КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОЕКТИРОВАНИЕ ОРГАНИЗАЦИОННО- РАСПОРЯДИТЕЛЬНЫХ И ЭКСПЛУАТАЦИОННО-ТЕХНИЧЕСКИХ ДОКУМЕНТОВ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Цель дисциплины - является подготовка студентов, обладающих глубокими теоретическими знаниями и практическими навыками в области разработки и внедрения документации для обеспечения информационной безопасности. Студенты должны быть способны эффективно анализировать и применять международные и национальные стандарты для создания и управления организационно-распорядительными и эксплуатационно-техническими документами, обеспечивающими защиту информационных систем. Они должны уметь разрабатывать и внедрять политики безопасности, соответствующие современным требованиям, а также использовать стандартизированные методы и инструменты для обеспечения безопасности и надежности данных в различных организациях.

Задачи: студент должен знать основные стандарты и нормативные документы, регулирующие проектирование и эксплуатацию систем обеспечения информационной безопасности; уметь применять стандарты для разработки организационно-распорядительных и эксплуатационно-технических документов, обеспечивающих защиту информационных систем; владеть методами и инструментами для разработки и внедрения политик безопасности, соответствующих международным и национальным требованиям

2. Место дисциплины в структуре образовательной программы

Дисциплина «Проектирование организационно- распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ОПК-16, ПК-3.3	Системный анализ и принятие решений	**Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности**	

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ОПК-16.1 Имеет практический опыт выявления нарушений информационной безопасности в компьютерных системах и сетях	Знать: основные концепции и принципы информационной безопасности, включая конфиденциальность, целостность и доступность данных, стандарты и нормативные документы в области информационной безопасности (например, ISO/IEC 27001, NIST), типы угроз и уязвимостей компьютерных систем, включая вредоносное ПО, социальную инженерию и DDoS-атаки. Уметь: идентифицировать компоненты компьютерной системы и сети, подлежащие анализу на предмет безопасности, проводить анализ рисков для компьютерной системы, включая оценку вероятности и воздействия угроз, выявлять уязвимости с использованием различных методов, таких как сканирование портов, аудит конфигураций и анализ кода. Владеть: навыками применения методов анализа защищённости компьютерных систем и сетей на практике, навыками выявления, оценки и классификации угроз и уязвимостей в различных типах компьютерных систем (серверы, рабочие станции, мобильные устройства), навыками разработки и реализации рекомендаций по повышению уровня защищённости и доверия к компьютерным системам на основе проведенного анализа.
	ОПК-16.2 Демонстрирует умение анализировать эффективность средств защиты информации в компьютерных системах и сетях	Знать: основные концепции информационной безопасности: понимание принципов конфиденциальности, целостности и доступности данных, стандарты информационной безопасности: знание международных и национальных стандартов (например, ISO/IEC 27001, NIST SP 800-53) и их применение в практике. Уметь: идентифицировать компоненты системы: способность определять ключевые элементы компьютерной системы и сети, которые требуют анализа на предмет защищённости, проводить анализ рисков: умение оценивать риски для компьютерной системы, включая вероятность наступления угроз и их потенциальное воздействие, выявлять уязвимости: способность

