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

«Управление информационной безопасностью»

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-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	-	**Знания** основные международные и национальные стандарты УИБ. организацию управления информационной безопасностью (УИБ). структуру профилей защиты и содержание задания по безопасности. основы управления рисками информационной безопасности. общие модели угроз безопасности информации. основные положения концепции информационной безопасности организации. основные требования, принципы и подходы к разработке политики безопасности. практики разработки политик управления информационной безопасности. цели и процедуры мониторинга информационной безопасности. организацию службы информационной безопасности. **Умения:** разрабатывать модели угроз безопасности информации; разрабатывать проекты «Концепции информационной безопасности» организации разрабатывать внутренние корпоративные документы, реализующие политики безопасности. **Опыт практической деятельности:** разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.

В результате изучения дисциплины студент должен:

Знать:

- основные международные и национальные стандарты УИБ.
- организацию управления информационной безопасностью (УИБ).
- структуру профилей защиты и содержание задания по безопасности.
- основы управления рисками информационной безопасности.
- общие модели угроз безопасности информации.
- основные положения концепции информационной безопасности организации.
- основные требования, принципы и подходы к разработке политики безопасности.
- практики разработки политик управления информационной безопасности.
- цели и процедуры мониторинга информационной безопасности.
- организацию службы информационной безопасности.

Уметь:

- разрабатывать модели угроз безопасности информации;
- разрабатывать проекты «Концепции информационной безопасности» организации
- разрабатывать внутренние корпоративные документы, реализующие политики безопасности.

Иметь практический опыт:

- разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Управление информационной безопасностью» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 1-м курсе во 2-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».

Знания и умения, полученные в результате изучения дисциплины, используются в 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			
1	2	5	180	84	16	-	48	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
	ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации			
1. Управление информационной безопасностью	84	16	-	48	20	60	16	Компьютерный тест КТ-1. Компьютерный тест КТ-2. Зачеты по ПЗ (ГУ) № 2, 3, 4, 8. 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	**Информационная безопасность - как организационно-технический объект управления.** Информационная безопасность как организационно-технический объект управления. Цели, критерии и ресурсы управления, эволюция подходов к управлению безопасностью – реактивный («продуктовый»), системно-сервисный, интеграционный, инфраструктурный, архитектурный. Управление адекватностью и управление рисками. Тактический уровень управления, текущее (ежедневное) управление функционированием и поддержкой компонентов и комплексов, оперативный уровень управления, управление модернизацией и ростом (масштабированием) комплексов и систем, стратегический уровень управления, управление развитием инфраструктуры и архитектуры безопасности в составе бизнес-процессов и информационных систем организации. Система управления безопасностью, область действия, стратегия построения и внедрения, процессный подход к управлению, задание, идентификация, описание (документирование) и измерение параметров процессов управления безопасностью. Цикличность и непрерывность управления – контроль (мониторинг, аудит), анализ (формирование решения), планирование (бюджетирование, формирование ресурсов, изменение организационной платформы), реализация решения (разработка, закупка, инсталляция, внедрение). Модель непрерывного совершенствования, цикл Шухарта-Деминга в управлении безопасностью. Организационные инструменты управления: внутренние инструменты – стратегия и концепция информационной безопасности, программа и план защиты, политики, внутренние положения, порядки, регламенты и инструкции, внешние инструменты – стандарты, решения (руководящие документы) государственных регуляторов и отраслевых ведомств.
	2.	2	**Стандартизация управления информационной безопасностью.** Организация управления информационной безопасностью и общая структура стандартов информационной безопасности, оценочные стандарты информационной безопасности («Оранжевая книга», ITSEC), «лучшие практики» информационной безопасности (стандарты BSI, BS 7799 / ISO 17799), отечественная и меж-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			дународная деятельность по стандартизации в сфере информационной технологии (20-й, 22-й и 27-й подкомитеты ISO). Стандарты менеджмента информационной безопасности (ISO 13335, ч.1 и 3). Структура и состав серии международных стандартов 270xx, стандартизация требований к системе управления (ISO 27001), процедур ее внедрения (ISO 27003), практических правил управления информационной безопасностью (ISO 27002), система частных менеджментов, на примере управления безопасностью телекоммуникационных услуг (ISO 27011), особенности применения стандартов ISO. Российские гармонизированные стандарты, стандарты российского Центробанка СТО БР ИББС-1.0 и СТО БР ИББС-1.2., стандарт безопасности бизнеса пластиковых карт PCI DSS. Другие стандарты управления информационной безопасности и сопряженные стандарты управления информационными технологиями (ISO 200xx, NIST,), стандартизованные модели управления (COSO, Cobit и ITIL).
	3.	2	**Методология «Общих критериев».** Высокоуровневые понятия информационной безопасности и семантическая сеть их взаимосвязей, объект оценки и пользователи стандарта, типы требований безопасности (функциональные и доверия), иерархия организации и описания требований, классы функциональных требований. Основные структуры стандарта, профиль защиты и задание по безопасности, структура профиля защиты, идентификация профиля, среда безопасности для объекта оценки, цели и требования для объекта оценки и среды, обоснование профиля, профиль защиты как функциональный норматив. Функции и механизмы безопасности, стойкость функции безопасности, уровни стойкости, потенциал нападения, факторы потенциала нападения, методики оценки стойкости функций безопасности и потенциала нападения, каталог требований доверия, оценочные уровни доверия (гарантированности) и безопасности. Этапы оценки и применение стандарта на различных стадиях жизненного цикла информационной системы, достоинства и ограничения методологии, принципиальная открытость подхода, адаптивность процедур и распространимость результатов оценки, развитие подхода (проект E-COFC).

