МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
проф. Таюрский Д.А.
"___"_____20___ г.

Программа дисциплины

Комплексное обеспечение информационной безопасности Б1.Б.31

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017
Автор(ы): Ситников С.Ю.
Рецензент(ы): Шерстюков О.Н.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Шерстюков О. Н.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Института физики:
Протокол заседания УМК No ____ от "____" _____ 20__г.

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) Ситников С.Ю.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты;
ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требований стандартов в области информационной безопасности;

Выпускник, освоивший дисциплину:

Должен знать:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспе-чения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодей-ствия, основные мероприятия по созданию и обеспечению функционирования комплекс-ной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

Должен уметь:

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информаци-онной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формули-ровать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации.

Должен владеть:

Владеть:

навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима.

Должен демонстрировать способность и готовность:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспе-чения информационной безопасности, основные составляющие проблемы и концепту-альные положения, угрозы информационной безопасности и меры защиты и противодей-ствия, основные мероприятия по созданию и обеспечению функционирования комплекс-ной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информаци-онной безопасности и комплексной защиты информации на предприятии и в организа-ции; строить концептуальные модели информационной безопасности объекта, формули-ровать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации.

Владеть:

навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима.

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Данная учебная дисциплина включена в раздел "Б1.Б.31 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность автоматизированных систем)" и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, в 7 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы), 144 часа(ов).

Контактная работа - 72 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа (ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 7 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине/ модулю

N	Раздел дисциплины/ модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности	7	4	0	2	6
2.	Тема 2. Концептуальные положения организационного обеспечения ИБ	7	4	0	2	6
3.	Тема 3. Информационная безопасность на объекте	7	4	0	2	6
4.	Тема 4. Конфиденциальная информация	7	4	0	2	6
5.	Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ	7	4	0	2	6
6.	Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ	7	4	0	2	6
7.	Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО	7	4	0	2	6
8.	Тема 8. Технология защиты от угроз экономической безопасности	7	4	0	2	6
9.	Тема 9. Требования и рекомендации по защите информации	7	4	0	2	6
	Итого		36	0	18	54

4.2 Содержание дисциплины

Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности

1.1 Задачи и методы комплексного обеспечения ИБ. Содержание основных используемых в ИБ понятий. Определение за-щиты информации. Основные методы обеспечения ИБ.

1.2 Проблема ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования системы ЗИ. Эле-менты эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида про-блем.

1.3. Основные составляющие ИБ. Категории спектра интересов, свя-занных с использованием инф. си-стем. Понятия доступности, целост-ности и конфиденциальности, их смысл в контексте проблемы ИБ.

Тема 2. Концептуальные положения организационного обеспечения ИБ

2.1. Общие сведения о доктрине и концепции организационного обеспе-чения безопасности. Цель и область применения концепции. Основания и исходные данные для разработки кон-цепции.

2.2. Задачи обеспечения нацио-нальной безопасности в информа-ционной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

Тема 3. Информационная безопасность на объекте

3.1 Угрозы ИБ на объекте. Источ-ники угроз безопасности. Деление источников угроз на группы, субъек-ты угроз. Виды угроз безопасности, классификация. Дополнительное де-ление на внутренние и внешние угро-зы. Каналы утечки информации.

3.2 Модель угроз безопасности на объекте. Методы защиты. Основ-ные группы методов (способов) за-щиты информации. Основные уровни защиты.

3.3 Принципы комплексной защи-ты информации. Основные принци-пы. Расшифровка понятий.

3.4 Система обеспечения ИБ, общие сведения об ИТКС. Стадии создания системы обеспечения безопасности. Организационные и технические мероприятия на каждой из стадий. Мероприятия, проводимые в процессе эксплуатации ИТКС. Понятие необходимого уровня защиты.

Тема 4. Конфиденциальная информация

4.1. Организация службы безопас-ности объекта. Отношения объекта и субъекта в информационном про-цессе с противоположными интере-сами с позиции активности в дей-ствиях. Определение понятия утеч-ки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфи-денциальной информацией. Каналы, способы и средства. Формы и мето-ды недобросовестной конкуренции в контексте проблемы защиты ин-формации. Совокупность определе-ний, способов и средств НСД к ин-формации на объекте.

