Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гаврилов Сергей Александрович
Должность: И.О. Ректора
Дата подписания: 24.06.2025 16:06:23
Уникальный программный ключ:
f17218015d82e3c1457d1df9e244def505047355

МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г.Игнатова
«23» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Организация аудита информационной безопасности»

Направление подготовки – 10.04.01 «Информационная безопасность»
Направленность (профиль) – «Аудит информационной безопасности»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 021B3F91004AAD61874DBC90987DB30618
Владелец: Беспалов Владимир Александрович
Действителен: с 17.06.2021 до 17.06.2022

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина «Организация аудита информационной безопасности» участвует в формировании следующих компетенций**:**

Компетенция ПК-3 «Способен проводить аудит информационной безопасности» сформулирована на основе проекта новой редакции профессионального стандарта 064.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

Обобщенная трудовая функция D/7. Аудит информационной безопасности автоматизированной системы.

Трудовая функция D/01.7. Подготовка к проведению аудита информационной безопасности автоматизированной системы.

Трудовая функция D/02.7. Проведение аудита информационной безопасности автоматизированной системы.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-3. Способен проводить аудит информационной безопасности	ПК-3.ОАИБ. Способен проводить аудит информационной безопасности	**Знания** требования национальных и международных стандартов в области аудита ИБ. Требования ведомственных и отраслевых стандартов в области аудита ИБ; объекты аудита ИБ. Виды аудита ИБ. Цели аудита. Методы аудита. Принципы проведения аудита; методы анализа и оценки рисков ИБ; требования к программе и плану проведения аудита, порядок их разработки; структуру отчёта о результатах аудита ИБ; порядок подготовки и проведения аудита ИБ; особенности аудита ИБ информационных систем различного назначения (ИсПДн, АСУ ТП, ГИС). **Умения:** разрабатывать программы и планы проведения аудита ИБ; использовать методы аудита ИБ;

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		проводить анализ документированной информации, полученной в ходе аудита ИБ; готовить заключения по результатам аудита ИБ. **Опыт практической деятельности:** разработки программ и планов проведения аудита ИБ.

В результате изучения дисциплины студент должен:

Знать:

- требования национальных и международных стандартов в области аудита ИБ. Требования ведомственных и отраслевых стандартов в области аудита ИБ;
- объекты аудита ИБ. Виды аудита ИБ. Цели аудита. Методы аудита. Принципы проведения аудита;
- методы анализа и оценки рисков ИБ при организации и проведении аудита;
- требования к программе и плану проведения аудита, порядок их разработки;
- структуру отчёта о результатах аудита ИБ;
- порядок подготовки и проведения аудита ИБ;
- особенности аудита ИБ информационных систем различного назначения (ИсПДн, АСУ ТП, ГИС).

Уметь:

- разрабатывать программы, методики и планы проведения аудита ИБ;
- применять методы аудита ИБ для организации и проведения аудита;
- проводить анализ документированной информации, полученной в ходе аудита ИБ;
- готовить заключения по результатам аудита ИБ.

Иметь практический опыт:

- проведения аудита информационной безопасности;
- разработки программ и планов проведения аудита ИБ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Организация аудита информационной безопасности» входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 2-м курсе во 3-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении дисциплин «Технологии защиты информации от несанкционированного доступа», «Технологии защиты информации от утечки по техническим каналам», «Правовые основы аудита информационной безопасности», изучаемых 1 – 2 семестрах магистратуры.

Знания и умения, полученные в результате изучения дисциплины, используются в

дисциплине «Аудит информационной безопасности автоматизированных систем» (деловая игра), производственной практике и при подготовке ВКР.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы*	Практическая подготовка при выполнении курсовой работы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации			
2	3	5	180	84	16	16	32	20	60	16	Экз. (36), КР

* Часы на самостоятельную работы, включая часы на практическую подготовку при выполнении курсовой работы

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы			Самостоятельная работа, часы*	Практическая подготовка при выполнении курсовой работы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия			
1. «Основы аудита информационной безопасности».	6	-	4	6	-	Компьютерный тест КТ-1.
2. «Организация и проведение аудита информационной безопасности».	10	16	28	54	16	Компьютерный тест КТ-2. Зачет по ЛР № 1 и 2. Зачет по ПЗ (ГУ) № 4 - 6. Сдача КР.