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	4.	2	**Управление рисками.** Минимизация затрат на обеспечение безопасности при заданных требованиях, риск-ориентированный подход, международная практика управления рисками, стандартизация риск-ориентированного подхода (ISO 13335, ч. 2, 27005), понятие и характеристики риска, связь с угрозами и уязвимостями, ценность (стоимость) информационного актива, снижение ценности актива (коэффициент потери), вероятность реализации угрозы, триггер-идентификатор риска, модель угроз как результат анализа рисков. Модель безопасности с полным перекрытием, дву- и трехдольные графы на множествах объектов, угроз и средств безопасности, параметры ребер и вершин этих графов, теоретическая система обеспечения безопасности Клементса. Технология анализа рисков, методы идентификации и оценивания рисков, допустимый уровень рисков, оценка рисков экспертными методами, оценка субъективной вероятности, методы оценки непрерывных распределений, агрегирование субъективных вероятностей, многомерные функции полезности. Использование анализа рисков для создания и поддержания политик безопасности различных уровней, выбор контрмер, классификаторы контрмер, корпоративная методика анализа рисков, учет остаточных рисков.
	5.	2	**Модель угроз безопасности информации.** Угроза как диалектика взаимодействия атаки (катастрофы) и уязвимости, объект и субъект угрозы источник и канал потенциальной реализации угрозы, виды системной классификации угроз, факторы (аспекты) системной классификации. Ретроспективный метод формирования модели угроз, модель нарушителя, нормативные требования по формированию моделей угроз и нарушителя, подходы к стандартизации моделей угроз и нарушителя. Общая методология формирования модели угроз, определение условий создания и процессов использования информационных ресурсов, описание форм представления данных в информационной системе, выявление и идентификация сведений, сопутствующих основным информационным процессам (источники косвенных угроз). Адаптация базовой модели угроз для использования в конкретной информационной системе (частная модель), оценка полноты базовой модели, инструментальная оценка актуальности угроз базовой

