

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

Автор(ы):

Ситников С.Ю.

Рецензент(ы):

Шерстюков О.Н.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Шерстюков О. Н.

Протокол заседания кафедры No _____ от "_____" _____ 201__ г

Учебно-методическая комиссия Института физики:

Протокол заседания УМК No _____ от "_____" _____ 201__ г

Регистрационный No

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) Ситников С.Ю. , ssitnikov@mail.ru

1. Цели освоения дисциплины

развитие у студентов личностных качеств, а также формирование общекультурных-универсальных (общенаучных, социально-личностных, инструментальных) и профессиональных компетенций в соответствии с требованиями ФГОС ВПО по данному направлению подготовки формирование универсальных (общенаучных, социально-личностных, общекультурных и инструментальных) и профессиональных (общепрофессиональных и профильно-специализированных) компетенций, позволяющих выпускнику успешно работать в избранной сфере деятельности, быть социальной мобильным и устойчивым на рынке труда укрепление равенства, развитие общекультурных потребностей, творческих способностей, социальной адаптации, коммуникативности, толерантности, настойчивости в достижении цели, выносливости и физической культуре

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

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

Дисциплина предназначена для подготовки бакалавров в соответствии с требованиями направления подготовки "Радиофизика", профилем подготовки "Информационная безопасность". Для освоения дисциплины необходимы знания дисциплин: информатика, радиотехника и радиоэлектроника, физические основы информационных систем. Освоение дисциплины будет способствовать успешной профессиональной деятельности, позволит сформировать у будущих специалистов представление о современных методах решения задач, связанных с организационным обеспечением информационной безопасности, построением системы защиты объекта и практическим определением возможных каналов утечки информации на конкретном объекте.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-7 (профессиональные компетенции)	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-13 (профессиональные компетенции)	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

В результате освоения дисциплины студент:

1. должен знать:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

2. должен уметь:

Уметь:

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

3. 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.

4. должен демонстрировать способность и готовность:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать 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.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 7 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи- ческие занятия	Лабора- торные работы	
1.	Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности	7	1	4	0	2	Письменная работа
2.	Тема 2. Концептуальные положения организационного обеспечения ИБ	7	3	4	0	2	Устный опрос
3.	Тема 3. Информационная безопасность на объекте	7	5	4	0	2	Устный опрос
4.	Тема 4. Конфиденциальная информация	7	7	4	0	2	Устный опрос
5.	Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ	7	9	4	0	2	Устный опрос
6.	Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ	7	11	4	0	2	Устный опрос
7.	Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО	7	13	4	0	2	Устный опрос
8.	Тема 8. Технология защиты от угроз экономической безопасности	7	15	4	0	2	Устный опрос
9.	Тема 9. Требования и рекомендации по защите информации	7	17	4	0	2	Устный опрос
.	Тема . Итоговая форма контроля	7		0	0	0	Зачет
	Итого			36	0	18	

4.2 Содержание дисциплины

Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности
лекционное занятие (4 часа(ов)):

1.1 Задачи и методы комплексного обеспечения ИБ. Содержание основных используемых в ИБ понятий. Определение защиты информации. Основные методы обеспечения ИБ. 1.2 Проблема ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования системы ЗИ. Элементы эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида проблем. 1.3. Основные составляющие ИБ. Категории спектра интересов, связанных с использованием инф. систем. Понятия доступности, целостности и конфиденциальности, их смысл в контексте проблемы ИБ.

лабораторная работа (2 часа(ов)):

Стратегия ИБ и её цели. Определение понятия. Главные цели ИБ. Административный уровень ИБ. Программа безопасности и политика безопасности. Процедурный уровень защиты. Уровни детализации политики безопасности, основные документы и их разделы.

Тема 2. Концептуальные положения организационного обеспечения ИБ

лекционное занятие (4 часа(ов)):

2.1. Общие сведения о доктрине и концепции организационного обеспечения безопасности. Цель и область применения концепции. Основания и исходные данные для разработки концепции. 2.2. Задачи обеспечения национальной безопасности в информационной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

лабораторная работа (2 часа(ов)):

Методы работы с персоналом. Понятие и состав персонала, как источника информации. Основные направления сотрудничества сотрудника организации со злоумышленником. Особенности приема сотрудников на работу с информацией ограниченного доступа. Подготовительные этапы, активный и пассивный методы. Технологическая цепочка процесса приема.

Тема 3. Информационная безопасность на объекте

лекционное занятие (4 часа(ов)):

3.1 Угрозы ИБ на объекте. Источники угроз безопасности. Деление источников угроз на группы, субъекты угроз. Виды угроз безопасности, классификация. Дополнительное деление на внутренние и внешние угрозы. Каналы утечки информации. 3.2 Модель угроз безопасности на объекте. Методы защиты. Основные группы методов (способов) защиты информации. Основные уровни защиты. 3.3 Принципы комплексной защиты информации. Основные принципы. 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.

