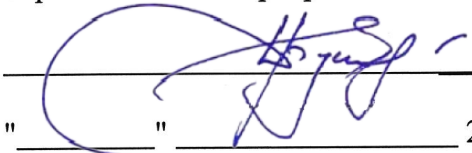


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы


" " 2024 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины

*Б1.О.28 Комплексное обеспечение защиты информации объекта
информатизации*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация

Бакалавр

Форма обучения

очная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов


Южно-Сахалинск

2024

Рабочая программа дисциплины Комплексное обеспечение защиты информации объекта информатизации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

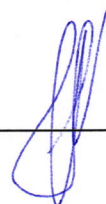
Программу составил(и):

Мазур И.К., доцент кафедры информатики,



Рабочая программа дисциплины Комплексное обеспечение защиты информации объекта информатизации утверждена на заседании кафедры информатики, протокол № 8 от 19.03.2024 г.

Исполняющий обязанности
заведующего кафедрой информатики



Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Изучение основ проектирования комплексной системы информационной безопасности (КСИБ), соотношения программных, аппаратных и организационных средств и методов в комплексной деятельности по защите информации (ЗИ) в автоматизированных системах (АС).

Задачи дисциплины

- освоение способов выделения информации в АС, подлежащей защите;
- изучение критериев защищённости АС, методологии построения современных КСИБ,
- технологий проектирования систем защиты информации;
- формирование комплексного подхода к обеспечению информационной безопасности АС.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации» относится к разделу обязательных дисциплин подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Для освоения данной дисциплины студент должен владеть основными понятиями дисциплин Основы информационной безопасности, Организационное и правовое обеспечение информационной безопасности, Основы управления информационной безопасностью, Методы и средства криптографической защиты информации.

Постреквизиты дисциплины:

Освоение данной дисциплины должно подготовить студентов к профессиональной деятельности в области информационной безопасности, призваны подготовить к прохождению преддипломной практики, написанию выпускной квалификационной работы.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знать основные методы принятия обоснованных экономических решений в профессиональной деятельности УК-9.2 Уметь принимать обоснованные экономические решения в различных областях жизнедеятельности УК-9.3 Иметь навыки принятия обоснованных экономических решений в различных областях жизнедеятельности
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и

	безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа.
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем; ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; ОПК-10.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 - Знает номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных автоматизированных систем; ОПК-12.2 - Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-12.3 - Владеет навыками проектирования элементов защищенных автоматизированных систем и разработки необходимой технической документации в области проектирования защищенных автоматизированных систем с учетом действующих нормативных и методических документов.
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 - Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; ОПК-4.1.2 - Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; ОПК-4.1.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **4** зачетные единицы (**144** академических часа).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	8	
Общая трудоемкость	144	144
Контактная работа:	52	52
Лекции (Лек)	22	22
Лабораторные работы (Лаб)	24	24
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	5	5
Контактная работа в период промежуточной аттестации (КонтПА)	1	1
Промежуточная аттестация – экзамен	35	35
Самостоятельная работа:	57	57
- самостоятельное изучение разделов (раздел 1);	10	10
- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);	10	10
- подготовка к лабораторным занятиям;	24	24
- подготовка к коллоквиумам;	4	4
- подготовка к промежуточной аттестации и т.п.)	9	9

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)					Формы текущего контроля успеваемости, промежуточной аттестации
		семестр	Контактная			Самостоятельная работа	
			Лекции	Практические занятия	Лабораторные занятия		
1.	Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)	8	4		5	11	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Методология формирования задач защиты; интеграция средств защиты в технологическую среду		4		5	10	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Типовая структура комплексной системы информационной безопасности (КСИБ); методы проектирования и оценки качества КСИБ		5		5	10	Устный опрос по теме лекции. Проверка домашнего задания.

4.	Этапы проектирования КСИБ и требования к ним		5		5	9	Устный опрос по теме лекции. Проверка домашнего задания.
5.	Структура политики информационной безопасности организации		4		4	9	Устный опрос по теме лекции. Проверка домашнего задания.
6.	<i>экзамен</i>					8	
	<i>итого</i>		22		24	57	

4.3. Содержание разделов дисциплины

Тема 1. Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)

Состав компонентов комплексной системы обеспечения информационной безопасности. Функциональные и обеспечивающие подсистемы, технология, управление. Законодательная, нормативно- методическая и научная базы разработки КСИБ. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС).