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			модели, стандартизованные каталоги и классификаторы угроз, актуализация множества угроз, вероятность реализации угрозы, опасность угрозы (характер и размеры потенциального ущерба), условные угрозы как предпосылки эшелонированной защиты.
	6.	2	**Концепция безопасности организации.** Роль концепции в процессах управления информационной безопасности. Принципы фундаментальности и декларативности при создании концепции ИБ как системы взглядов на обеспечение безопасности, три базовых вопроса концепции ИБ: что защищаем, от чего (кого) защищаем и как защищаем, связь стратегии безопасности с информационными процессами в организации. Основные (обязательные, типовые) положения концепции, определение безопасной информационной деятельности организации, определение целей, задач и принципов безопасности в терминах основной деятельности, определение области действия концепции и соотнесение ее с внешним нормативным пространством. Установление состава и структуры информационных ресурсов, подлежащих защите (объекта угроз), моделей угроз и нарушителя (субъекта угроз). Определяющая роль концепции по отношению к политикам безопасности следующего уровня, формирование системы полномочий и ответственности за реализацию и поддержку концепции жизненный цикл концепции безопасности.
	7.	2	**Политики безопасности.** Понятие политики безопасности. Основные требования, принципы и подходы к разработке политики безопасности, компромисс между защищенностью и производительностью. Многоуровневый подход, эволюция (детализация) и адекватность требований безопасности на разных уровнях политик. Структура политики информационной безопасности (организационные и технические компоненты), область действия и цикл жизни политики безопасности, непрерывность и цикличность развития политики безопасности. Политика обеспечения информационной безопасности и политика безопасности организации, политика управления информационной безопасностью. Диалектика взаимодействия процессов формирования (поддержания) политик безопасности и процессов проектирования (разви-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			тия) средств защиты информации, разрешение на уровне политик ресурсных конфликтов с основными информационными процессами. Политики безопасности видов информационной деятельности и политики видов информационной защиты, типовые направления создания политик. Процесс разработки политики безопасности, организационные аспекты (постановка задачи, мотивация, обеспечение и контроль) процесса разработки. Инструментальные системы разработки и управления политиками безопасности, справочники детализации требований к политикам безопасности, роль политик в стандартах безопасности.
	8.	2	**Организация службы информационной безопасности.** Структура и содержание организационно-управленческой деятельности в сфере безопасности, работа с политиками, инцидентами, внутренний аудит, организационно-технические мероприятия, организация режима секретности. Концепции должностных лиц различных уровней по вопросам информационной безопасности, руководители организации (ответственные за информатизацию и за безопасность), офицеры (менеджеры) подразделения безопасности, информационно-технологические руководители, администраторы информационных систем и безопасности, пользователи. Служба (департамент) информационной безопасности, типовые задачи и функции службы (формирование, поддержка и документальное обеспечение политик, внедрение средств защиты, администрирование информационных систем и средств защиты, контроль выполнения политик и аудит безопасности, реагирование на инциденты), организационная структура и персонал службы, взаимодействие с другими организационными структурами и должностными лицами в процессе управления безопасностью, правовой статус службы, баланс полномочий и ответственности в сфере безопасности.

