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» мая 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Технологии защиты информации от несанкционированного доступа»

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

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций**:**

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1. ТЗИНСД. Способен обосновывать требования к системе защиты автоматизированной системы от несанкционированного доступа к информации	**Знания:** цели, задачи и терминологию в области защиты информации от несанкционированного доступа, несанкционированного и неправомерного воздействий; понятия и составляющие безопасности компьютерной сети, понятие угроз безопасности, основы их классификации (каталогизации), методы и проблемы оценки угроз безопасности; угрозы безопасности информации в автоматизированных системах; методы обнаружения уязвимостей компьютерных сетей, возможные типы атак на компьютерные сети; модели нарушителей; современные технологии идентификации и аутентификации; современные технологии управления доступом к информации; современные технологии регистрации и учета; современные технологии защиты информации и программного обеспечения от вредоносных программ; современные технологии обеспечения целостности информации. **Умения:** обосновывать требования к системе защиты автоматизированной системы от несанкционированного доступа к информации; осуществлять выбор функциональной структуры системы обеспечения безопасности ин-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		формации, обрабатываемой в автоматизированных системах; **Опыт практической деятельности:** обоснования требований к системе защиты автоматизированной системы от несанкционированного доступа к информации
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2. ТЗИНСД. Способен разрабатывать технические решения по защите автоматизированной системы от несанкционированного доступа к информации	**Знания:** современные технологии межсетевого экранирования; защищенные протоколы передачи данных в сетях; основные методы и технологии обеспечения безопасности сетей при подключении их к сети Интернет; современные технологии обнаружения вторжений; требования нормативных документов ФСТЭК России по защите автоматизированных систем и сетей от несанкционированного доступа к информации. **Умения:** разрабатывать технические решения по защите автоматизированной системы от несанкционированного доступа к информации; обосновывать выбор технологий для обеспечения безопасности информации, обрабатываемой в автоматизированных системах. проводить установку и настройку средств обеспечения безопасности открытой сети, обеспечивающих авторизацию, контроль доступа и обнаружение вторжений при сетевых и межсетевых взаимодействиях; устанавливать, настраивать, тестировать и отлаживать программные и программно-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		аппаратные средства защиты информации. **Опыт практической деятельности:** разработки технических решений по защите автоматизированной системы от несанкционированного доступа к информации.

В результате изучения дисциплины студент должен:

Знать:

цели, задачи и терминологию в области защиты информации от несанкционированного доступа, несанкционированного и неправомерного воздействий;

понятия и составляющие безопасности компьютерной сети, понятие угроз безопасности, основы их классификации (каталогизации), методы и проблемы оценки угроз безопасности;

угрозы безопасности информации в автоматизированных системах;

методы обнаружения уязвимостей компьютерных сетей, возможные типы атак на компьютерные сети;

модели нарушителей;

современные технологии идентификации и аутентификации;

современные технологии управления доступом к информации;

современные технологии регистрации и учета;

современные технологии защиты информации и программного обеспечения от вредоносных программ;

современные технологии обеспечения целостности информации;

современные технологии межсетевого экранирования;

защищенные протоколы передачи данных в сетях;

основные методы и технологии обеспечения безопасности сетей при подключении их к сети Интернет;

современные технологии обнаружения вторжений;

требования нормативных документов ФСТЭК России по защите автоматизированных систем и сетей от несанкционированного доступа к информации.

Уметь:

обосновывать требования к системе защиты автоматизированной системы от несанкционированного доступа к информации;

осуществлять выбор функциональной структуры системы обеспечения безопасности информации, обрабатываемой в автоматизированных системах;

разрабатывать технические решения по защите автоматизированной системы от несанкционированного доступа к информации;

обосновывать выбор технологий для обеспечения безопасности информации, обрабатываемой в автоматизированных системах;

проводить установку и настройку средств обеспечения безопасности открытой сети, обеспечивающих авторизацию, контроль доступа и обнаружение вторжений при сетевых и межсетевых взаимодействиях.

устанавливать, настраивать, тестировать и отлаживать программные и программно-аппаратные средства защиты информации.

Иметь опыт практической деятельности:

обоснования требований к системе защиты автоматизированной системы от несанкционированного доступа к информации;

разработки технических решений по защите автоматизированной системы от несанкционированного доступа к информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Технологии защиты информации от несанкционированного доступа» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 1-м курсе в 1-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при освоении основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность при изучении следующих дисциплин: «Физика», «Теория вероятностей и математическая статистика», «Информатика», «Теория информации», «Аппаратные средства вычислительной техники», «Сети и системы передачи информации», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Защита информации от НСД».

