МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

УТВЕРЖДАЮ
Директор Политехнического института
_____ Артамонов Д.В.
«_3_» ___10_____ 2014 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

А1.В.ДВ2.2 «ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Направление подготовки

10.06.01 Информационная безопасность

Направленность (профиль):

Методы и системы защиты информации, информационная безопасность

Квалификация (степень) – Исследователь. Преподаватель-исследователь.

Форма обучения: очная, заочная

Пенза, 2014

Рабочая программа составлена в соответствии с ФГОС ВО по направлению 10.06.01 Информационная безопасность подготовки научно-педагогических кадров в аспирантуре (уровень подготовки кадров высшей квалификации).

Программу составили:

1. Зефиров С.Л., к.т.н., зав.кафедрой _____

2. Лупанов М.Ю., к.т.н., доцент _____

Программа обсуждена на заседании кафедры «Информационная безопасность систем и технологий»

Протокол № 1 от « 16 » 09 2014 года

Зав. кафедрой ИБСТ _____ С.Л. Зефиров

(подпись, Ф.И.О.)

Программа согласована с деканом факультета приборостроения, информационных технологий и электроники

Декан факультета ПИТЭ _____ В.Д. Кревчик

(подпись, Ф.И.О., дата)

Программа одобрена методической комиссией факультета ПИТЭ

Протокол № 1 от « 1 » 10 2014 года

Председатель методической комиссии

факультета ПИТЭ _____ А.В. Задера

(подпись, Ф.И.О.)

1. Цели и задачи изучения дисциплины

Цель изучения дисциплины – формирование у аспирантов углубленных профессиональных знаний о методах и моделях информационной безопасности автоматизированных систем.

Задачи дисциплины:

– изучить основные модели информационной безопасности автоматизированных систем;

– изучить основные методы оценки информационной безопасности автоматизированных систем;

– подготовить аспирантов к применению полученных знаний для моделирования автоматизированных систем и их анализа и исследования.

2. Место дисциплины в структуре ОПОП аспирантуры

Дисциплина «Проблемы обеспечения информационной безопасности автоматизированных систем» относится к дисциплинам по выбору вариативной части учебного плана по направлению подготовки 10.06.01 – Информационная безопасность, направленность (профиль) «Методы и системы защиты информации, информационная безопасность».

Дисциплина предполагает наличие у аспирантов знаний по основам информационной безопасности, теории риска, теории принятия решений и управлению информационной безопасностью.

Знания и навыки, полученные аспирантами при изучении данной дисциплины, могут быть применены при изучении дисциплин «Методы и средства защиты информации в условиях информационного противоборства», «Методы и системы защиты информации, информационная безопасность», «Проблемы и методы защиты информации в телекоммуникационных системах специального назначения», а также в процессе научно-исследовательской деятельности и подготовки НКР (диссертации).

3. Компетенции аспиранта, формируемые в результате освоения программы дисциплины

Изучение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОПК-1	способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	*Знать:* современные методы решения научных задач в области обеспечения информационной безопасности автоматизированных систем
		Уметь: применять современные методы решения научных задач в области обеспечения информационной безопасности автоматизированных систем
		Владеть: навыками внедрения полученных научных результатов в практическую деятельность.

ОПК-3	способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	*Знать:* методы оценки степени соответствия защищаемых объектов автоматизированных систем действующим стандартам в области информационной безопасности.
		Уметь: использовать методы оценки степени соответствия защищаемых объектов автоматизированных систем действующим стандартам в области информационной безопасности.
		Владеть: современными методиками оценки степени соответствия защищаемых объектов автоматизированных систем действующим стандартам в области информационной безопасности..
ПК-4	способность разрабатывать методы и модели информационной безопасности, проводить анализ защищенности и оценивать информационную безопасность объектов	*Знать:* - действующие нормативные документы в области оценки информационной безопасностью
		Уметь: - разрабатывать и выбирать модели и методы измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
		Владеть: навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
ПК-5	способность анализировать риски информационной безопасности, разрабатывать и применять современные методы и модели обеспечения информационной безопасности, оценки информационной безопасности автоматизированных систем	*Знать:* методы анализа и оценки рисков информационной безопасности автоматизированных систем
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от целей систем и их особенностей; - определить метод оценки информационной безопасности автоматизированных систем в зависимости от целей оценки и особенностей систем.
		Владеть: методиками оценки информационной безопасности автоматизированных систем
ПК-7	способность создавать и исследовать модели систем защиты информации различного назначения, проводить анализ и обосновывать выбор решений по их применению	*Знать* модели управления информационной безопасностью систем различного назначения
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от назначения
		Владеть: методиками анализа и оценки информационной безопасности автоматизированных систем