4.2. Практические занятия

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
1.	1.	4	**Практическое занятие (семинар). Стандарты в области информационной безопасности** ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса. ГОСТ Р 54582-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия. Стандарты менеджмента информационной безопасности (ISO 13335, ч.1 и 3). Структура и состав серии международных стандартов 270xx, стандартизация требований к системе управления (ISO 27001), процедур ее внедрения (ISO 27003), практических правил управления информационной безопасностью (ISO 27002), система частных менеджментов, на примере управления безопасностью телекоммуникационных услуг (ISO 27011), особенности применения стандартов ISO. Российские гармонизированные стандарты, стандарты российского Центробанка СТО БР ИББС-1.0 и СТО БР ИББС-1.2., стандарт безопасности бизнеса пластиковых карт PCI DSS. Другие стандарты управления информационной безопасности и сопряженные стандарты управления информационными технологиями (ISO 200xx, NIST,), стандартизованные модели управления (COSO, Cobit и ITIL): область применения, основные положения содержания, практическое использование в процессах проектирования и оценки систем безопасности.
	2.	4	**Практическое занятие (групповое упражнение). Анализ рисков информационной безопасности.** Расчет и анализ рисков с помощью методик CRAMM, Microsoft, FRAP, OCTAVE и RiskWatch, категоризация потенциальных потерь, составление расчетных таблиц, обсуждение практики применения программных продуктов АванГард, Риск Менеджер, Кондор+. Расчет экономических показателей эффективности: совокупной стоимости активов информационной безопасности (TCO) и возврата инвестиций (ROI), на примере информационной системы страховой компании
	3.	4	**Практическое занятие (групповое упражнение). Разработка «Модели угроз безопасности информации» и «Модели нарушителя»** (на примерах методологии Центробанка РФ и персональных данных, методика отбора угроз IBM, модель нарушителя в документах ФСБ РФ, методика эмпирического моделирования

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			«Элвис+», систематическое моделирование в информационной практике ФНС РФ).
	4.	4	**Практическое занятие (групповое упражнение). Разработка проекта «Концепции информационной безопасности» организации** (на примерах государственного учреждения, организации кредитной сферы и коммерческой непроизводственной структуры).
	5.	4	**Практическое занятие (семинар). Практика управления информационной безопасностью.** Практика управления безопасностью персональных данных, эволюция общей концепции (правовые и технические аспекты) на примере развития нормативной базы, функции государственных регуляторов, типовые и специальные системы, категоризация систем, методы и правовая основа обезличивания персональных данных, практические примеры решений в области здравоохранения и образования.
	6.	4	**Практическое занятие (семинар). Практика разработки политик управления информационной безопасности** Практика разработки политик сервисов информационной безопасности (управление доступом к информационным ресурсам, шифрование данных, использование паролей, защита от вредоносного программного обеспечения, аутентификация, инфраструктура открытых ключей) Практика разработки политик технических мер безопасности внутренней зоны и электронной почты (использование информационных активов и инфраструктуры, подключение во внутренней зоне, управление правами, использование электронной почты, хранение и перенаправление сообщений, обмен почтовыми сообщениями с внешней зоной). Практика разработки политик технических мер сетевой безопасности, защиты периметра и контента (межсетевые экраны, VPN, обнаружения сетевых атак и аномальной активности, доступ во внутренней зоне через модем, удаленный доступ, беспроводной доступ, демилитаризованная зона, использование Интернет-ресурсов, контентная фильтрация, защита от утечек) Практика разработки политик мониторинга событий безопасности на примере решений IBM (TSIEM), Symantec (SSIM) и на базе открытого кода (OSSIEM).
	7.	4	**Практическое занятие (семинар). Практика разработки политик управления информационной безопасности** Практика разработки политик обеспечивающих технических мер безопасности (физическая защита инфраструктуры и информационных активов, резервное копирование и аварийное восстановление, повторное использование и очистка ресурсов, обеспечение