Знания и умения, полученные в результате изучения дисциплины, используются в дисциплинах «Управление информационной безопасностью», «Защищенные информационные системы», «Организация аудита информационной безопасности», 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	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1	1	8	288	160	64	48	16	32	92	Экз. (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы					Самостоятельная работа, часы	Формы текущего контроля
	ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1. «Угрозы безопасности информации, обрабатываемой в автоматизированных системах и вычислительных сетях»	12	4	4	-	4	8	Компьютерный тест РК 1. Зачет по ЛР № 1
2. «Основные технологии идентификации и аутентификации при обеспечения безопасности информации, обрабатываемой в автоматизированных системах и сетях»	24	16	4	-	4	10	Компьютерный тест РК 2. Зачет по ЛР № 2
3. «Основные технологии обеспечения конфиденциальности и целостности информации, обрабатываемой в автоматизированных системах»	84	24	36	8	16	62	Компьютерный тест РК 3. Зачет по ЛР № 3-11
4. «Особенности и проблемные вопросы обеспечение информационной безопасности обрабатываемой в автоматизированных системах и сетях»	40	20	4	8	8	12	Компьютерный тест РК 4. Зачет по Лр № 12

4.1. Лекционные занятия

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
1	1.	2	**Вводная лекция. Угрозы и уязвимости информации при обработке в автоматизированных системах (АС), понятие технологий обеспечения безопасности.** Модели угроз безопасности информации, обрабатываемой и источники уязвимостей АС и их характеристика. Классификация способов обеспечения информационной безопасности (управление доступом; регистрация и учет; обеспечение целостности; контроль отсутствия недекларированных возможностей; антивирусная защита; криптографическая защита информации; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений; предотвращение утечек и т.д.). Основные функциональные задачи информационной безопасности и их реализация для сетевой безопасности модель AAA (аутентификация, авторизация и акаунтинг).
	2.	2	**Задачи и основные принципы сетевой безопасности** Проблемы обеспечения информационной безопасности в распределенных вычислительных сетях. Важность, актуальность и сложность решения задач обеспечения сетевой безопасности. Интеграция принципов защиты вычислительных систем и сетей передачи данных. Основные функциональные задачи информационной безопасности и их реализация для сетевой безопасности модель AAA (аутентификация, авторизация и акаунтинг) в сетях. Уровни стека протоколов TCP/IP. Соотношение с моделью ISO-OSI. Возможные угрозы сети на различных уровнях стека протоколов. Структура сетевых атак. Банк данных о атаках и уязвимостях. Матрица MITRE.
2	3.	2	**Технологии идентификации и аутентификации:** Аутентификация, авторизация и идентификация (определения). Технологии аутентификации: одноразовые пароли, многоразовые пароли, базы учетных записей, многофакторная аутентификация. Технологии идентификации и аутентификации пользователей по специальным устройствам. Технологии идентификации и аутентификации пользователей по биометрическим характеристикам человека. Технологии идентификации и аутентификации используемых компонентов обработки информации (аппаратных и программных средств)