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		использовать различные методы и инструменты для обнаружения уязвимостей в программном обеспечении и конфигурациях. Владеть: навыками применения методов анализа: способность эффективно использовать методы и инструменты для анализа защищённости компьютерных систем на практике, навыками выявления и классификации угроз: умение систематически выявлять, оценивать и классифицировать угрозы и уязвимости в различных типах компьютерных систем, навыками разработки рекомендаций: способность разрабатывать и внедрять рекомендации по повышению уровня защищённости и доверия к компьютерным системам на основе проведенного анализа.
ПК-3.3 Способен участвовать в проведении экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-3.3.1 Реализует технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов	Знать: основные концепции информационной безопасности: понимание принципов конфиденциальности, целостности и доступности данных, а также их важности в контексте расследования инцидентов, стандарты и методологии расследования инцидентов: знание международных стандартов (например, ISO/IEC 27037) и методологий, применяемых для сбора и анализа цифровых доказательств. Уметь: идентифицировать компоненты системы для анализа: способность определять ключевые элементы компьютерной системы, которые могут содержать следы преступлений или инцидентов, проводить анализ рисков: умение оценивать риски для компьютерной системы, включая вероятность наступления угроз и их потенциальное воздействие на безопасность, выявлять уязвимости: способность использовать различные методы и инструменты для обнаружения уязвимостей в программном обеспечении и конфигурациях. Владеть: навыками применения методов анализа следов: способность эффективно использовать методы и инструменты для поиска и анализа следов компьютерных преступлений на практике, навыками выявления и классификации угроз: умение систематически выявлять, оценивать и классифицировать угрозы и уязвимости в различных типах компьютерных систем.
	ПК-3.3.2 Применяет методы и средства прогнозирования	Знать: основные концепции и теории прогнозирования: понимание принципов и

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
	возможных путей развития новых видов компьютерных преступлений	подходов к прогнозированию, включая качественные и количественные методы, современные тенденции в области компьютерных преступлений: знание актуальных видов компьютерных преступлений, их характеристик и методов, используемых злоумышленниками. Уметь: анализировать текущие тренды в киберпреступности: способность исследовать и интерпретировать данные о текущих инцидентах и угрозах для выявления возможных будущих направлений развития преступной деятельности, применять методы прогнозирования: умение использовать различные методы (например, статистический анализ, моделирование) для предсказания новых видов компьютерных преступлений, выявлять факторы, способствующие развитию киберпреступлений: способность определять социальные, экономические и технологические факторы, которые могут влиять на эволюцию киберугроз. Владеть: навыками проведения комплексного анализа угроз: способность интегрировать данные из различных источников для создания целостного представления о возможных путях развития киберпреступлений, навыками разработки прогнозов на основе анализа данных: умение формулировать обоснованные прогнозы о будущем развитии компьютерных преступлений на основе собранной информации, навыками взаимодействия с другими специалистами: способность работать в команде с экспертами по безопасности, аналитиками и правоохранительными органами для обмена данными и совместной разработки стратегий защиты.

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			10
1. Контактная работа обучающихся с преподавателем:		35	35
Аудиторные занятия, часов всего, в том числе:		34	34
• занятия лекционного типа		18	18
• занятия семинарского типа:		16	16
практические занятия		16	16
лабораторные занятия		-	-
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		37	37
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		15	15
- выполнение домашних заданий по практическим занятиям		15	15
- подготовка к зачету		7	7
Промежуточная аттестация: зачет		-	-
ИТОГО:	часов	72	72
общая трудоемкость	зач. ед.	2	2

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Раздел 1. Определение информационной безопасности.

Определение и важность информационной безопасности. Основные принципы и методы защиты данных. Роль информационной безопасности в современном обществе.

Раздел 2. Анализ международных и национальных стандартов в области защиты информации, их сходства и различия.

Обзор международных и национальных стандартов защиты информации. Сравнительный анализ и применение стандартов в различных юрисдикциях. Взаимодействие стандартов на глобальном уровне.

Раздел 3. Специфика стандартизации и стандарты сетевой безопасности в интернете.

Стандартизация и интернет-безопасность. Основные стандарты, регулирующие безопасность в сети. Проблемы и вызовы стандартизации в цифровой среде.

Раздел 4. Характерные черты государственных стандартов для

программного обеспечения.

Государственные требования к программному обеспечению в области безопасности. Особенности разработки и сертификации программных продуктов. Влияние стандартов на качество и надежность программных решений.

Раздел 5. Основные положения государственных стандартов.

Основные положения и структура государственных стандартов в области информационной безопасности. Принципы разработки и внедрения стандартов. Роль стандартов в обеспечении национальной безопасности.

Раздел 6. Регламентирующий документ Гостехкомиссии: межсетевые экраны.

Руководящие документы Гостехкомиссии. Особенности применения межсетевых экранов для защиты информации. Практические аспекты использования данных документов.

Раздел 7. Принципы сертификации на примере средств защиты информации.