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			безопасности приложений, серверов и Web-активов) Практика разработки политик организационных и организационно-технических меры безопасности (классификация данных, работа с конфиденциальной информацией, передача сведений третьим лицам и организациям, разработка, хранение и распространение программного обеспечения, обновление, контроль версий и внесение изменений в систему, управление квалификацией сотрудников)
	8.	4	**Практическое занятие (групповое упражнение). Разработка внутренних корпоративных документов реализующих политики безопасности:** Разработка инструкции администратора безопасности корпоративной сети. Разработка инструкции пользователя корпоративной системы по работе с Интернет-ресурсами.
	9.	4	**Практическое занятие (семинар). Непрерывность информационной деятельности.** Управление непрерывностью услуг (ITSCM) и управление непрерывностью бизнеса (BCM), как процессы управление информационной безопасностью, критические системы информационной инфраструктуры в России и за рубежом, анализ влияния (критичности) факторов окружения на жизнедеятельность информационных систем организации. Эффективность принимаемых мер по обеспечению непрерывности информационной деятельности (живучести информационных систем). Цели, составляющие виды деятельности и жизненный цикл ITSCM. Стадии управления непрерывностью, предварительные действия в рамках BCM (инициализация и формирование), стадии ITSCM, запуск, формирование требований и стратегии (системы политик управления непрерывностью), реализация (внедрение) и непрерывная эксплуатация. План обеспечения непрерывности услуг и план обеспечения непрерывности бизнеса (BCP), режимы реагирования на возникновение нештатных ситуаций, постепенное, промежуточное, быстрое и немедленное восстановление, аварийная модель угроз информационной безопасности, антикризисное управление безопасностью. Стандартизация (BS 25999 и ГОСТ 53647) управления непрерывностью информационной деятельности и методов оценки эффективности принимаемых мер.
	10.	4	**Практическое занятие (семинар). Оценки эффективности ин-**

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			формационной безопасности. Gap-анализ (анализ упущений) в практике информационной безопасности, методы оценки и метрики эффективности системы информационной безопасности (ISO 27004, NIST 800-55), стандартизация методологии оценки безопасности информационных технологий (ISO 18045), спецификации безопасности (Security benchmark) как основа оценки зрелости системы управления, инструментальные средства контроля защищенности, тестирование на «проникновение». Уровни зрелости системы управления безопасностью, корпоративная программа и модель измерения эффективности управления, меры и процессы измерений, агрегирование и анализ результатов, жизненный цикл программы измерений. Идеализированная модель соотношения "затраты на защиту - ожидаемые потери (уровень защищенности)", виды возможного ущерба в зависимости от нарушаемого критерия безопасности, структура затрат на обеспечение безопасности (предупреждение ущерба), меры по минимизации ущерба, затраты на восстановление информационных активов, учет затрат на безопасность. Экономические модели управления безопасностью, аналитическая модель Хаббарда, потребительский индекс, исходная и добавленная стоимость, портфель технологических активов, модели жизненного цикла искусственных систем и сбалансированных показателей, совокупная стоимость владения (TCO) и возврат инвестиций (ROI).
	11.	4	**Практическое занятие (семинар). Мониторинг событий информационной безопасности.** Цели и процедуры мониторинга безопасности и информационной технологии, уровень мониторинга, влияние на производительность, система и корпоративная политика управления инцидентами, стандартизация управления инцидентами (ISO 18044). Структура факторов фиксации событий, непосредственные и косвенные факторы, понятие первичного сенсора, регистрация события, компоненты описания и проблема унификации формата, общая схема SIEM-решения, категория события, классификаторы событий. События безопасности и инциденты, идентификация инцидента по маске и по контексту безопасности, корреляция событий и инцидентов.

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			Реагирование на события и инциденты, оповещение, отчетность, коррекция структур данных, экстренное реагирование и эскалация решений, использование документов NIST 800-61, защита коммуникаций реагирования, условия для эффективной обработки инцидентов, анализ результатов мониторинга и планирование мер защиты. Расследование инцидентов, сбор и оформление доказательной информации, план расследования, обеспечение сохранности свидетельств инцидента, ограниченность нормативной базы и правоприменительной практики при расследовании инцидентов информационной безопасности, профилактика инцидентов.
	12.	4	**Практическое занятие (семинар). Управление персоналом и защита от инсайдера.** Процедуры подбора, обучения и контроля знаний сотрудников, организационно-психологическая работа, оценка и развитие лояльности персонала, контроль исполнения политик, информирование о проблемах безопасности, корпоративный портал информационной безопасности. Мотивация и ответственность участников управления безопасностью: первые лица организации, руководитель подразделения, CIO, CISO, HR-руководитель, администратор (офицер) безопасности, системный администратор, пользователь. Специфика инсайдерских угроз, классификация инсайдера-вредителя, принципиальная избыточность полномочий пользователя, факторы возникновения избыточности и мероприятия по ее снижению, персонификация политик доступа, сегментация и регламентация функций пользователей, корпоративная политика работы с персоналом. Программно-технические средства предотвращения утечки информации, цели и методика внедрения системы защиты от инсайдера, выявление каналов утечки, анализ «системного ландшафта», классификация контента, защита агрегатов данных, защита на каналах утечки, контроль деятельности пользователя.