* Часы на самостоятельную работы, включая часы на практическую подготовку при выполнении курсовой работы

4.1. Лекционные занятия

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
1	1.	2	**Основы организации аудита информационной безопасности. Введение в учебную дисциплину** Понятие аудита информационной безопасности (ИБ). Объекты аудита ИБ. Виды аудита ИБ. Внешний аудит. Внутренний аудит. Цели аудита. Методы аудита. Принципы проведения аудита. Структура отчёта о результатах аудита ИБ. Аудит ИБ информационной системы. Сертификационный аудит системы управления ИБ организации.
	2.	2	**Нормативно-методическое регулирование в области аудита информационной безопасности** Требования национальных и международных стандартов в области аудита ИБ. Требования ведомственных и отраслевых стандартов в области аудита ИБ. Требования нормативных и методических документов ФСТЭК России.
	3.	2	**Особенности аудита ИБ информационных систем различного назначения** Аудит ИБ на соответствие требованиям ФЗ «О персональных данных», назначение и методы проведения. Аудит ИБ на соответствие стандартам СТО БР, назначение, методы проведения, анализ результатов, оценка рисков ИБ. Аудит ИБ государственных информационных систем (ГИС) на соответствие требованиям ФСТЭК России. Аудит ИБ автоматизированных систем управления технологическими процессами (АСУ ТП).
2	4.	2	**Порядок проведения аудита информационной безопасности** Порядок проведения аудита ИБ. Регламент взаимодействия сторон и план проведения аудита. Подготовка и сбор исходных данных для проведения аудита ИБ. Методы сбора исходных данных, интервьюирование сотрудников заказчика, предоставление опросных листов, анализ организационно-технической документации. Исходные данные (документация) необходимые для аудита.
	5.	2	**Выбор средств проведения внутреннего и внешнего аудита автоматизированных систем управления технологическими процессами** Выбор инструментальных средств проведения аудита ИБ. Оценка полноты и правильности реализации ключевых средств контроля, а также анализ их адекватности рискам. Программные средства анализа и управления рисками (CRAMM, RiskWatch, COBRA, Buddy System). Средства контроля защищённости ИС.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	6.	2	**Разработка программы и плана проведения аудита** Инициирование процедуры аудита. Цели и объект программы аудита, ресурсы и процедуры. Правовое регулирование процедуры подготовки аудита ИБ. Техническое задание на проведение аудита ИБ. Управление программой аудита, цели и объем программы аудита, ответственность за программу аудита, ресурсы и процедуры, внедрение программы аудита, записи по программе аудита, мониторинг и анализ программы аудита. Различие между программой и планом аудита.
	7.	2	**Сертификационный аудит автоматизированных систем управления технологическими процессами** Порядок оценки соответствия АСУ ТП требованиям международных и национальных стандартов и других нормативных и методических документов в области ИБ. Сертификат соответствия.
	8.	2	**Анализ данных, полученных в результате аудита автоматизированных систем управления технологическими процессами** Методы анализа данных, полученных в результате аудита АСУ ТП. Моделирование угроз безопасности информации и действий нарушителя. Анализ рисков ИБ и управление рисками. Методы оценки рисков ИБ. Виды ущерба. Методы оценки ущерба.

4.2. Практические занятия

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
1.	1.	4	**Практическое занятие (семинар). Общие вопросы организации аудита информационной безопасности** Организация разработки, внедрения и поддержания актуальности политики в области защиты информации. Управление информационными активами; Защита. Физическая и экологическая безопасность. Организация эксплуатации технических и программных средств. Управление доступом. Приобретение, разработка и поддержание в рабочем состоянии информационных систем. Управление инцидентами в системе защиты информации. Управление непрерывностью бизнеса. Обеспечение соответствия требо-