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	4.	4	**Технологии аутентификации на основе симметричных криптосистем** Аутентификацияна основе симметричных критографических протоколов. Протоколы взаимной аутентификациию Протоколы с распределением колючей. Двух, трех и многосторонние протоколы. Виды атак на протоколы аутентификации. Протоколы ISO. Протокол Нидхема-Шрейдера. Другие виды протоколов.
	5.	4	**Технологии аутентификации на основе асимметричных криптосистем** Аутентификация на основе ключевых хеш-функций. Аутентификация на основе асимметричных критографических протоколов. Модификация парольной схемы. Использование цифровой подписи. Структурв PKI. Протоколы взаимной аутентификациию Протоколы с распределением колючей. Двух, трех и многосторонние протоколы. Виды атак на протоколы аутентификации. Протоколы ISO. Протокол Нидхема-Шрейдера. Другие виды протоколов.
	6.	2	**(Часть 4) Технологии аутентификации на основе хеш-функций** Особенности использования хеш-функций. Технологии построения ключевых хеш-функций на осонове бесключевых. Протоколы аутентификации. Аутентификация в сетях WiFi, GSM, GPRS, LTE.
	7.	4	**Протоколы аутентификации и авторизации в вычислительных сетях** Простейшие протоколы удаленной аутентификации: PAP и CHAP. Аутентификация и авторизация. Сетевые протоколы и службы авторизации: RADIUS, TACACS, KERBEROS. Аутентификаци в беспроводных сетях.
3	8.	2	**Современные технологии управления доступом к информации, модель механизма защиты:** Субъектно-объектная модель управления доступом. Модель абстрактного механизма защиты и политики безопаности.
	9.	4	**Современные технологии управления доступом к информации, использующие дискреционный принцип:** Технологии управления доступом к АРМ и серверам. Технологии управления учетными записями. Дискреционный принцип доступа. Модели Грехема-Денинига, Хартсона, HRU, T-G. Реализации этих моделей в информационных системах. Сравнение результа-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			тов моделирования. Задачи по анализу передачи прав или утечки информации.
	10.	4	**Современные технологии управления доступом к информации, использующие мандатный принцип принцип:** Принципы военной безопасности MLS. Понятие решетки безопасности. Модель Деннинг. Технологии управления доступом на основе мандатного принципа. Модели Белла-ЛаПадулы (простая, RW, классическая и пр.). Реализации этих моделей в информационных системах.
	11.	4	**Современные технологии управления доступом к информации, использующие тематический принцип:** Принципы тематического подхода. Примеры и типы тематических моделей. Построение тематических решеток безопасности. Монорубрицированные классификации. Мультирубрицированные классификации. Реализации тематических моделей в информационных системах.
	12.	2	**Современные технологии управления доступом к информации, использующие ролевой принцип:** Принципы ролевого подхода. Примеры и типы ролевых моделей. Индивидуально-групповое управление доступом. Реализации ролевых моделей в информационных системах.
	13.	4	**Современные технологии управления доступом для обеспечения целостности информации:** Основные требования к подсистеме обеспечения целостности информации. Подсистема резервного копирования: основные требования к подсистеме резервного копирования; типы резервного копирования; типы резервных носителей; хранение и использование резервных копий; архитектура подсистемы резервного копирования. Подсистема распределения обновлений: основные требования к подсистеме распределения обновлений; возможные варианты построения системы; архитектура подсистемы распределения обновлений. Модель Биба.
	14.	2	**Современные технологии контроля доступа в вычислительных сетях** Задачи фильтрации сетевого трафика. Межсетевые экраны. Фильтрация пакетов. Коммутация каналов. Анализ приложений. Анализ состояний. Прокси сервер. Понятие DMZ.
	15.	2	**Современные технологии обеспечения изоляции, изоляция в**

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			сети, защищенные сетевые протоколы. Основные требования к обеспечению изоляции. Изоляция в операционных системах, в СУБД, в сетях. Реализации технологии изоляции. Развитие IPv4 и свойства защищенности протокола IPv6. Протоколы IPsec, SSL, TLS, PPTP. Построение VPN
4	16.	2	**Пассивные сетевые атаки.** Атаки не нарушающие функционирование сети. Сбор информации выбор целей, подготовка проникновения. Анонимное сканирование. Возможности обнаружения пассивных атак.
	17.	2	**Активные сетевые атаки.** Атаки на слабости протоколов. Имперсонация. Методы внедрения ложного сервера. MitM атаки. Методы десинхронизации TCP соединений. DOS атаки.
	18.	2	**Системы выявления утечек и обнаружения вторжений.** Задачи сетевого мониторинга на разных уровнях стека протокола TCP\IP. DLO, IDS и IPS системы.
	19.	4	**Современные технологии обеспечения безопасности информации в виртуальных машинах и сетях, в Центрах Обработки Данных и при выполнении «облачных вычислений»:** Назначение Центра Обработки Данных (ЦОД) и виртуальных сред. Характерные особенности виртуализации с точки зрения ИБ. Угрозы безопасности виртуальным инфраструктурам. Основные требования по обеспечению ИБ виртуальных инфраструктур. Обеспечение ИБ при переходе к «облачным» вычислениям.
	20.	4	**Скрытые каналы утечки информации.** (Часть 1).Утечки информации в статистических БД. (Часть 2). Понятие примеры и классификация скрытых каналов. Методы и средства борьбы со скрытыми каналами. (Часть 3). Общие вероятностные модели - невлияния и невыводимоти. Автоматная модель невмешательства.
	21.	2	**Анонимные сети**. Понятие анонимных сетей. Примеры анонимных сетей. TOR. I2P. Уязвимости. Обнаружение.
	22.	4	**Специальные сети и глобальные сети.** Альтернативные топологии. Проблема маршрутизации. Атаки на интернет.

4.2. Практические занятия

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
3	1.	4	Практическое занятие (групповое упражнение) № 1. Обоснование требований к системе защиты распределенной автоматизированной системы на основе ОС Windows Server от несанкционированного доступа к информации.
	2.	4	Практическое занятие (групповое упражнение) № 2. Разработка решений для защиты от несанкционированного доступа к информации и их развертывание на основе служб каталогов ОС Windows Server.
4	3.	4	Практическое занятие (групповое упражнение) № 3. Обоснование требований к системе защиты вычислительной сети от активных атак и сетевых вторжений.
	4.	4	Практическое занятие (групповое упражнение) № 4. Разработки технических решений по защите вычислительной сети на основе систем обнаружения и предупреждения вторжений (IDS/IPS), их развертывание в сети и настройка.