Тема 2. Методология формирования задач защиты; интеграция средств защиты в технологическую среду

Параллельная разработка АС и КСИБ. Системный подход к построению КСИБ. Архитектура защищенных АС. Соотношение программных, аппаратных и административных средств в комплексном обеспечении информационной безопасности АС. Разработка и содержание аварийного плана действий в случае нарушения ИБ АС.

Тема 3. Типовая структура КСИБ; методы проектирования и оценки качества КСИБ

Организация доступа к ресурсам АС. Система разграничения доступа к техническим средствам. Система разграничения доступа к программам и данным. Средства блокировки неправомерных действий субъектов. Задача интеграции средств защиты информации в технологическую среду АС. Требования к составу проектной и эксплуатационной документации. Порядок подготовки и проведения аттестации АС. Сертификация программного обеспечения.

Тема 4. Этапы проектирования КСИБ и требования к ним

Предпроектное обследование: инвентаризация ресурсов. Предпроектное обследование: модели угроз и нарушителя. Предпроектное обследование: анализ рисков. Техническое задание. Техническое и рабочее проектирование. Испытания и внедрение в эксплуатацию, сопровождение. Оценка эффективности. Особенности проектирования на современном уровне и синтез КСИБ. Автоматизация процесса анализа и управления рисками. Моделирование процедуры.

Тема 5. Структура политики информационной безопасности организации (ПИБ)

Методики формирования ПИБ верхнего уровня (цели, концепции, доктрины). Методики формирования ПИБ среднего уровня (стандарты). Способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции). Типовой перечень задач службы информационной безопасности.. Организационно- технические и режимные меры.

4.4. Темы и планы лабораторных занятий

Лабораторное занятие №1 (5 ч.)

Тема Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)

Вопросы для обсуждения:

1. Инвентаризация АС в соответствии с Руководящими документами Гостехкомиссии при Президенте Российской Федерации (рд ГТК РФ)
2. Инфраструктура
3. Технические ресурсы
4. Программные ресурсы
5. Информационные ресурсы.

Лабораторное занятие №2 (5 ч.)

Тема Методология формирования задач защиты; интеграция средств защиты в технологическую среду

Вопросы для обсуждения:

1. Анализ угроз информационным ресурсам и обеспечивающей инфраструктуре на базе учебных лабораторий.
2. Построение моделей угроз и нарушителя.
3. Разработка и содержание аварийного плана действий в случае нарушения информационной безопасности автоматизированной системы

Лабораторное занятие №3 (5 ч.)

Тема Типовая структура КСИБ; методы проектирования и оценки качества КСИБ

Вопросы для обсуждения:

1. Оценка рисков информационной безопасности автоматизированной системы на базе учебных лабораторий.
2. Интеграция средств защиты информации в технологическую среду АС.
3. Требования к составу проектной и эксплуатационной документации.
4. Разработка порядка подготовки и проведения аттестации АС.

Лабораторное занятие №4 (5 ч.)

Тема Этапы проектирования КСИБ и требования к ним

Вопросы для обсуждения:

1. Разработка контрмер.
2. Экономическая оценка затрат на защиту информации (на базе учебных лабораторий).
3. Разработка эскизного проекта КСИБ.
4. Моделирование процедуры.

Лабораторное занятие №5 (4 ч.)

Тема Структура политики информационной безопасности организации (ПИБ)

Вопросы для обсуждения:

1. Выбор концепции, определяющей миссию и ключевые цели политики.
2. Определение стандартов, принципов обеспечения безопасности.
3. Перечень конкретных действий, которые сотрудники должны совершать в процессе взаимодействия с конфиденциальными данными организации.
4. Порядок работы с носителями данных.
5. Правила доступа к корпоративным документам и другим важным ресурсам.
6. Инструкции, касающиеся реализации методов защиты и применения принятых стандартов.
7. Аварийные планы — порядок действий по реагированию и оперативному восстановлению информационных систем в случае непредвиденных обстоятельств.