4. Структура и содержание дисциплины

4.1. Структура дисциплины

4.1.1. Структура дисциплины для очной формы

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость *(в часах)*						Формы текущего контроля успеваемости *(по неделям семестра)*	
				Аудиторная работа			Самостоятельная работа				
				Всего	Лекция	Практические занятия	Всего	Подготовка к аудиторным занятиям	Подготовка к экзамену	Собеседование	
1	Тема 1. Моделирование автоматизированных систем	1	1-3	6	2	4	6	6		3	
2	Тема 2. Теоретические основы информационного управления	1	4-6	6	4	2	6	6		6	
3	Тема 3. Анализ и синтез систем обеспечения и систем управления информационной безопасностью автоматизированных систем	1	7-9	6	2	4	6	6		9	
4	Тема 4. Основы теории конфликта	1	10-12	6	4	2	6	6		12	
5	Тема 5. Моделирование автоматизированных систем в условиях риска	1	13-15	6	2	4	6	6		15	
7	Тема 6. Проблема измерения и оценивания информационной безопасности автоматизированных систем	1	16-18	6	4	2	6	6		18	
	Подготовка к экзамену						36		36		
	Общая трудоемкость, в часах			36	18	18	72	36	36	Промежуточная аттестация	
										Форма	Семестр
										Экзамен	1

4.1.2. Структура дисциплины для заочной формы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость *(в часах)*					Формы текущего контроля успеваемости *(по неделям семестра)*	
				Аудиторная работа		Самостоятельная работа				
				Всего	Лекция	Всего	Подготовка к аудиторным занятиям	Подготовка к экзамену	Собеседование	
1	Тема 1. Моделирование автоматизированных систем	1	1-3	1	1	10	10		3	
2	Тема 2. Теоретические основы информационного управления	1	4-6	2	2	9	9		6	
3	Тема 3. Анализ и синтез систем обеспечения и систем управления информационной безопасностью автоматизированных систем	1	7-9	1	1	12	12		9	
4	Тема 4. Основы теории конфликта	1	10-12	2	2	11	11		12	
5	Тема 5. Моделирование автоматизированных систем в условиях риска	1	13-15	1	1	11	11		15	
6	Тема 6. Проблема измерения и оценивания информационной безопасности автоматизированных систем	1	16-18	2	2	10	10		18	
	Подготовка к экзамену					36		36		
	Общая трудоемкость, в часах			9	9	99	63	36	Промежуточная аттестация	
									Форма	Семестр
									Экзамен	1

4.2. Содержание дисциплины

Тема 1. Моделирование автоматизированных систем

Методы управления и их характеристики. Информационное управление, характеристики и методы. Объекты информационного управления и их характеристики.

Процессная модель автоматизированной системы. Вероятностные модели автоматизированной системы. Модели автоматизированной системы на основе цепей Маркова. Модель автоматизированной системы с использованием сетей Петри.

Тема 2. Теоретические основы информационного управления

Основные проблемы и задачи теоретического исследования информационного управления.

Основные положения информационно-логического подхода. Основные положения системно-логического подхода. Основные положения структурного подхода. Стратегии информационного управления с использованием сценарного подхода. Моделирование и формирование сценариев информационного управления.

Тема 3. Анализ и синтез систем обеспечения и систем управления информационной безопасностью автоматизированных систем

Уязвимости, угрозы, риски, рисковые события, негативные последствия, ущербы. Риск-ориентированный подход к обеспечению информационной безопасности. Идентификация событий информационной безопасности. Предварительный анализ событий информационной безопасности. Накопление знаний о событиях информационной безопасности. Общая модель обеспечения информационной безопасности автоматизированной системы. Механизмы и методы защиты. Модели и методы синтеза систем обеспечения информационной безопасности. Модели и методы синтеза систем управления информационной безопасностью.

Тема 4. Основы теории конфликта

Системное исследование конфликта. Функциональные пространства и переменные. Классификация конфликтов. Абстрактный конфликт. Реальный конфликт. Причины конфликта. Неопределённость и самоорганизация. Решение конфликта.

Тема 5. Моделирование автоматизированных систем в условиях риска

Модель управления риском. Основные методы моделирования автоматизированных систем в условиях риска. Модели на основе марковских случайных процессов. Модели на основе теории игр. Модели на основе сетей Петри. Графовая форма представления информационных моделей. Методы имитационного моделирования автоматизированных систем в условиях риска.