4.3. Лабораторные работы

Не предусмотрены

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
	2	**Подготовка к практическому занятию (групповому упражнению) № 2** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 1.
	2	**Подготовка к практическому занятию (групповому упражнению) № 3** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 2.
	2	**Подготовка к практическому занятию (групповому упражнению) № 4** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 3.
	4	**Подготовка к практическому занятию (семинару) № 5** 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) № 6** 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 (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
	2	**Подготовка к практическому занятию (групповому упражнению) № 8** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 4.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	4	**Подготовка к практическому занятию (семинару) № 9** 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 практическому занятию (семинару) № 10** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 6. Подготовка доклада и презентации по одному из вопросов плана занятия
	4	**Подготовка к практическому занятию (семинару) № 11** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 7. Подготовка доклада и презентации по одному из вопросов плана занятия
	4	**Подготовка к практическому занятию (семинару) № 12** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы. Изучение плана проведения семинарского занятия № 8. Подготовка доклада и презентации по одному из вопросов плана занятия
	2	**Подготовка к компьютерному тесту КТ-2** Изучение материалов лекции №№ 4 - 8 и рекомендованной литературы.
	16	**Подготовка курсовой работы**

4.5. Примерная тематика курсовых работ

Тема курсовой «Разработка профиля защиты подсистемы защиты информации»:

1. Подсистема поддержания локальной изолированной среды для запуска и исполнения приложений.
2. Подсистема проверки целостности и восстановления средств поддержания изолированной среды.
3. Подсистема учета использования ресурсов вычислительной инфраструктуры при исполнении приложений.
4. Подсистема гарантированного уничтожения остаточной информации в элементах вычислительной инфраструктуры после исполнения приложений.
5. Подсистема проверки целостности и восстановления средств учета использования вычислительных ресурсов и гарантированного уничтожения остаточной информации.
6. Подсистема создания сетевой изолированной среды для запуска и исполнения приложений.
7. Подсистема контроля сетевой изолированной среды для запуска и исполнения приложений.

8. Подсистема тестирования локальной изолированной среды для запуска и исполнения приложений
9. Подсистема контроля приложений для исполнения в доверенной среде.
10. Подсистема распространения криптографических ключей при локальном хранении результатов.
11. Подсистема распространения криптографических ключей при централизованном хранении результатов.
12. Подсистема аутентификации абонентов при локальном хранении результатов.
13. Подсистема аутентификации абонентов при централизованном хранении результатов.
14. Подсистема управления дискреционным доступом при локальном хранении результатов.
15. Подсистема управления дискреционным доступом при централизованном хранении результатов.
16. Подсистема управления мандатным доступом.
17. Подсистема проверки целостности и восстановления средств аутентификации, распространения криптографических ключей и управления дискреционным доступом при локальном хранении результатов.
18. Подсистема проверки целостности и восстановления средств аутентификации, распространения криптографических ключей и управления дискреционным доступом при централизованном хранении результатов.
19. Подсистема проверки целостности и восстановления средств управления мандатным доступом при локальном хранении результатов.
20. Подсистема проверки целостности и восстановления средств управления мандатным доступом при централизованном хранении результатов.

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 «Управление информационной безопасностью»:

Тексты лекций № 1 – 8. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинаров № 1 - 8. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению практических занятий (групповых упражнений) № 1 – 4: 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 : 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.
6. 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.
7. 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.