Процессы и методы сертификации средств защиты информации. Основные этапы и требования сертификации. Роль сертификации в обеспечении доверия к системам безопасности.

Раздел 8. Сертификация на соответствие нормам информационной безопасности.

Критерии и процедуры сертификации для соответствия требованиям безопасности информации. Методы оценки и подтверждения соответствия. Влияние сертификации на уровень защиты информации.

Раздел 9. Системы сертификации средств защиты информации и требования к безопасности данных.

Структура и функционирование систем сертификации. Требования к средствам защиты информации в контексте сертификации. Взаимодействие систем сертификации с другими элементами информационной безопасности.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
1	Раздел 1. Определение информационной безопасности.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
2	Раздел 2. Анализ международных и национальных стандартов в области защиты информации, их сходства и различия.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
3	Раздел 3. Специфика стандартизации и стандарты сетевой безопасности в интернете.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
4	Раздел 4. Характерные черты государственных стандартов для программного обеспечения.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
5	Раздел 5. Основные положения государственных стандартов.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
6	Раздел 6. Регламентирующий документ Гостехкомиссии: межсетевые экраны.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
7	Раздел 7. Принципы сертификации на примере средств защиты информации.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
8	Раздел 8. Сертификация на соответствие нормам информационной безопасности.	2	2	4	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
9	Раздел 9. Системы сертификации средств защиты информации и требования к безопасности данных.	2	-	5	ОПК-16, ОПК-16.1, ОПК-16.2, ПК-3.3, ПК-3.3.1, ПК-3.3.2
	Всего	**18**	**16**	**37**	

6. Практические занятия

№ п/п	Наименование раздела, темы	Содержание практических занятий	Объем (час.)

	дисциплины		Очная форма обучения
1.	Практическая работа 1. Основы информационной безопасности.	Ознакомление студентов с основными понятиями и принципами информационной безопасности, изучение методов защиты информации и формирование практических навыков оценки рисков и угроз в области кибербезопасности. Информационная безопасность — состояние защищенности информации, обеспечивающее её конфиденциальность, целостность и доступность. Основные принципы информационной безопасности включают: конфиденциальность: защита информации от несанкционированного доступа, целостность: обеспечение точности и полноты информации, доступность: гарантия доступности информации для уполномоченных пользователей. Методы защиты информации: шифрование, авторизация и аутентификация, контроль доступа, резервное копирование, обнаружение вторжений	2
2.	Практическая работа 2. Сравнительный анализ международных и российских стандартов защиты информации.	Изучение основных международных и российских стандартов информационной безопасности, выявление сходства и различий между ними, приобретение навыков сравнительного анализа требований стандартов. Международные стандарты информационной безопасности включают: ISO/IEC 27001: стандарт управления информационной безопасностью организаций, NIST SP 800-серии: серия руководств по защите информации государственных учреждений США, COBIT: Фреймворк управления ИТ-процессами и информационной безопасностью. Российские стандарты информационной безопасности включают: ГОСТ Р 50922-2006: основные положения информационной безопасности, Федеральный закон №152-ФЗ "О персональных данных": регулирует обработку персональных данных, руководящие документы ФСБ России.	2
3.	Практическая работа 3. Стандартизация безопасности в сети Интернет: особенности и ключевые стандарты.	Изучить процесс стандартизации безопасности в Интернете, ознакомиться с ключевыми стандартами, определяющими правила безопасной передачи данных, и научиться анализировать их влияние на инфраструктуру современных сетей. Стандартизация в сфере информационной безопасности играет ключевую роль в обеспечении надежного функционирования Интернета. Она регламентирует механизмы защиты данных, управление доступом и предотвращение киберугроз. Основные направления стандартизации: политики и процедуры управления информацией, методы идентификации и аутентификации, средства защиты от сетевых атак, протоколы шифрования и кодирования данных.	2
4.	Практическая работа 4. Специфика государственных стандартов для программных	Изучение особенностей государственных стандартов, применяемых к программным продуктам, ознакомление с основами сертификации программного обеспечения и понимание важности следования стандартам при создании программных приложений. Государственные стандарты определяют обязательные требования к	2