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			ваниям нормативно правовых актов, нормам, стандартам. Требования о защите информации, содержащейся в информационных системах общего пользования. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Национальные стандарты по защите информации.
2.	2.	4	**Практическое занятие (семинар). Порядок подготовки аудита информационной безопасности** Инициирование аудита, установление контакта с проверяемой организацией, определение возможности проведения аудита. Подготовка к проведению аудита, анализ документированной информации. Планирование аудита, риск-ориентированный подход при планировании. Планирование аудита, подробности планирования аудита. Планирование аудита, распределение заданий в группе по аудиту. Планирование аудита, подготовка рабочих документов. Проведение аудита, общие положения, назначение ролей и обязанностей, сопровождающих и наблюдателей. Проведение открывающего совещания. Обмен информацией в ходе аудита, места получения информации для аудита и доступ к ней. Анализ документированной информации в ходе аудита, сбор и проверка информации. Формирование выводов аудита. Подготовка заключений аудита. Подготовка и рассылка отчета об аудите.
	3.	4	**Практическое занятие (семинар). Оценка компетентности аудиторов информационной безопасности** Порядок оценки компетентности аудиторов. Порядок оценки компетентности аудиторов. Определение компетентности аудитора, общие положения, требования к личным качествам. Требования к знаниям и навыкам, общие положения, требования к общим знаниям и навыкам. Требования к компетентности аудиторов в конкретных отраслях. Требование к общей компетентности руководителя группы по аудиту и к компетентности аудитора. Определение критериев оценки аудитора, выбор метода оценки аудитора. Порядок поддержания и повышение компетентности аудитора. Методы аудита. Дополнительные руководящие указания для аудиторов по планированию и проведению аудитов. Сущность процессного подхода к аудиту, о профессиональном суждении, о результатах функционирования. Порядок проверки исходной информации. Порядок формирования аудиторской выборки, детерминированная и случайная выборки. Аудит соответствия результативности основных процессов. Аудит контекста. Аудит лидерства и обязательств. Аудит рисков и возможностей. Порядок

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			подготовки рабочих документов и выбора источников информации. Порядок проведения аудита на месте. Порядок проведения удаленного аудита. Порядок проведения интервью. Порядок формирования выводов аудита.
	4.	4	**Практическое занятие (групповое упражнение). Разработка программы и плана аудита информационной безопасности** Инициирование аудита ИБ. Подготовка к проведению аудита ИБ. Определение целей программы аудита. Разработка эталонной модели объекта аудита ИБ. Нормирование труда аудитора. Оценка выделенных для аудита ИБ сил и средств. Определение и оценка рисков и возможностей, связанных с программой аудита ИБ. Разработка программы аудита ИБ. Разработка плана аудита ИБ.
	5.	4	**Практическое занятие (групповое упражнение). Организация проведения аудита информационной безопасности** Порядок применения методов аудита. Порядок формирования аудиторской выборки. Порядок проведения удаленного аудита и аудита на месте. Организация обмена информацией в ходе аудита. Анализ документированной информации, полученной в ходе аудита. Добывание объективных свидетельств аудита, проверка их достоверности, обобщение (вывод групповых свидетельств аудита). Формирование выводов аудита ИБ
	6.	4	**Практическое занятие (групповое упражнение). Оформление результатов аудита информационной безопасности** Подготовка заключений аудита. Организация заключительного совещания. Порядок подготовки и рассылки отчета об аудите. Порядок завершения аудита. Корректирующие действия по результатам аудита.
	7.	4	**Практическое занятие (семинар). Организация аудита информационной безопасности информационных систем персональных данных** Выделение информационных систем персональных данных. Модели угроз и модели нарушителя. Уровень защищенности ИСПДн. Состав и содержания организационных и технических мер. Базовый набор мер ИСПДн. Адаптированный базовый набор мер защиты. Компенсирующие, организационные меры защиты. Пакет организационных документов. Организация работ и назначение ответственных лиц.
	8.	4	**Практическое занятие (семинар). Организация аудита информационной безопасности информационных систем критической инфраструктуры** Выделение информационных систем критической информационной инфраструктуры (КИИ). Типология объектов критической

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			информационной инфраструктуры. Признаки критического процесса. Модели угроз и модели нарушителя. Категорирование объекта КИИ. Состав и содержания организационных и технических мер. Базовый набор мер защиты. Адаптированный базовый набор мер защиты. Компенсирующие, организационные меры защиты. Пакет организационных документов. Организация работ и назначение ответственных лиц.

