная литература

1. Загинайлов, Ю. Н. Основы информационной безопасности : курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=362895 (дата обращения: 16.04.2026). – Библиогр. в кн. – ISBN 978-5-4475-3947-4. – DOI 10.23681/362895. – Текст : электронный.

2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : практическое пособие : [16+] / А. Е. Фаронов. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 138 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=233763 (дата обращения: 15.04.2026). – Текст : электронный.

3. Чернова, Е. В. Информационная безопасность человека: учебник для вузов / Чернова Е. В.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2025. – 327 с. – ISBN 978-5-534-16772-6. – URL: https://urait.ru/book/informacionnaya-bezopasnost-cheloveka-566457 (дата обращения: 23.03.2026). – Текст : электронный.

4. Суворова, Г. М. Информационная безопасность: учебник для вузов / Суворова Г. М.. – 2-е изд., пер. и доп. – Москва : Юрайт, 2025. – 277 с. – ISBN 978-5-534-16450-3. – URL: https://urait.ru/book/informacionnaya-bezopasnost-567672 (дата обращения: 23.03.2026). – Текст : электронный.

6.3 Методическая литература

1. Основы информационной безопасности : методические материалы для обучающихся по 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. – Кемерово : КузГТУ, 2018. – 25 с. – URL: http://library.kuzstu.ru/meto.php?n=4603 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. База данных Springer Materials http://materials.springer.com/
2. База данных zbMath https://zbmath.org/
3. Цифровая библиотека IPRsmart https://ipr-smart.ru/
4. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
5. Электронная библиотечная система «Лань» http://e.lanbook.com
6. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
7. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
8. Образовательная платформа «Юрайт» https://urait.ru/
9. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
10. Национальная электронная библиотека https://rusneb.ru/
11. Базы данных Springer Journals, Springer eBooks https://link.springer.com/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646
2. Информация и безопасность : научный журнал
3. Прикладная информатика : научно-практический журнал https://eivis.ru/browse/publication/66410

4. Статистика и экономика (До №5 2016 г. Экономика, статистика и информатика) : научно-практический 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 "Информационные угрозы"

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 "Информационные угрозы", 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 "Информационные угрозы"

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.