4.2. Направления обеспечения ИБ на объекте. Нормативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характери-стики. Средства и методы организа-ционной защиты. Определение орга-низационной защиты. Состав меро-приятий организационной защиты.

4.3. Специальные штатные служ-бы и структуры ЗИ. Служба без-опасности предприятия, её струк-турные единицы. Задачи службы безопасности предприятия.

4.4. Концепция создания физиче-ской защиты важных объектов. Основные термины и определения. Система физической защиты, опре-деление. Деление СФЗ на подсисте-мы. Стадии проектирования объек-тов защиты. Основные этапы стадии концептуального проекта. Концеп-ция физической безопасности объ-екта. Основные вопросы концепции: предметы защиты, угрозы безопас-ности и модель вероятных исполни-телей угроз, оценка и анализ уязви-мости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ

5.1. Цели, задачи и субъекты ИБ. Основные цели и задачи обеспечения ИБ. Управление ИБ. Классификация субъектов, влияющих на состояние ИБ.

5.2. Организационная структура системы обеспечения ИБ. Регла-ментация действий пользователей и обслуживающего персонала АС. Служба (подразделение) ЗИ. Уровни организационной структуры системы обеспечения ИБ АС организации. Технология обеспечения ИБ.

Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ

6.1. Концепция обеспечения ИБ на предприятии. Документ ?Концепция обеспечения ИБ организации?.

Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО

7.1. Задачи концептуального проектирования. Концептуальный проект. Оценка эффективности вариантов.

7.2. Создание службы безопасности организации. Разрешенные виды деятельности СБ. Организация службы экономической безопасности. Этапы, рекомендуемые при создании СЭБ.

Тема 8. Технология защиты от угроз экономической безопасности

8.1. Общий алгоритм действий и активная модель реагирования. Последовательность операций (дей-ствий). Система предупредительных мер. Нестандартные угрозы. Актив-ная модель реагирования.

8.2. Предупредительная работа с персоналом. Индикаторы выявле-ния. Потенциальные нарушители. Проверки персонала, некоторые способы.

Тема 9. Требования и рекомендации по защите информации

10.1. Требования по технической защите информации.

Организация охраны объектов.

11.1. Организационно-пропускной режим на предприятии.

11.2. Подготовка исходных данных.

11.3. Оборудование пропускных пунктов.

11.4. Организация пропускного ре-жима.

Система защиты информации и ее задачи.

12.1. Организационная система за-щиты информации.

Государственная политика и об-щее руководство деятельностью по защите информации.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года N301).

Письмо Министерства образования Российской Федерации N14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Положение от 24 декабря 2015 г. № 0.1.1.67-06/265/15 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение N 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение N 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет""

Регламент N 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Регламент N 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет""

Регламент N 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет""

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 7			
	Текущий контроль		
1	Письменное домашнее задание	ОПК-7	3. Информационная безопасность на объекте

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
	Экзамен	ОПК-7, ПК-10, ПК-13, ПК-14, ПК-15	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Семестр 7					
Текущий контроль					
Письменное домашнее задание	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	1
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.	

6.3 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

Семестр 7

Текущий контроль

1. Письменное домашнее задание

Тема 3

Аспекты информационной безопасности на охраняемом объекте

Экзамен

Вопросы к экзамену:

1.1. Комплексное обеспечение информационной безопасности автоматизированных систем. Системный подход к защите информации.

1.2. Комплексное обеспечение информационной безопасности автоматизированных систем. Основные цели систем защиты информации.

1.3. Комплексное обеспечение информационной безопасности автоматизированных систем. Основные задачи систем защиты информации.

1.4. Методология формирования задач защиты информации.

1.5. Интеграция средств информационной безопасности в технологическую среду.

1.6. Основные этапы проектирования КСИБ, требования к ним. Принципы проектирования систем защиты информации.

