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

Управление информационной безопасностью

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 "Управление информационной безопасностью", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем

Результаты обучения по дисциплине:

Знать базовые понятия и подходы к управлению информационной безопасностью; международные и российские стандарты по УИБ; политика и ресурсное обеспечение ИБ организации.

Уметь анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ.

Владеть современными методами и средствами разработки процессов управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность.

2 Место дисциплины "Управление информационной безопасностью" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Безопасность операционных систем, Безопасность систем баз данных, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Сети и системы передачи информации, 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 "Управление информационной безопасностью" 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 "Управление информационной безопасностью" составляет 4 зачетных единицы, 144 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 4/Семестр 7			
Всего часов	144		
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	26		

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Самостоятельная работа	54		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Управление информационной безопасностью", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Базовые понятия и подходы к управлению информационной безопасностью (УИБ)	6
2. Международные и российские стандарты по УИБ	6
3. Политика ИБ организации	6
4. Система управления информационной безопасностью организации (СУИБ)	6
5. Ресурсное обеспечение СУИБ	4
6. Контроль и проверка процессов УИБ	4
Итого	**32**

4.2 Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах
	ОФ
1. Базовые понятия и подходы к управлению информационной безопасностью	2
2. Международные и российские стандарты по УИБ	6
3. Политика ИБ организации	6
4. Система управления информационной безопасностью организации (СУИБ)	6
5. Ресурсное обеспечение СУИБ	6
6. Контроль и проверка процессов УИБ	2
7. Документационное обеспечение СУИБ	4
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	20
Оформление отчетов по практическим и(или) лабораторным работам	28
Подготовка к промежуточной аттестации	6
Итого	**54**
Самостоятельная работа под руководством преподавателя	26

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Управление информационной безопасностью"

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	ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем	**Знать** базовые понятия и подходы к управлению информационной безопасностью; международные и российские стандарты по УИБ; политика и ресурсное обеспечение ИБ организации. **Уметь** анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ. **Владеть** современными методами и средствами разработки процессов управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность.	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. Базовые понятия и подходы к управлению информационной безопасностью (УИБ)

1. Объекты управления в системе ИБ
2. Методики и технологии управления рисками в сфере ИБ
3. Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика.
4. Понятие «Управление информационной безопасностью»
5. Модели безопасности. Управление доступом

2. Международные и российские стандарты по УИБ

1. Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования»
2. Сертификация СУИБ на соответствие ISO 27001
3. Стандарты управления информационной безопасность BS 7799 и ISO/IEC 17799. Их основные положения.
4. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.
5. Российские стандарты управления ИБ: ГОСТ Р ИСО/МЭК 27002-2012 "Свод норм и правил менеджмента информационной безопасности" и ГОСТ Р ИСО/МЭК 17799-2005 "Практические правила управления информационной безопасностью"

3. Политика ИБ организации

1. Основные вопросы, рассматриваемые в политике ИБ организации
2. Назначение и правовая основа политики информационной безопасности

3. Принципы формирования политики информационной безопасности на объектах информатизации
4. Нормативные документы для разработки политики ИБ организации
5. Понятие политики ИБ

4. Система управления информационной безопасностью организации (СУИБ)

1. Приведите пример наиболее известных методик управления рисками в контексте ИБ
2. Основные этапы разработки системы управления ИБ
3. Роль руководства компании в системе управления ИБ
4. Основные компоненты системы управления ИБ
5. Частью какого подхода является процесс управления ИБ?

5. Ресурсное обеспечение СУИБ

1. Какие виды ресурсов необходимы для обеспечения СУИБ?
2. Приведите пример (номер) документа, в котором подробно описывается ресурсное обеспечение СУИБ банковской системы РФ
3. Назовите ГОСТ, в котором описывается общий обзор и методология системы управления ИБ
4. Что такое COBIT ?
5. Назовите главный вид ресурсного обеспечения для создания СУИБ

6. Контроль и проверка процессов УИБ

1. Назовите основной международный стандарт по управлению информационной безопасностью (УИБ).
2. Основные методики контроля и проверки системы УИБ
3. Основные средства контроля и проверки системы УИБ
4. Основные критерии корректности работы системы УИБ
5. Оформление и документирование результатов проведения проверки процессов УИБ

Примерный перечень тестовых заданий:

1. Базовые понятия и подходы к управлению информационной безопасностью (УИБ)

1. Основной целью управления является обеспечение эффективного управления информационной безопасностью всех услуг и деятельностей в рамках Управления услуг за счет: выбрать все верные

конфиденциальность
целостность
доступность
актуальность
оперативность

2. Политика информационной безопасности должна включать в себя следующее: выбрать все верные

реализация аспектов Политики информационной безопасности;
возможные злоупотребления аспектами Политики информационной безопасности;
политика контроля доступа;
политика Интернета

3. Лица, которые обязаны ознакомиться с политикой информационной безопасности, отвечают за исполнение политики, процедур и стандартов информационной безопасности:

владельцы информации
хранители информации
пользователи информации

2. Международные и российские стандарты по УИБ

1. Выберите наиболее подходящий ответ на вопрос «Что такое стандарты информационной безопасности?»

система официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере
документация, определяющая высокоуровневые цели, содержание и основные направления

деятельности по обеспечению ИБ, предназначенная для организации в целом
обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным ИС
свойство ИБ организации сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах

2. Какие категории требований безопасности указаны в «Оранжевой книге»: выбрать все верные

политика ИБ
аудит ИБ
корректность работы средств защиты
политика доступа к информации
политика паролей

3. Какой из стандартов описывает практические правила управления информационной безопасностью

ISO/IEC 15408
ГОСТ Р ИСО/МЭК 17799:2005
ГОСТ Р ИСО/МЭК 27001-2006

3. Политика ИБ организации

1. Принципом политики информационной безопасности является принцип:

Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

2. Политика безопасности в системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети

3. Наиболее важным при реализации защитных мер политики безопасности является:

Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций +

4. Система управления информационной безопасностью организации (СУИБ)

1. Согласно ГОСТ Р ИСО/МЭК 27000 ключевыми компонентами системы управления информационной безопасности являются: выбрать все верные

Локальные нормативные акты (ЛНА)
Сотрудники с определенными должностными обязанностями
Процессы управления
аппаратное обеспечение
программное обеспечение
бизнес-процессы организации

2. Основные функции систем управления информационной безопасностью (СУИБ) — это: выбрать все верные

выявление и анализ рисков информационной безопасности
планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ
контролирование этих процессов, направленных на минимизацию рисков ИБ
построение оптимальной политики ИБ предприятия

3. Какие основные элементы включает в себя типовая структура системы управления ИБ ? выбрать все верные

Поддержка
планирование

оценка
реализация
контроль
прогнозирование
реструктуризация

5. Ресурсное обеспечение СУИБ

1. Ресурсное обеспечение СУИБ это:

аппаратное обеспечение средств обеспечения ИБ
программное обеспечение средств обеспечения ИБ
кадровые ресурсы (персонал)
процесс управления, обеспечивающий определение потребностей в ресурсах ИБ и контроль эффективности использования ресурсов ИБ

2. Для полноценной деятельности служб и систем управления информационной безопасности необходимы следующие виды ресурсов: выбрать все верные

финансовые
материальные
технические
энергетические
информационные
временные
пространственные
методические и законодательные
кадровые

3. Основные ресурсы обеспечения ИБ: выбрать все верные

финансовые
материальные
технические
энергетические
информационные
временные
пространственные
методические и законодательные
кадровые

6. Контроль и проверка процессов УИБ

1. Контроль, проверка и сертификация системы УИБ на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

внешнего аудита
внутреннего аудита
инструментальной проверки защищенности

2. Контроль и проверка процессов УИБ подразделяется на:

текущие и итоговые
внешние и внутренние
объективные и субъективные

3. Автоматизированный анализ процессов УИБ предполагает:

внесение данных в соответствии с вопросами задаваемыми программой
загрузку политик безопасности в виде электронных документов
внесение данных из журналов систем контроля безопасности

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 являетя 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 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	0–24	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 зачет:

1. Понятие информационной безопасности. Термины и определения. Общие сведения об информационной безопасности. Основные составляющие информационной безопасности.
2. Обоснование необходимости рассмотрения вопросов информационной безопасности. Система информационной безопасности. Проблемы построения современных систем безопасности.
3. Стандарты информационной безопасности ISO/IEC, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27005, ISO/IEC 27007, COBIT 5 for Information Security, ITIL.
4. Стандарты и нормативные акты РБ в области информационной безопасности.
5. Средства управления информационной безопасностью. Ключевые средства контроля. Группы требований к информационной безопасности организации.
6. Оценка рисков нарушения безопасности. Факторы, необходимые для успешной реализации системы

информационной безопасности в организации.
7. Политика информационной безопасности. Документ о политике информационной безопасности.
8. Инфраструктура информационной безопасности.
9. Безопасность доступа сторонних организаций.
10. Ответственность за ресурсы.
11. Классификация информации.
12. Безопасность в должностных инструкциях.
13. Обучение пользователей правилам информационной безопасности.
14. Реагирование на события, таящие угрозу безопасности.
15. Охраняемые зоны.
16. Безопасность оборудования.
17. Операционные процедуры и обязанности.
18. Планирование систем и их приемка.
19. Защита от вредоносного программного обеспечения.
20. Обслуживание систем.
21. Сетевое администрирование.
22. Оперирование с носителями информации и их защита.
23. Обмен данными и программами.
24. Требование бизнеса по обеспечению контроля доступа.
25. Управление доступом пользователей. Обязанности пользователей.
26. Контроль сетевого доступа.
27. Управление доступом к компьютерам.
28. Управление доступом к приложениям.
29. Слежение за доступом к системам и их использованием.
30. Требования к безопасности систем.
31. Безопасность в прикладных системах.
32. Защита файлов прикладных систем.
33. Безопасность в среде разработки и рабочей среде.
34. Система планирования бесперебойной работы организации.
35. Обновление планов обеспечения бесперебойной работы.
36. Выполнение правовых требований.
37. Проверка безопасности информационных систем. Аудит систем.
38. Продукты компании Cisco для управления безопасностью сетей.
39. Продукты компании IBM для управления средствами безопасности.
40. Продукты компании Check Point Software Technologies для управления средствами безопасности.