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
	продуктов.	качеству, функциональности и надежности программных продуктов. Их соблюдение гарантирует пользователям высокий уровень качества ПО и минимизирует риски эксплуатации ненадежных систем. Основные характеристики стандартов: качество продукции, безопасность, совместимость: Продукты должны соответствовать международным стандартам и быть совместимы с существующими системами.	
5.	Практическая работа 5. Общие принципы государственных стандартов.	Ознакомление с общими принципами формирования и реализации государственных стандартов, получение базовых знаний о структуре и содержании национальных стандартов, закрепление навыков самостоятельного изучения нормативных документов. Государственный стандарт является обязательным документом, определяющим минимальные требования к характеристикам продукции, услуг и процессов производства. Государственные стандарты играют важную роль в поддержании высокого уровня качества товаров и услуг, способствуя росту конкурентоспособности отечественных производителей на внутреннем и международном рынках. Принципы стандартизации: обоснованность, единство, научность, перспективность. Виды государственных стандартов: технические регламенты, национальные стандарты, методические документы.	2
6.	Практическая работа 6. Межсетевые экраны: руководящие документы Гостехкоммиссии.	Ознакомление с нормативно-правовым обеспечением и технической документацией, регламентирующей использование межсетевых экранов (брандмауэров), выработка навыков анализа и интерпретации требований государственных стандартов и руководящих документов Гостехкомиссии. Межсетевые экраны являются одним из важнейших элементов защиты компьютерных сетей от несанкционированного доступа и вредоносных воздействий извне. Федеральная служба по техническому и экспортному контролю (ФСТЭК) устанавливает строгие требования к конфигурации и использованию межсетевых экранов. Основные документы Гостехкомиссии: руководящий документ Гостехкомиссии РФ РД "Средства вычислительной техники. Межсетевые экраны. Показатели защищенности.". Приказ ФСТЭК №17 "Об утверждении Положения о порядке аттестации средств защиты информации"	2
7.	Практическая работа 7. Введение в сертификацию средств защиты информации. помещений, Звукоизоляция.	Получение начальных сведений о процедуре сертификации средств защиты информации (СЗИ), освоение процедур оценки соответствия и подготовка материалов для прохождения сертификации. Сертификация средств защиты информации представляет собой процедуру официального признания соответствия определённым критериям безопасности. Эта процедура необходима для подтверждения того, что средства защиты соответствуют установленным нормам и правилам, гарантирующим надежную защиту	2

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
		информации. Основные виды сертификатов: сертификат соответствия, аттестация объекта информатизации. Процедура сертификации включает несколько этапов: подготовка исходных данных, тестирование и экспертиза, оформление заключения, получение сертификата.	
8.	Практическая работа 8. Процесс сертификации на соответствие требованиям информационной безопасности	Освоение последовательности действий, необходимой для успешного прохождения процедуры сертификации информационных систем и средств защиты информации (СЗИ) на соответствие требованиям информационной безопасности. Процесс сертификации информационных систем и средств защиты информации направлен на подтверждение их соответствия установленным требованиям безопасности. Этот процесс необходим для гарантированной защиты информации и снижения потенциальных рисков. Основные этапы сертификации: 1. Предварительная оценка готовности. 2. Подготовка пакета документов. 3. Экспертиза и тестирование. 4. Принятие решения о выдаче сертификата. 5. Периодический контроль состояния сертифицированной системы. Документы, требуемые для сертификации: - заявка на проведение сертификации. - документация на систему или средство защиты информации. - акты проведенных испытаний и проверок. Основные организации, проводящие сертификацию: - Федеральная служба по техническому и экспортному контролю (ФСТЭК). - Центры сертификации Федеральной службы безопасности (ФСБ).	2
9	Практическая работа 9. Требования безопасности в системах сертификации средств защиты информации.	Изучение специфики требований безопасности, установленных государственными органами, для средств защиты информации (СЗИ), знакомство с процессом сертификации таких средств и освоение методик оценки соответствия этим требованиям. Система сертификации средств защиты информации регулируется рядом нормативных актов и ведомственных инструкций. Наиболее важными документами, определяющими требования безопасности, являются: - Постановление Правительства РФ №156 «Об утверждении Правил оказания услуг связи». - Приказ ФСТЭК №17 «Об утверждении Положения о порядке аттестации средств защиты информации». - Руководящие документы ФСБ России («Регламентация использования средств защиты информации»). Основные требования безопасности включают: - Конфиденциальность передаваемых данных. - Целостность информации и защита от несанкционированного изменения. - Доступность ресурсов для легитимных пользователей. - Устойчивость к внешним воздействиям и противодействие попыткам взлома.	-
	Всего		**16**