1.7. Основные этапы проектирования КСИБ, требования к ним. Основные средства систем защиты информации.

1.8. Основные этапы проектирования КСИБ, требования к ним. Стратегии применения средств защиты информации.

2.1. Порядок и особенности проведения испытаний КСИБ.

2.2. Порядок и особенности внедрения КСИБ в эксплуатацию.

2.3. Мониторинг окружающей среды, выявление каналов несанкционированного доступа. Общие сведения о поисковых мероприятиях.

2.4. Мониторинг окружающей среды, выявление каналов несанкционированного доступа. Перечень поисковых работ.

2.5. Особенности эксплуатации КСИБ на объекте защиты. Основы, направления и этапы защиты информации.

2.6. Особенности эксплуатации КСИБ на объекте защиты. Правовые аспекты защиты информации. Общие сведения.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 7			
Текущий контроль			
Письменное домашнее задание	Обучающиеся получают задание по освещению определённых теоретических вопросов или решению задач. Работа выполняется письменно дома и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1	50
		Всего:	50
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4

- http://znanium.com/catalog.php?bookinfo=402686

Партыка Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - 432 с.: ил.; 60x90 1/16. - (Проф. обр.). (п) ISBN 978-5-91134-246 -http://znanium.com/catalog.php?bookinfo=167284

7.2. Дополнительная литература:

Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 544 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0449-7, 1500 экз. - http://znanium.com/bookread.php?book=207105

Аверченков, В. И. Аудит информационной безопасности [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков. - 2-е изд., стереотип. - М. : Флинта, 2011. - 269 с. - ISBN 978-5-9765-1256-6 - http://znanium.com/catalog.php?bookinfo=453734

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Гарант - http://www.garant.ru/

Консультант Плюс - http://www.consultant.ru/

Официальный портал правовой информации - http://pravo.gov.ru/

Российская газета - http://www.rg.ru/

Собрание законодательства РФ - http://www.szrf.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Реферат - краткое изложение в письменном виде или форме публичного доклада содержания научногао труда (трудов), литературы по теме. Это самостоятельная научно-исследовательская работа студента, где раскрывается суть исследуемой проблемы, приводятся различные точки зрения, собственные взгляды на нее. Содержание реферата должно быть логическим, изложение материала носит проблемно-тематический характер. Отличие доклада от реферата в том, что он отражает одну точку зрения на проблему, не предполагает ее исследования в сравнении и анализе.
Методические рекомендации при работе над рефератом или докладом
1. Сформулировать тему работы, причем она должна быть не только актуальной по своему значению, но оригинальной, интересной по содержанию. Тематика обычно определяется преподавателем, но в определении конкретной темы студент может проявить инициативу.
2. Подобрать и изучить основные источники по теме (как правило, при разработке реферата или доклада используется не менее 8-10 различных источников).
3. Составить библиографию.
4. Обработать и систематизировать подобранную информацию по теме.
5. Разработать план реферата или доклада исходя из имеющейся информации.
6. Написать реферат или доклад на компьютере.
7. Подготовить публичное выступление по материалам реферата или доклада, желательно подготовить презентацию, иллюстрирующую основные положения работы.
План - это 'скелет' текста, компактно отражающий последовательность изложения материала.
Методические рекомендации
1. Составляя план при чтении текста старайтесь определить границы мыслей. Эти места в книге отмечайте. Нужным отрывкам дайте заголовки, формулируя соответствующий пункт плана. Затем снова просмотрите прочитанное, чтобы убедиться, правильно ли установлен 'поворот' содержания, уточните формулировки.
2. Стремитесь, чтобы заголовки-пункты плана наиболее полно раскрывали мысли автора. Последовательно прочитывая текст, составляйте к нему черновой набросок плана с нужной детализацией.
3. Записи делайте так, чтобы ее легко можно было охватить одним взглядом.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Освоение дисциплины "Комплексное обеспечение информационной безопасности" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Освоение дисциплины "Комплексное обеспечение информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность автоматизированных систем .