лабораторная работа (2 часа(ов)):

3.5. Предпосылки появления угроз в ИТКС, их возможные разновидности, интерпретация. Определение угрозы ИБ в ИТКС. Существующие классификации угроз и их источников в ИТКС. 3.6. Классификация угроз безопасности в ИТКС по 5 группам различных угроз. Классификация угроз в ИТКС по источнику возможной опасности. Классификация по защите информации от НСД. Четыре уровня угроз в модели нарушителя в АСОД. Классификация угроз по способам их возможного негативного воздействия с описанием способов реализации. Критерии деления множества угроз в ИТКС на классы. Наиболее опасные угрозы ИБ в ИТКС. Воздействия нарушителя на систему на различных этапах функционирования ИТКС, направления воздействия. 3.6. Уязвимости. Причины появления уязвимостей. Воздействия нарушителя на систему через её уязвимости на различных этапах функционирования ИТКС. Реализация угроз через КНПИ. Классификация КНПИ по двум критериям.

Тема 4. Конфиденциальная информация

лекционное занятие (4 часа(ов)):

4.1. Организация службы безопасности объекта. Отношения объекта и субъекта в информационном процессе с противоположными интересами с позиции активности в действиях. Определение понятия утечки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфиденциальной информацией. Каналы, способы и средства. Формы и методы недобросовестной конкуренции в контексте проблемы защиты информации. Совокупность определений, способов и средств НСД к информации на объекте. 4.2. Направления обеспечения ИБ на объекте. Нормативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характеристики. Средства и методы организационной защиты. Определение организационной защиты. Состав мероприятий организационной защиты. 4.3. Специальные штатные службы и структуры ЗИ. Служба безопасности предприятия, её структурные единицы. Задачи службы безопасности предприятия. 4.4. Концепция создания физической защиты важных объектов. Основные термины и определения. Система физической защиты, определение. Деление СФЗ на подсистемы. Стадии проектирования объектов защиты. Основные этапы стадии концептуального проекта. Концепция физической безопасности объекта. Основные вопросы концепции: предметы защиты, угрозы безопасности и модель вероятных исполнителей угроз, оценка и анализ уязвимости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

лабораторная работа (2 часа(ов)):

Концепция создания физической защиты важных объектов. Основные термины и определения. Система физической защиты, определение. Деление СФЗ на подсистемы. Стадии проектирования объектов защиты. Основные этапы стадии концептуального проекта. Концепция физической безопасности объекта. Основные вопросы концепции: предметы защиты, угрозы безопасности и модель вероятных исполнителей угроз, оценка и анализ уязвимости 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

лекционное занятие (4 часа(ов)):

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. Регламентация действий пользователей и обслуживающего персонала АС. Служба (подразделение) ЗИ. Уровни организационной структуры системы обеспечения ИБ АС организации. Технология обеспечения ИБ.

лабораторная работа (2 часа(ов)):

Основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ. Классификация мероприятий. Распределение функций по обеспечению ИБ.

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

лекционное занятие (4 часа(ов)):

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

лабораторная работа (2 часа(ов)):

Категорирование и перечень информационных ресурсов, подлежащих защите. Положение об определении требований по защите (категорировании) ресурсов. Классификация защищаемой информации. Инструкции по организации защиты.

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

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (2 часа(ов)):

Структура службы экономической безопасности

Тема 8. Технология защиты от угроз экономической безопасности

лекционное занятие (4 часа(ов)):

8.1. Общий алгоритм действий и активная модель реагирования. Последовательность операций (действий). Система предупредительных мер. Нестандартные угрозы. Активная модель реагирования. 8.2. Предупредительная работа с персоналом. Индикаторы выявления. Потенциальные нарушители. Проверки персонала, некоторые способы.

лабораторная работа (2 часа(ов)):

Служба безопасности и проверка контрагентов. Причины, снижающие надежность контрагентов. Криминалистическая экспертиза документов. Формирование картотеки клиентов и участие организации в формировании банков данных о контрагентах.

Тема 9. Требования и рекомендации по защите информации

лекционное занятие (4 часа(ов)):

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 режима. Система защиты информации и ее задачи. 12.1. Организационная система защиты информации. Государственная политика и общее руководство деятельностью по защите информации.

лабораторная работа (2 часа(ов)):

Направления формирования системы защиты информации. Этапы реализации концепции защиты информации. Финансирование мероприятий по защите информации. Результаты реализации концепции защиты информации.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности	7	1	подготовка к письменной работе	6	Письменная работа
2.	Тема 2. Концептуальные положения организационного обеспечения ИБ	7	3	подготовка к устному опросу	6	устный опрос
3.	Тема 3. Информационная безопасность на объекте	7	5	подготовка к устному опросу	6	устный опрос

N	Раздел дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Конфиденциальная информация	7	7	подготовка к устному опросу	6	устный опрос
5.	Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ	7	9	подготовка к устному опросу	6	устный опрос
6.	Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ	7	11	подготовка к устному опросу	6	устный опрос
7.	Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО	7	13	подготовка к устному опросу	6	устный опрос
8.	Тема 8. Технология защиты от угроз экономической безопасности	7	15	подготовка к устному опросу	6	устный опрос
9.	Тема 9. Требования и рекомендации по защите информации	7	17	подготовка к устному опросу	6	устный опрос
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