5. Темы дисциплины (модуля) для самостоятельного изучения

Законодательная, нормативно-методическая и научная базы разработки КСИБ (тема 1. Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС))

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)	Лекции 1-2	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 1-3	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Методология формирования задач защиты; интеграция средств защиты в технологическую среду	Лекции 3-4	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 3-5	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Типовая структура КСИБ; методы проектирования и оценки качества КСИБ	Лекции 5-7	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 6-8	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
4.	Этапы проектирования КСИБ и требования к ним	Лекции 7-9	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 8-10	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
5.	Структура политики информационной безопасности организации (ПИБ)	Лекции 10-11	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 11-12	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Оценочные средства составляются преподавателем самостоятельно при ежегодном обновлении банка средств. Количество вариантов зависит от числа обучающихся.

Задания для текущего контроля

№ раздела	Наименование лабораторных работ
-----------	---------------------------------

дисциплины	
1.	Классификация автоматизированных систем (АС) Требования по защите информации от несанкционированного доступа для АС. Анализ угроз информационным ресурсам и обеспечивающей инфраструктуре.
2.	Построение моделей угроз и нарушителя. Разработка и содержание аварийного плана действий
3.	Оценка рисков информационной безопасности автоматизированной системы на базе учебных лабораторий. Интеграция средств защиты информации в технологическую среду АС. Требования к составу проектной и эксплуатационной документации
4.	Разработка контрмер. Экономическая оценка затрат на защиту информации. Разработка проекта КСИБ. Моделирование процедур.
5.	Методики формирования политики информационной безопасности. Типовой перечень задач службы информационной безопасности. Организационно-технические и режимные меры.

Примерные темы самостоятельной работы

1. Инвентаризация АС в соответствии с Руководящими документами Гостехкомиссии при Президенте Российской Федерации (рд ГТК РФ)
2. Анализ угроз информационным ресурсам и обеспечивающей инфраструктуре на базе учебных лабораторий.
3. Построение моделей угроз и нарушителя.
4. Разработка и содержание аварийного плана действий в случае нарушения информационной безопасности автоматизированной системы
5. Оценка рисков информационной безопасности автоматизированной системы на базе учебных лабораторий.
6. Интеграция средств защиты информации в технологическую среду АС.
7. Требования к составу проектной и эксплуатационной документации.
8. Разработка порядка подготовки и проведения аттестации АС.
9. Экономическая оценка затрат на защиту информации
10. Выбор концепции, определяющей миссию и ключевые цели политики.
11. Определение стандартов, принципов обеспечения безопасности.
12. Определение списка конкретных действий, которые сотрудники должны совершать в процессе взаимодействия с конфиденциальными данными организации.
13. Порядок работы с носителями данных.
14. Правила доступа к корпоративным документам и другим важным ресурсам.
15. Инструкции, касающиеся реализации методов защиты и применения принятых стандартов.
16. Аварийные планы — порядок действий по реагированию и оперативному восстановлению информационных систем в случае непредвиденных обстоятельств

Примерные темы рефератов:

1. Понятие о комплексном обеспечении информационной безопасности
2. Угрозы информационной безопасности и уязвимости информационной системы
3. Изучение методов комплексного исследования объекта информатизации
4. Изучение информации циркулирующей в корпоративной информационной системе
5. Изучение построения системы защиты информации на основе нормативных актов и методических указаний
6. Информационные риски. Оценка рисков информационной безопасности
7. Построение модели угроз информационной системы
8. Виды защиты информации. Организационно-правовые основы технической защиты информации
9. Физическая защита информации
10. Изучение действующей нормативной документации объекта информатизации

11. Составление плана мероприятий по улучшению защищённости объекта информатизации
12. Разработка политики информационной безопасности
13. Исследование методов выбора рационального варианта системы защиты информации на основе экспертной информации
14. Исследование методик расчета показателя качества системы защиты информации
15. Изучение методов построения комплексной системы организационных и технических мер по защите информации
16. Изучение методов построения комплексной защиты сетевой файловой системы
17. Комплексная защита электронной почты и документооборота
18. Понятие о менеджменте информационной безопасности. Серия ГОСТ Р ИСО/МЭК 2700х
19. Изучение методов построения комплексной защиты сетевых приложений и баз данных
20. Изучение методов построения комплексной защиты телекоммуникационной инфраструктуры
21. Изучение методов построения комплексной защиты управления информационной безопасностью
22. Изучение методики составления испытаний системы защиты информации

Примерные вопросы к экзамену.