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; 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.

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: 10.03.2021)- Текст: электронный.

15. 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: 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 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 ра-	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
	бочее 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.	
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: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	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

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по компетенции ОПК-3. «Способен разрабатывать проекты организационно-распорядительных документов по обеспечению 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 практические занятия (групповые упражнения), семинары и выполнение курсовой работы.

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

Групповые упражнения и курсовая работа выполняются каждым студентом индивидуально.

По результатам выполнения 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 групповым упражнениям

Выполнение студентами групповых упражнений (ГУ) 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 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 исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, оформлять результаты).

Групповое упражнение, как вид учебного занятия проводиться в мультимедийных аудиториях. Продолжительность - не менее двух академических часов.

По каждому ГУ разработаны и утверждены методические указания по их проведению.

Групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория), порядок выполнения работы, контрольные вопросы, учебная и специальная литература.

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

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

Методические рекомендации по выполнению ГУ работ включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ГУ;
- наименование темы ГУ;
- цель 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 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 ГУ студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ГУ;
- ознакомиться с методическими рекомендации по выполнению 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 ГУ;
- подготовить отчеты для заполнения.

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

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

При защите отчета о 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, после чего отчитаться в проделанной работе перед преподавателем.

11.3. Методические указания студентам по подготовке курсовой работы

Тема курсовой «Разработка профиля защиты подсистемы защиты информации» (по выбору студента).

Основные вопросы, подлежащие разработке:

1. Описание функциональности подсистемы, формулировка содержания работы.
2. Разработка фрагмента модели угроз, на защиту от которых ориентирована подсистема, включая угрозы локального и удаленного администрирования.
3. Разработка положений корпоративной концепции безопасности, ограничивающих функциональность подсистемы и политик безопасности, определяющих эту функциональность.
4. Разработка профиля защиты (ISO 15408) для подсистемы, включающего предположения безопасности, угрозы безопасности, цели безопасности (для подсистемы и среды), требования безопасности (функциональные и доверия) с их логическим обоснованием.
5. Разработка спецификаций проектирования, инструкции администратору безопасности по установке и настройке подсистемы и инструкции пользователю по работе с ней.

Структура курсовой работы должна отвечать традиционным требованиям, предъявляемым 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:

- описание функциональности подсистемы, формулировка содержания работы;
- модель угроз, на защиту от которых ориентирована подсистема, включая угрозы локального и удаленного администрирования;
- положения корпоративной концепции безопасности, ограничивающих функциональность подсистемы и политик безопасности, определяющих эту функциональность;
- описание профиля защиты (ISO 15408) для подсистемы, включающего предположения безопасности, угрозы безопасности, цели безопасности (для подсистемы и среды), требования безопасности (функциональные и доверия) с их логическим обоснованием.
- инструкции администратору безопасности по установке и настройке подсистемы и инструкции пользователю по работе с ней.

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, доклады на семинарах), 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)	4	2
6	Практическое занятие (групповое упражнение) № 2	6	3
7	Практическое занятие (групповое упражнение) № 3	6	3
8	Практическое занятие (групповое упражнение) № 4	6	3
9	Практическое занятие (семинар) № 5	4	2
10	Практическое занятие (семинар) № 6	4	2
11	Практическое занятие (семинар) № 7	4	2
12	Практическое занятие (групповое упражнение) № 8	6	3
13	Практическое занятие (семинар) № 9	4	2
14	Практическое занятие (семинар) № 10	4	2
15	Практическое занятие (семинар) № 11	4	2
16	Практическое занятие (семинар) № 12	4	2
16	Компьютерный тест (КТ-2)	4	2
16	Посещаемость, активность	4	2
	Итого за текущий контроль	***68***	***34***
	Итоговый контроль	***32***	***16***
	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, профессор _____ А.Н.Петухов

Рабочая программа дисциплины «Управление информационной безопасностью» 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 /