4.3. Лабораторные работы

Номер модуля дисциплины	Номер лабораторной работы	Объем занятий, часы	Краткое содержание
1	1.	4	Выявление угроз несанкционированного доступа к конфиденциальной информации.
2	2.	4	Технологии управления доступом: идентификация и аутентификация. Управление потоками информации.
3	3.	4	Технология изолированной среды (chroot, apparmor, sandboxie)
	4.	4	Технологии аудита доступа к объектам ОС
	5.	4	Технологии восстановления системного и прикладного программного обеспечения после сбоев и отказов оборудования и программно-математического воздействия средствами ОС Windows»
	6.	4	Технологии проверки целостности данных и резервирование:

Номер модуля дисциплины	Номер лабораторной работы	Объем занятий, часы	Краткое содержание
			надежность данных в ОС Linux.
	7.	4	Сбор информации о сети стандартными сетевыми утилитами
	8.	4	Внешняя разведка - контроль и сканирование сетей.
	9.	4	Межсетевой экран. Настройка межсетевого экрана.
	10.	4	Анализ защищенного протокола SSL\TLS
	11.	4	Создание зашифрованных каналов с помощью OpenVPN.
4	12.	4	Скрытый канал для передачи данных ICMP Tunnel».

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к лабораторной работе № 1:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	4	**Подготовка к компьютерному тестированию (РК1)** Изучение материалов лекции №№ 1 – 3 и рекомендованной литературы.
2	6	**Подготовка к лабораторной работе № 2:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	4	**Подготовка к компьютерному тестированию (РК2)** Изучение материалов лекции №№ 4 – 13 и рекомендованной литературы.
3	6	**Подготовка к лабораторной работе № 3:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	6	**Подготовка к лабораторной работе № 4:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	6	**Подготовка к лабораторной работе № 5:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	4	**Подготовка к лабораторной работе № 6:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	6	**Подготовка к лабораторной работе № 7:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	6	**Подготовка к лабораторной работе № 8:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	6	**Подготовка к лабораторной работе № 9:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	6	**Подготовка к лабораторной работе № 10:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	6	**Подготовка к лабораторной работе № 11:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	3	**Подготовка к практическому занятию № 1:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	3	**Подготовка к практическому занятию № 2:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	4	**Подготовка к компьютерному тестированию (РК3)** Изучение материалов лекции №№ 1 – 3 и рекомендованной литературы.
4	4	**Подготовка к лабораторной работе № 12:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.6

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	2	**Подготовка к практическому занятию № 3:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	2	**Подготовка к практическому занятию № 4:** Изучение материалов лекции и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы. Подготовка отчета.
	4	**Подготовка к компьютерному тестированию (РК4)** Изучение материалов лекции и рекомендованной литературы.

4.5. Примерная тематика курсовых работ

Не предусмотрены

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. Угрозы безопасности информации, обрабатываемой в автоматизированных системах и вычислительных сетях:

Тексты лекций № 1 - 2. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по проведению лабораторной работы № 1. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Основные технологии идентификации и аутентификации при обеспечения безопасности информации, обрабатываемой в автоматизированных системах и сетях:

Тексты лекций № 3 – 7. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по проведению лабораторной работы № 2. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 3. Основные технологии обеспечения конфиденциальности и целостности информации, обрабатываемой в автоматизированных системах:

Тексты лекций № 8 - 15. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 3 - 11 и п.з. №1. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению практических занятий (групповых упражнений) № 1 и 2: ОРИОКС// URL: http://orioks.miet.ru/

Модуль 4. Особенности и проблемные вопросы обеспечение информационной без-

опасности обрабатываемой в автоматизированных системах и сетях:

Тексты лекций № 16 – 22. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по проведению лабораторной работы № 12: ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению практических занятий (групповых упражнений) № 3 и 4: ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. 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.

2. 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.

3. 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.

4. 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 .

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. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 30.11.2020) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации".

4. Постановление Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (ред. от 30.11.2020)

5. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией огра-

ниченного распространения в федеральных органах исполнительной власти»;

6. 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.)

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

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

9. 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.

10. 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.

11. 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.