4.3. Лабораторные работы

Номер модуля дисциплины	Номер лабораторной работы	Объем занятий, часы	Краткое содержание
2.	1.	8	Аудит автономной АС на соответствие требованиям по защите информации от несанкционированного доступа
	2	8	Аудит АС (ЛВС) на соответствие требованиям по защите информации от несанкционированного доступа

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к практическому занятию (семинару) № 1** Изучение материалов лекции №№ 1 - 3 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 1. Подготовка доклада и презентации по одному из вопросов плана занятия.
	2	**Подготовка к компьютерному тесту КТ-1** Изучение материалов лекции №№ 1 - 3 и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
2	4	**Подготовка к практическому занятию (семинару) № 2** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 2. Подготовка доклада и презентации по одному из вопросов плана занятия.
	4	**Подготовка к практическому занятию (семинару) № 3** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 3. Подготовка доклада и презентации по одному из вопросов плана занятия.
	4	**Подготовка к практическому занятию (групповому упражнению) № 4** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 1.
	4	**Подготовка к практическому занятию (групповому упражнению) № 5** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 2.
	4	**Подготовка к практическому занятию (групповому упражнению) № 6** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 3.
	4	**Подготовка к практическому занятию (семинару) № 7** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 4. Подготовка доклада и презентации по одному из вопросов плана занятия.
	4	**Подготовка к практическому занятию (семинару) № 8** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 5. Подготовка доклада и презентации по одному из вопросов плана занятия.
	4	**Подготовка к лабораторной работе № 1** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 1
	4	**Подготовка к лабораторной работе № 2** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 2
	2	**Подготовка к компьютерному тесту КТ-2** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы.
2	16	**Подготовка курсовой работы**

4.5. Примерная тематика курсовых работ

Тема курсовой работы «Разработка программы, плана и методики проведения аудита информационной безопасности автоматизированной системы».

Автоматизированные системы (по выбору студента):

- автоматизированная система обработки конфиденциальной информации;
- информационных систем персональных данных;
- автоматизированная система информационных управления технологическими процессами;
- автоматизированная система критической информационной инфраструктуры.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Модуль 1 «Основы аудита информационной безопасности»:

Тексты лекций № 1 – 3. ОРИОКС// URL: http://orioks.miet.ru/

План проведения семинара № 1 . ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2 «Организация и проведение аудита информационной безопасности»:

Тексты лекций № 4 – 8. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению практических занятий (групповых упражнений) № 1 – 7: ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 1и 2. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по выполнению курсовой работы ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Воеводин, В. А. Аудит информационной безопасности автоматизированных систем учебное пособие / В. А. Воеводин, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0974-5 : - Текст : непосредственный.

2. Мельников, Д. А. Информационная безопасность открытых систем: учебник / Д. А. Мельников. - Москва : Флинта : Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 16.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.

3. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158 (дата обращения: 15.03.2021). - ISBN 978-5-534-03600-8. - Текст : электронный.

4. Воеводин, В. А. Правовые основы аудита информационной безопасности: учебное пособие / В. А. Воеводин, П. Л. Пилюгин; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - Москва : МИЭТ, 2021. - 180 с. - ISBN 978-5-7256-0961-5 - Текст : непосредственный.

5. Программно-аппаратные средства защиты информации : учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1 : Текст : непосредственный.

6. Программно-аппаратные средства защиты информации : учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 : Текст : непосредственный.

7. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.

8. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8 : - Текст : непосредственный.

9. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : [сайт]. – URL: https://docs.cntd.ru/document/901990051. - (дата обращения 15.03.2021)

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ: (ред. от 02.07.2021) «О персональных данных»; Текст: электронный // Техэксперт : [сайт]. https://docs.cntd.ru/document/573249803?marker=64U0IK - (дата обращения 15.03.2021).

3. Методический документ. Методика оценки угроз безопасности информации. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2021 г. (утверждена ФСТЭК России 5 февраля 2021 г.)

4. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.

5. Методика определения актуальных угроз безопасности персональных данных

при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

6. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

7. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

8. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

9. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

10. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

11. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Общие положения; Национальный стандарт РФ : Введ. 09.02.1995: М.: Издательство стандартов (Переиздание) Стандартинформ, август 2006 -URL: https://docs.cntd.ru/document/1200004675 (дата обращения: 15.03.2021) -Текст: электронный.

12. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; Protection of information. Basic terms and definitions: Национальный стандарт РФ: Введ. 01.02.2008: М.: Стандартинформ, 2008. URL: https://docs.cntd.ru/document/1200058320 (дата обращения 16.03.2021).- Текст: электронный.

13. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatisation. Factors influencing the information. General: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, (Переиздание) 2018. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021) -Текст: электронный.

14. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Information protection. Sequence of protected operational system formation. General provisions; Национальный стандарт РФ: Введ. 01.09.2014.- М.: Стандартинформ, (Переиздание) октябрь 2018.-URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 15.03.2021) Текст: электронный.

15. ГОСТ Р 51583-2014. Рекомендации по стандартизации Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.

16. Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Technical information protection. Terms and definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.

Периодические издания

1. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный : непосредственный.
2. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.
3. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.
4. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.
4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021). - Текст: электронный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС http://orioks.miet.ru.

Для взаимодействия студентов с преподавателем используются сервисы обратной

связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (http://orioks.miet.ru).

Тестирование проводится в ОРИОКС (MOODLe).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome/Explorer).
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL (Из реестра МИЭТ п.18) – 28 шт. 3. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	на использование Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-3. ОАИБ «Способен проводить аудит информационной безопасности».

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/**.**

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В целях практической подготовки в дисциплине предусмотрены лабораторные работы, практические занятия (групповые упражнения), семинары и выполнение курсовой работы.

Каждая лабораторная работа (ЛР), групповое упражнение (ГУ), семинар и курсовая работа (КР) направлены на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

Лабораторные работы, групповые упражнения и курсовая работа выполняются каждым студентом индивидуально.

По результатам выполнения каждой ЛР и ГУ и КР студент оформляет и представляет отчет. При защите отчетов преподаватель разбирает типовые ошибки и указывает их причины.

11.1. Методические указания студентам по подготовке к семинарам

Семинар - развернутая беседа с обсуждением доклада. Проводится на основе заранее разработанного плана, по вопросам которого готовится вся учебная группа. Основными компонентами такого занятия являются: вступительное слово преподавателя, доклады обучаемых, вопросы докладчикам, выступления студентов по докладу и обсуждаемым вопросам, заключение преподавателя.

Развернутая беседа позволяет вовлечь в обсуждение проблем наибольшее число обучаемых. Главная задача преподавателя при проведении такого семинарского занятия состоит в использовании всех средств активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов, умелой концентрации внимания на наиболее важных проблемах, умения обобщать и систематизировать высказываемые в выступлениях идеи, сопоставлять различные точки зрения, создавать обстановку свободного обмена мнениями. Данная форма семинара способствует выработке у обучаемых коммуникативных навыков.

Как правило, темы докладов разрабатываются преподавателем заранее и включаются в планы семинаров. Доклад носит характер краткого (10-15 мин.) аргументированного изложения одной из центральных проблем семинарского занятия с использованием презентации.

В ходе семинаров заслушиваются выступления по вопросам семинара, также доклады по рефератам, темы которых соответствующих вопросам, рассматриваемым на семинаре.

11.2. Методические указания студентам по подготовке к лабораторным работам и групповым упражнениям

Выполнение студентами к лабораторным работам и групповых упражнений направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Ведущей дидактической целью ЛР (ГУ) является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Наряду с ведущей дидактической целью в ходе выполнения заданий у студентов формируются практические умения и навыки обращения с различными приборами, установками, лабораторным оборудованием, аппаратурой, которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).

Лабораторные работы и групповые упражнения, как виды учебных занятий прово-

диться в специально оборудованных учебных лабораториях. Продолжительность - не менее двух академических часов. Необходимыми структурными элементами ЛР (ГУ), помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

По каждой ЛР (ГУ) разработаны и утверждены методические указания по их проведению.

Лабораторные работы и групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов на ЛР (ГУ): индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения ЛР (ГУ) преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждой ЛР (ГУ), предусмотренными рабочей программой учебной дисциплины: в соответствии с количеством часов, требованиями к знаниям и умениям, темой практических занятий и лабораторных работ, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению ЛР (ГУ) включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ЛР (ГУ);
- наименование темы ЛР (ГУ);
- цель ЛР (ГУ) (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);
- требования по теоретической готовности студентов к выполнению ЛР (ГУ) (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;
- список рекомендуемой литературы;
- приложения.