Примерный перечень тестовых заданий на зачет:

1. Основной целью управления является обеспечение эффективного управления информационной безопасностью всех услуг и деятельностей в рамках Управления услуг за счет: выбрать все верные

конфиденциальность
целостность
доступность
актуальность
оперативность

2. Политика информационной безопасности должна включать в себя следующее: выбрать все верные

реализация аспектов Политики информационной безопасности;
возможные злоупотребления аспектами Политики информационной безопасности;
политика контроля доступа;
политика Интернета

3. Лица, которые обязаны ознакомиться с политикой информационной безопасности, отвечают за исполнение политики, процедур и стандартов информационной безопасности:

владельцы информации
хранители информации

пользователи информации

4. Выберите наиболее подходящий ответ на вопрос «Что такое стандарты информационной безопасности?»

система официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере
документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации в целом
обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным ИС
свойство ИБ организации сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах

5. Какие категории требований безопасности указаны в «Оранжевой книге»: выбрать все верные

политика ИБ
аудит ИБ
корректность работы средств защиты
политика доступа к информации
политика паролей

6. Какой из стандартов описывает практические правила управления информационной безопасностью

ISO/IEC 15408
ГОСТ Р ИСО/МЭК 17799:2005
ГОСТ Р ИСО/МЭК 27001-2006

7. Принципом политики информационной безопасности является принцип:

Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

8. Политика безопасности в системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети

9. Наиболее важным при реализации защитных мер политики безопасности является:

Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций +

10. Согласно ГОСТ Р ИСО/МЭК 27000 ключевыми компонентами системы управления информационной безопасности являются: выбрать все верные

Локальные нормативные акты (ЛНА)
Сотрудники с определенными должностными обязанностями
Процессы управления
аппаратное обеспечение
программное обеспечение
бизнес-процессы организации

11. Основные функции систем управления информационной безопасностью (СУИБ) — это: выбрать все верные

выявление и анализ рисков информационной безопасности
планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ
контролирование этих процессов, направленных на минимизацию рисков ИБ
построение оптимальной политики ИБ предприятия

12. Какие основные элементы включает в себя типовая структура системы управления ИБ ? выбрать все верные

Поддержка
планирование
оценка
реализация
контроль
прогнозирование
реструктуризация

13. Ресурсное обеспечение СУИБ это:

аппаратное обеспечение средств обеспечения ИБ
программное обеспечение средств обеспечения ИБ
кадровые ресурсы (персонал)
процесс управления, обеспечивающий определение потребностей в ресурсах ИБ и контроль эффективности использования ресурсов ИБ

14. Для полноценной деятельности служб и систем управления информационной безопасности необходимы следующие виды ресурсов: выбрать все верные

финансовые
материальные
технические
энергетические
информационные
временные
пространственные
методические и законодательные
кадровые

15. Основные ресурсы обеспечения ИБ: выбрать все верные

финансовые
материальные
технические
энергетические
информационные
временные
пространственные
методические и законодательные
кадровые

16. Контроль, проверка и сертификация системы УИБ на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

внешнего аудита
внутреннего аудита
инструментальной проверки защищенности

17. Контроль и проверка процессов УИБ подразделяется на:

текущие и итоговые
внешние и внутренние
объективные и субъективные

18. Автоматизированный анализ процессов УИБ предполагает:

внесение данных в соответствии с вопросами задаваемыми программой
загрузку политик безопасности в виде электронных документов
внесение данных из журналов систем контроля безопасности

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. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Давыдов, А. И. Управление информационной безопасностью : учебное пособие / А. И. Давыдов, Д. А. Елизаров. — Омск : ОмГУПС, 2023. — 91 с. — ISBN 978-5-949-41321-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/419255 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Милославская, Н. Г. Управление информационной безопасностью: Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. — Москва : НИЯУ МИФИ, 2020. — 536 с. — ISBN 978-5-7262-2694-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/284378 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

5. Дронова, Г. А. Управление информационной безопасностью : учебно-методическое пособие : [16+] / Г. А. Дронова. – Новосибирск : Новосибирский государственный технический университет, 2016. – 28 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575356 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3113-9. – Текст : электронный.

6.2 Дополнительная литература

1. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — ISBN 978-5-907336-42-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/411836 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255569 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 27.03.2026). – Режим доступа: по подписке.

5. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 27.03.2026). – Режим доступа: по

подписке.

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 библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Образовательная платформа «Юрайт» https://urait.ru/
6. Электронная библиотечная система «Znanium» https://new.znanium.com/my/documents
7. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
8. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

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

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

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

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

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Управление информационной безопасностью"

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 "Управление информационной безопасностью", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

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

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Управление информационной безопасностью"

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.