7. Лабораторные работы

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Проектирование организационно- распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Зачетно-экзаменационные материалыдля промежуточной аттестации (экзамен/зачет)

1.Что такое организационно-эксплуатационная техническая документация в контексте информационной безопасности?

2. Роль и место организационной защиты в структуре мер по защите информации.

3. Основные принципы организационной защиты информации.

4. Организационные мероприятия по обеспечению информационной безопасности

5. Какие основные этапы проектирования организационно-эксплуатационной технической документации?

6. Какие документы входят в состав организационно-эксплуатационной технической документации?

7. Какие системы безопасности должны быть учтены при проектировании организационно- эксплуатационной технической документации?

8. Что такое "политика информационной безопасности" и как она связана с организационно- эксплуатационной технической документацией?

9. Какие методы и подходы можно использовать при разработке организационно-эксплуатационной технической документации?

10. Какие требования часто включаются в организационно-эксплуатационную техническую документацию для обеспечения безопасности информационных систем?

11. Какие риски и угрозы необходимо учитывать при проектировании организационно- эксплуатационной технической документации в сфере информационной безопасности?

12. Как организовать эффективное взаимодействие между различными заинтересованными сторонами при разработке организационно-эксплуатационной технической документации?

13. Назовите основные организационно-технические мероприятия по защите информации.

14. Что включают в себя организационные средства обеспечения защиты информации?

15. Что включают в себя правовые средства обеспечения защиты информации?

16. Какие основные разделы должны включать документы по обеспечению информационной безопасности организации?

17. Какие требования должны быть учтены при разработке инструкций по использованию информационных систем?

18. Какие факторы необходимо учитывать при разработке политики управления доступом к информационным ресурсам организации?

19. Какие основные шаги следует выполнить при разработке эксплуатационной документации для информационной системы?

20. Какие меры безопасности должны быть учтены при разработке процедур резервного копирования и восстановления данных?

21. Объясните концепцию "жизненного цикла документации" и

опишите основные этапы этого
цикла.

22. Какие меры безопасности следует учитывать при проектировании организационно-
эксплуатационная техническая документация (ОЭТД)?

23. Какие изменения и обновления могут потребоваться в процессе эксплуатации ОЭТД?

24. Какие требования нормативно-правового характера необходимо учитывать при разработке ОЭТД?

25. Какие роли и ответственности назначаются при разработке и эксплуатации ОЭТД?

26. Какая роль соответствия стандартам и регулятивным требованиям играет при проектировании ОЭТД?

27. Какие основные цели и задачи проектирования организационно-эксплуатационной технической документации (ОЭТД) в сфере обеспечения информационной безопасности

28. Какие основные документы обычно включаются в состав ОЭТД в области информационной безопасности?

29. Какое значение имеет обучение пользователей по вопросам информационной безопасности при внедрении ОЭТД?

30. Какие обязанности пользователей следует учесть в рамках безопасного использования документов?

31. Концепция и политики ИБ на предприятии. Основные разделы концепции.

32. Концептуальная модель безопасности информации организации (предприятия).

33. Опишите процесс отнесения сведений к государственной тайне.

34. Опишите процесс отнесения сведений к конфиденциальной информации.

35. Охарактеризуйте законодательство РФ об информации, информационных технологиях и о защите информации. Раскройте основные положения ФЗ№149.