При подготовке к ЛР (ГУ) студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ЛР (ГУ);
- ознакомиться с методическими рекомендации по выполнению ЛР (ГУ);
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к ЛР (ГУ);
- изучить схемы лабораторных установок (стендов), порядок работы на аппара-

туре и технике, правила и меры безопасности;

- подготовить отчеты для заполнения.

На ЛР (ГУ) студент должен выполнить задание в соответствии с методическими указаниями.

Отчет о ЛР (ГУ) должен быть оформлен в соответствии методическими указаниями и ГОСТами.

При защите отчета о ЛР (ГУ) убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и провести исследования, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на ЛР (ГУ) обязаны соблюдать меры безопасности при работе на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

11.3. Методические указания студентам по подготовке курсовой работы

Тема курсовой работы «Разработка программы, плана и методики проведения аудита информационной безопасности автоматизированной системы».

Автоматизированные системы (по выбору студента):

– автоматизированная система обработки конфиденциальной информации;

– информационных систем персональных данных;

– автоматизированная система информационных управления технологическими процессами;

– автоматизированная система критической информационной инфраструктуры.

При выполнении курсовой работы студенты проводят:

1. Анализ исходных данных по АС.
2. Исследование технологического процесса обработки и хранения информации.
3. Анализ состояния организации работ и выполнения требований по защите информации:

A. Анализ документов по обеспечению информационной безопасности АС.

B. Правильность категорирования и классификации АС.

C. Оценку уровня подготовки специалистов и распределения ответственности пользователей ОИ.

D. Проверку выполнения требований к помещениям, в которых производится обработка информации.

4. Анализ АС на соответствие требованиям по защите информации от несанкционированного доступа.
5. На основе проведенного анализа разрабатывают:

A. Программу и методики аудита информационной безопасности АС.

B. План проведения аудита информационной безопасности АС.

Структура курсовой работы должна отвечать традиционным требованиям, предъявля-

емым к научным работам и включать следующие части (структурные элементы):

Титульный лист.

Задание на КР.

Реферат.

Содержание.

Перечень условных обозначений и сокращений.

Введение.

Основная часть (основные разделы работы, предусмотренные заданием).

Заключение.

Список использованных источников.

Приложения.

Объем пояснительно записки составляет 50 – 70 страниц машинописного текста с приложениями, выполненных на стандартных листах формата А4.

Титульный лист является первым листом в пояснительной записке.

Реферат – это сокращенное изложение содержания и существа КР с основными сведениями о выполненных разработках и полученных результатах.

Реферат имеет следующую структуру:

− перечень количественных сведений о КР;

− перечень ключевых слов;

− текст реферата.

Перечень количественных сведений о КР должен включать количество: ___ с., ___ рис., ___ табл., __ источник, ___ прил.)..

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста КР, которые в наибольшей мере характеризуют содержание и обеспечивают возможность информационного поиска. Ключевые слова приводятся в именительном падеже и печатаются строчными буквами в строку через запятые.

Текст реферата в общем случае должен отражать сведения:

− об объекте аттестации;

− о цели аттестации;

− об использованных методах и средствах, использованных при аттестационных испытаниях;

− о результатах аттестации.

Если КР не содержит сведений по какой-либо из перечисленных структурных частей реферата, то в тексте реферата она опускается, при этом последовательность изложения сохраняется.

Объем реферата определяется содержанием КР, количеством сведений и их научной и практической ценностью. Средний объем реферата составляет 1500 − 2000 знаков.

Перечень условных обозначений и сокращений. Принятые в работе малораспространенные условные обозначения, сокращения, символы, единицы и специфические термины необходимо представлять в виде отдельного списка. Если сокращения, условные обозначения, символы, единицы и термины повторяются в работе менее трех раз, отдельный список не составляют, а расшифровку дают непосредственно в тексте при первом упоминании.