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

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

14. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования; Computers technique. Information protection against unauthorised access to information. General technical requirements: Национальный стандарт РФ: Введ. 01.01.1996: М.: Издательство стандартов, 1995 Стандартинформ, 2006.- URL: https://docs.cntd.ru/document/9039120 (дата обращения 16.03.2021).- Текст: электронный.

15. 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.

16. 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.

17. 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: 10.03.2021)- Текст: электронный.

18. 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.

19. 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: 16.03.2021). - 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: 15.03.2021). - 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: 15.03.2021). - 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 реализации 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:	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.

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	
Учебная аудитория № 3225: «Программно-аппаратных средств обеспечения информационной безопасности»	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: КорпусInWin S617 450W; Монитор 22" Samsung S22B370H Red Black, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 15 шт. 3. Серверное оборудование: Сервер Flagman-G (Сервер): платформа SERVER SYSTEM 2U SATA BLACK SYS-6026T-URF SUPERMICRO; процессор Intel CPUX4C 2530/5.8GT/12M S136 OEM E5630 - 2шт; ИБП Smart-UPS 5000RT Online 5000BA; Маршрутизатор Cisco 2901 w/2 GE,4 EHWIC,2 DSP,256MB CF,512MB DRAM;	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. (Из реестра МИЭТ п.18) – 16 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 16 шт. 5. Неисключительное право на использование операционной системы Microsoft Win Pro 7. (Из реестра МИЭТ п.22) 6. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL. (Из реестра МИЭТ п.18) 7. Неисключительное право на использование DallasLock 8.0-C (СЗИ НСД) (ПО) (до 10) (Из реестра МИЭТ п.17) 8. Неисключительное право на использование сканера безопасности XSpider (Из реестра МИЭТ п.27) 9. Программа поиска и гарантированного уничтожения информации на дис-

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	Точка доступа D-Link DAP-1150; Программно-аппаратный межсетевой экран со средством обнаружения атак IPS Cisco ASA5505-50-AIP5-K8; Коммутатор 2 Cisco SRW2016; Коммутатор 1 Cisco Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image.	ках «TERRIER» (Из реестра МИЭТ п.36) 10. Программный комплекс защиты информации (для сетевой защиты серверов) «Шлюз безопасности» (Из реестра МИЭТ п.38) 11. Сетевой сканер "Ревизор сети" версия 2.0 (Из реестра МИЭТ п.41) 12. Средство контроля защищенности от несанкционированного доступа "Ревизор 2 XP". (Из реестра МИЭТ п.42) 13. Средство создания модели системы разграничения доступа "Ревизор 1 XP". (Из реестра МИЭТ п.43) 14. Средство фиксации и контроля исходного состояния программного комплекса "ФИКС". (Из реестра МИЭТ п.44)
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 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:	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право 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

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-1. ТЗИНСД «Способен обосновывать требования к системе защиты автоматизированной системы от несанкционированного доступа к информации «.

ФОС по подкомпетенции ОПК-2. ТЗИНСД «Способен разрабатывать технические решения по защите автоматизированной системы от несанкционированного доступа к информации».

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 и практические занятия (групповые упражнения).

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

Лабораторные работы и групповые упражнения выполняются каждым студентом индивидуально.

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

11.1. 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 проводиться 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 аппаратуре 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).

11.2. 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 отчетов по лабораторным работам), посещаемость занятий и активность на занятиях, результаты итогового контроля (сда-

ча 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
2	Лабораторная работа № 1	4	2
2	Компьютерный тест КТ-1	2	1
4	Лабораторная работа № 2	4	2
4	Компьютерный тест КТ-2	2	1
5	Лабораторная работа № 3	4	2
6	Лабораторная работа № 4	4	2
7	Лабораторная работа № 5	4	2
8	Лабораторная работа № 6	4	2
9	Лабораторная работа № 7	4	2
10	Лабораторная работа № 8	4	2
11	Лабораторная работа № 9	4	2
12	Лабораторная работа № 10	4	2
13	Лабораторная работа № 11	4	2
14	Практическое занятие (групповое упражнение) № 1	2	1
14	Практическое занятие (групповое упражнение) № 2	2	1
14	Компьютерный тест КТ-3	2	1
15	Лабораторная работа № 12	4	2
16	Практическое занятие (групповое упражнение) № 3	2	1
16	Практическое занятие (групповое упражнение) № 4	2	1
16	Компьютерный тест КТ-4	2	1
16	Посещаемость, активность	6	3
	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 ито-

гового 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 экзаменационную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в экзаменационную ведомость.

РАЗРАБОТЧИК
Доцент кафедры «Информационная безопасность»
Кандидат технических наук _____ П.Л. Пилюгин

Рабочая программа дисциплины «Технологии защиты информации от несанкционированного доступа» 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 /