36. Федеральная служба по техническому и экспортному контролю (ФСТЭК России), ее функции и полномочия в информационной сфере.

37. Федеральная служба безопасности Российской Федерации, ее функции и полномочия в информационной сфере.

38. Аттестация объектов информатизации. Основные требования согласно нормативному документу ФСТЭК "Положение по аттестации объектов информатизации по требованиям безопасности информации".

39. Какие последствия могут возникнуть в случае невыполнения требований, изложенных в документах по информационной безопасности?

40. Какой документ выдается по окончании аттестационных мероприятий по системе защиты организации?

41. Есть ли требования для состава комиссии для аттестации системы.

42. Что такое акт классификации?

43. В чем отличие между ИСПДн и ГИС?
44. Какие основные разделы должны быть в техническом паспорте?
45. Оцените степень важности правильного составления модели угроз
46. Какие виды инструкций по системе безопасности вы знаете?
47. Опишите содержание каждого из вида инструкций
48. Организации по аттестации информационных систем.
49. Какой принцип работы у данных организаций
50. Какое требование для организации должно быть на данный вид деятельности.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-45723-6. — Текст : электронный // Лань : электронно-библиотечная система. — [Электронный ресурс] URL: https://e.lanbook.com/book/311825 .
2. Петренко В.И., Мандрица И.В. Защита персональных данных в информационных системах. Практикум. – М. Лань, 2022 - 108 с. [Электронный ресурс] – URL: https://lanbook.com/catalog/informatika/zashchita- personalnykh-dannykh-v-informatsionnykh-sistemakh-praktikum/
3. Кудашкин Я. В. Правовое обеспечение безопасности обработки персональных данных в сети интернет. Автореф. дис. на соискание уч. ст. к.ю.н. Специальность: 12.00.13 –Информационное право. Москва – 2019. [Электронный ресурс] – URL: https://istina.msu.ru/download/212806666/1hiKtk:UrCunoF4PcIPFMt1qAIZRF_dTmA/
4. Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы X Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской, М.Ю. Рытова. – Брянск: БГТУ, 2018. – 187 с. [Электронный ресурс] – URL: https://www.tu-bryansk.ru/upload/medialibrary/8d4/Konf_IB_2018.pdf

Дополнительная литература:

1. Лапина М. А. Защита персональных данных в информационных системах / М. А. Лапина, М. В. Песков. – Ставрополь: Изд-во СКФУ, 2014. – 199 с. [Электронный ресурс] – URL: https://www.ncfu.ru/export/uploads/imported-from-dle/op/doclinks2015/Metod_UPPDN_10.05.03_19.05.15.pdf

2. Комплексные системы защиты информации предприятия: учебное пособие / В.Т. Еременко, М.Ю. Рытов, О.М. Голембиовская, П.Н. Рязанцев. – Орел: ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. –116 с. [Электронный ресурс] – URL: https://studfile.net/preview/16707511/page:12/#16707511

3. Такидзе Д.Т. Защита персональных данных в России. // Вестник магистратуры. 2021 №5-4 (116) с. 108-111. [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/zaschita- personalnyh-dannyh-v-rossii

4. Виссия, Х. Э. Принятие решений в информационном обществе : учебное пособие / Х. Э. Виссия, В. В. Краснопрошин, А. Н. Вальвачев. — Санкт-Петербург : Лань, 2022. — 228 с. — ISBN 978-5-8114-3747-4. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс] — URL: https://e.lanbook.com/book/206723 .

5. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с. [Электронный ресурс] – URL: https://books.ifmo.ru/file/pdf/2372.pdf

6. Исаев А.С., Хлюпина Е.А. «Правовые основы организации защиты персональных данных» – СПб: НИУ ИТМО, 2014. – 106 с. [Электронный ресурс] – URL: https://books.ifmo.ru/file/pdf/1570.pdf

7. Кондрашов А.Э., Варламова Л.Н. Национальные стандарты РФ по различным аспектам защиты информации и информационной безопасности. [Электронный ресурс] – URL: https://www.top-personal.ru/officeworkissue.html?510

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) – 1.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____