Содержание пояснительной записки включает введение, наименования всех разделов, подразделов и пунктов (если последние имеют наименования), заключение, список использованных источников и наименование приложений с указанием номеров страниц, с которых

начинаются эти элементы пояснительной записки.

Введение должно содержать:

− развернутую оценку современного состояния решаемой задачи;

− актуальность и новизну темы;

− постановку задачи исследования с указанием цели, используемых методов и средств;

− исходные данные для исследования;

− планируемые результаты.

Объем введения 3 − 5 страниц.

Основная часть. Основная часть включает две главы и приложение А. Традиционно каждая глава подразделяется на несколько (как правило, 3 – 5) параграфов.

Основная часть. Основная часть должна включать:

– Программу аудита информационной безопасности АС.

– Методики аудита информационной безопасности АС.

– План проведения аудита информационной безопасности АС.

Заключение должно содержать:

− краткие выводы по результатам выполнений работы;

− оценку полноты решений поставленных задач.

Типовой объем заключения составляет 1-2 страницы.

Список использованных источников должен содержать сведения обо всех источниках, использованных при написании КР. В список следует включать только те наименования, с которыми автор КР ознакомился лично. На все источники, приведенные в списке, должны быть ссылки в тексте. На источники, содержащие общие сведения по теме ВКР, ссылки делаются обычно во введении.

Источники в списке нумеруются в порядке появления ссылок в тексте.

При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ 7.1–2003.

Курсовая работа должна быть написана студентом самостоятельно, грамотно, по логически построенному плану. Прямое переписывание в работе текста из учебной и научной литературы не допускается.

11.4. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-бальная система.

Под накопительно-бальной системой понимается система количественной, балльно - рейтинговой оценки качества освоения учебной дисциплины студентом $R_{нак}$ по суммарному результату текущего $R_{тек}$ и итогового контроля $R_{итог}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{пр}$.

Выполнение контрольных мероприятий текущего контроля (сдача компьютерных тестов, защита отчетов по групповым упражнениям, защита курсовой работы, доклады с рефератами), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача экзамена) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Примерные структура и график контрольных мероприятий приведены в таблице 11.1.

Таблица 11.1

Структура и график контрольных мероприятий дисциплины

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
3	Практическое занятие (семинар) № 1	4	2
3	Компьютерный тест (КТ-1)	6	3
6	Практическое занятие (семинар) № 2	4	2
7	Практическое занятие (семинар) № 3	4	2
8	Практическое занятие (групповое упражнение) № 4	4	3
9	Практическое занятие (групповое упражнение) № 5	6	3
10	Практическое занятие (групповое упражнение) № 6	4	3
11	Практическое занятие (семинар) № 7	4	2
12	Практическое занятие (семинар) № 8	6	2
14	Лабораторная работа № 1	6	4
16	Лабораторная работа № 2	8	2
16	Компьютерный тест (КТ-2)	6	3
16	Посещаемость, активность	8	4
	Итого за текущий контроль	***70***	***35***
	Итоговый контроль	***30***	***15***
	Накопленный рейтинг	**100**	**50**

В экзаменационную ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Примерная структура и график контрольных мероприятий при выполнении курсовой работы приведены в таблице 11.2.

Таблица 11.2

Структура и график контрольных курсовой работы

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
10	Контроль № 1	10	5
12	Контроль № 2	10	5
14	Контроль № 3	10	5
16	Итоговый просмотр (оценка качества курсового проекта)	40	20
	Итого за текущий контроль	***70***	***35***
17	***Итоговый контроль*** *(защита курсового проекта)*	***30***	***15***
	Накопленный рейтинг	**100**	**50**

За курсовую работу в зачетную ведомость и зачетную книжку вносится ***итоговая 5-балльная оценка***, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в зачетную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в зачетную ведомость.

РАЗРАБОТЧИК

Доцент кафедры «Информационная безопасность»
Кандидат технических наук _____ В.А. Воеводин

Рабочая программа дисциплины «Организация аудита информационной безопасности» по направлению подготовки 10.04.01 «Информационная безопасность», направленности (профилю) «Аудит информационной безопасности» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А. Хорев

Лист согласования

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества
Начальник АНОК _____/ И.М. Никулина /

Рабочая программа согласована с библиотекой МИЭТ
Директор библиотеки _____/ Т.П. Филиппова /