1. Основные понятия и определения информационной безопасности. Общие цели и задачи защиты информации.
2. Принципы организации комплексной системы защиты информации. Системно-концептуальный подход к защите информации.
3. Основные требования и основные задачи защиты информации в автоматизированных системах.
4. Действующие стандарты в области информационной безопасности. Содержание и основные позиции. Документационное сопровождение комплексной информационной безопасности автоматизированных систем (КИБ АС).
5. Направления работ по созданию КИБ АС. Аспекты планирования инженерно-технического обеспечения КСЗИ.
6. Этапы работ по созданию КИБ АС. Определение и анализ объектов защиты. Базовые понятия и элементы. Формализация описания архитектуры автоматизированной системы.
7. Определение и анализ объектов защиты. Определение исходного уровня защищенности.
8. Классификация защищенности АС в соответствии с РД. Основные требования.
9. Оценка угроз ИБ. Выявление способов НСД и каналов утечки информации.
10. Объективные и субъективные факторы, воздействующие на информацию (по ГОСТ).
11. Виды угроз и основные последствия их реализации.
12. Понятие «нарушителя» и модели нарушителя. Классификации.
13. Модель угроз и принцип ее формирования. Базовая модель угроз безопасности персональных данных (ФСТЭК).
14. Модель угроз и принцип ее формирования. Методология формирования модели угроз в соответствии с рекомендациями ФСБ.
15. Методики оценки рисков. Применяемые на практике подходы.
16. Структура процесса управления рисками.
17. Средства защиты информации и механизмы обеспечения безопасности информации. Идентификация и аутентификация.
18. Средства защиты информации и механизмы обеспечения безопасности информации. Разграничение доступа. Регистрация и аудит.
19. Средства защиты информации и механизмы обеспечения безопасности информации. Криптографическая подсистема.
20. Средства защиты информации и механизмы обеспечения безопасности информации. Межсетевое экранирование.
21. Планирование мероприятий КСЗИ.
22. Контроль мероприятий КИБ АС. Основные аспекты.
23. Оценка эффективности КИБ АС. Общая характеристика применяемых методов.
24. Оценка эффективности КИБ АС. Оценочные подходы.

8. Система оценивания планируемых результатов обучения

Критерии оценивания:

Критерием оценивания является выполнение самостоятельных заданий, контрольных и лабораторных работ.

Самостоятельные задания, контрольные и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

- своевременное выполнение работы;
- полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий, студент имеет возможность сдавать теоретический экзамен по вопросам.

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.

Оценка «удовлетворительно» выставляется студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

оценка **«неудовлетворительно»** выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (зачет)			20	43
Итого за семестр			60	100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература:

1. Мирошников, А. И. Комплексное обеспечение защиты информации объекта информатизации и защита информации : учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128718.html>
2. Комплексное обеспечение защиты информации объекта информатизации : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/72444.html>.
3. Галатенко, В. А. Комплексное обеспечение защиты информации объекта информатизации : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет

Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97562.html>

9.2. дополнительная литература:

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: <http://www.iprbookshop.ru/63800.html>
2. Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 с. — 978-5-94774-708-9. — Режим доступа: <http://www.iprbookshop.ru/62827.html>
3. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В. — Электрон.текстовые данные. — Самара: Самарский государственный архитектурно- строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183>.
4. Сагдеев К.М. Физические основы защиты информации [Электронный ресурс] : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига. — Электрон. текстовые данные. — Ставрополь: Северо- Кавказский федеральный университет, 2015. — 394 с. —2227-8397. — Режим доступа: <http://www.iprbookshop.ru/63152.html>

9.3. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
13. Visual Studio Professional
14. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление).
15. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
16. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

9.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные

технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)

5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Polpred.com Обзор СМИ (<http://polpred.com/>)
14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).