лекция-визуализация, мультимедийная презентация

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

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

Письменная работа , примерные вопросы:

Цели защиты информации на объектах защиты могут быть достигнуты при проведении работ по таким направлениям: - определение охраняемых сведений об объектах защиты; - оценка возможностей и степени опасности технических средств разведки; - выявление возможных технических каналов утечки информации; - анализ возможностей и опасности несанкционированного доступа к информационным объектам; - анализ опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты; - разработка и реализация организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз; - создание комплексной системы защиты; - организация и проведение контроля состояния и эффективности системы защиты информации; - обеспечение устойчивого управления процессом функционирования системы защиты информации. Существует три уровня формирования режима информационной безопасности: - законодательно-правовой; - административный (организационный); - программно-технический.

Тема 2. Концептуальные положения организационного обеспечения ИБ

устный опрос , примерные вопросы:

Реферат на тему "Организационное и правовое обеспечение информационной безопасности"

2.1. Общие сведения о доктрине и концепции организационного обеспечения безопасности. Цель и область применения концепции. Основания и исходные данные для разработки концепции. 2.2. Задачи обеспечения национальной безопасности в информационной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

Тема 3. Информационная безопасность на объекте

устный опрос , примерные вопросы:

3.1 Угрозы ИБ на объекте. Источники угроз безопасности. Деление источников угроз на группы, субъекты угроз. Виды угроз безопасности, классификация. Дополнительное деление на внутренние и внешние угрозы. Каналы утечки информации. 3.2 Модель угроз безопасности на объекте. Методы защиты. Основные группы методов (способов) защиты информации. Основные уровни защиты. 3.3 Принципы комплексной защиты информации. Основные принципы. 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

устный опрос , примерные вопросы:

4.1. Организация службы безопасности объекта. Отношения объекта и субъекта в информационном процессе с противоположными интересами с позиции активности в действиях. Определение понятия утечки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфиденциальной информацией. Каналы, способы и средства. Формы и методы недобросовестной конкуренции в контексте проблемы защиты информации. Совокупность определений, способов и средств НСД к информации на объекте. 4.2. Направления обеспечения ИБ на объекте. Нормативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характеристики. Средства и методы организационной защиты. Определение организационной защиты. Состав мероприятий организационной защиты. 4.3. Специальные штатные службы и структуры ЗИ. Служба безопасности предприятия, её структурные единицы. Задачи службы безопасности предприятия. 4.4. Концепция создания физической защиты важных объектов. Основные термины и определения. Система физической защиты, определение. Деление СФЗ на подсистемы. Стадии проектирования объектов защиты. Основные этапы стадии концептуального проекта. Концепция физической безопасности объекта. Основные вопросы концепции: предметы защиты, угрозы безопасности и модель вероятных исполнителей угроз, оценка и анализ уязвимости 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

устный опрос , примерные вопросы:

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. Регламентация 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

устный опрос , примерные вопросы:

6.1. Концепция обеспечения ИБ на предприятии. Документ Концепция обеспечения ИБ организации. Категорирование и перечень информационных ресурсов, подлежащих защите. Положение об определении требований по защите (категорировании) ресурсов. Классификация защищаемой информации. Инструкции по организации защиты.

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

устный опрос , примерные вопросы:

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

устный опрос , примерные вопросы:

8.1. Общий алгоритм действий и активная модель реагирования. Последовательность операций (действий). Система предупредительных мер. Нестандартные угрозы. Активная модель реагирования. 8.2. Предупредительная работа с персоналом. Индикаторы выявления. Потенциальные нарушители. Проверки персонала, некоторые способы.

Тема 9. Требования и рекомендации по защите информации

устный опрос , примерные вопросы:

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 режима. Система защиты информации и ее задачи. 12.1. Организационная система защиты информации. Государственная политика и общее руководство деятельностью по защите информации.

Итоговая форма контроля

зачет (в 7 семестре)

Примерные вопросы к итоговой форме контроля

1

7.1. Основная литература:

1. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. - М. : ИД 'ФОРУМ' : ИНФРА-М, 2019. - 592 с. - (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/996789>
2. Криптографические методы защиты информации. Т.1: Уч.-метод. пос./Бабаш А. В., 2-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с.: - (Высшее образование: Бакалавриат) - Режим доступа: <http://znanium.com/catalog/product/960001>

7.2. Дополнительная литература:

1. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. ? М. : ИД 'ФОРУМ' : ИНФРА-М, 2019. - 542 с. - Режим доступа:
<http://znanium.com/catalog/product/999615>
2. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - URL:
<http://znanium.com/catalog/product/1021578>

7.3. Интернет-ресурсы:

- 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/>

8. Материально-техническое обеспечение дисциплины(модуля)

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 оборудование 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен студентам. 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.

стандартная аудитория с доской и мелом

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

Автор(ы):

Ситников С.Ю. _____

"__" _____ 201__ г.

Рецензент(ы):

Шерстюков О.Н. _____

"__" _____ 201__ г.