Тема 6. Проблема измерения и оценивания информационной безопасности автоматизированных систем

Методы оценки автоматизированных систем. Принципы функциональной декомпозиции автоматизированных систем. Модель оценки информационной безопасности на основе оценки процессов. Оценка информационной безопасности на основе модели зрелости процессов. Риск-ориентированная оценка информационной безопасности.

Процесс функциональной декомпозиции автоматизированных систем. Использование функциональной декомпозиции для проведения оценки информационной безопасности автоматизированных систем.

5. Образовательные технологии

В ходе освоения дисциплины «Проблемы обеспечения информационной безопасности автоматизированных систем управления» при проведении аудиторных занятий используются следующие образовательные технологии:

1. Технология развития критического мышления реализуется в ходе проведения следующих видов учебной работы:

1.1. *Проблемные лекции*, которые предполагают диалоговый тип лекционного преподавания, предметом которого выступает вводимый лектором материал и система познавательных задач, отражающих основное содержание темы. В виде проблемных лекций реализуется темы 3, 6

1.2. *Семинары-круглые столы*, в ходе которых происходит групповое обсуждение аспирантами учебной проблемы под руководством преподавателя. В ходе проведения круглого стола аспиранты приобретают навыки устного изложения заранее подготовленного материала, умение выслушивать коллег-сокурсников, делать заключения. В виде семинаров-круглых столов реализуются темы 1, 4.

1.3. *Семинары-дискуссии*, в ходе которых обсуждается проблемная ситуация, поставленная преподавателем, а аспиранты защищают различные точки зрения на поставленную проблему. В ходе проведения дискуссии аспиранты приобретают умение излагать и аргументировано отстаивать точку зрения, обоснованно критиковать оппонентов, сопоставлять различные подходы к решению проблемной ситуации, делать выводы. В виде семинаров-дискуссий реализуются темы 2, 5

2. Медиатехнология реализуется в ходе проведения следующих видов учебной работы:

2.1. *Проблемные лекции*, в ходе которых используются презентации, выполненные в в открытом программном продукте Libreoffice Impress, и содержащие иллюстрации приводимых положений, видео-фрагменты, элементы работы математических моделей – симуляций экологических закономерностей. В виде проблемных лекций с использованием медиатехнологий реализуется темы 3, 6.

2.2. *Семинары-круглые столы*, в ходе которых аспиранты делают краткие сообщения по рассматриваемой проблематике с использованием презентации. В результате использования этой технологии аспиранты учатся лаконично и ярко представлять информацию в аудитории. В виде семинаров-круглых столов с использованием медиатехнологий реализуются темы 1, 4.

3. Кейс-технология реализуется в ходе проведения следующих видов учебной работы:

3.1. *Семинары-дискуссии*, в ходе которых в качестве одной из технологий используются такие приемы как мозговой штурм и дебаты. Мозговой штурм позволяет, используя групповую форму работы смоделировать процесс получения абсолютно новых для аспирантов знаний. Дебаты позволяют сопоставлять существующие в экологии сообществ и экосистем противоположные подходы для решения одной и той же проблемы. В виде семинаров-дискуссий с использованием кейс-технологий реализуются темы 2, 5.

При организации самостоятельной работы используются следующие технологии:

1. Технология систематизации имеющейся информации (работа с конспектом лекции для подготовки к экзамену; темы 1-6)

2. Технология поиска и сбора новой информации (работа на компьютере с целью поиска информации в базах данных, работа с учебной, справочной и научной литературой с целью подготовки к семинарам: темы 1–6);

3. Технология анализа и представления новой информации (работа по подготовке устных сообщений на семинарах-круглых столах (темы 1, 4), по подготовке для выступлений презентациями на семинарах-дискуссиях (темы 2, 5), по подготовке к экзамену).

В целях реализации индивидуального подхода к обучению аспирантов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы с аспирантами, в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

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

6.1. План самостоятельной работы аспирантов

6.1.1 План самостоятельной работы аспирантов очной формы обучения

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-3	Тема 1. Моделирование автоматизированных систем	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	6
4-6	Тема 2. Теоретические основы информационного управления	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка выступления и презентации для семинара-дискуссии	См. раздел 7 РПД	6
7-9	Тема 3. Анализ и синтез систем обеспечения и систем управления информационной безопасностью автоматизированных систем	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	6
10-12	Тема 4. Основы теории конфликт	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	6
13-15	Тема 5. Моделирование автоматизированных систем управления в условиях риска	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка выступления и презентации для семинара-дискуссии	См. раздел 7 РПД	6
16-18	Тема 6. Проблема измерения и оценивания информационной безопасности автоматизированных систем	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	6

6.1.2 План самостоятельной работы аспирантов заочной формы обучения

№ сем.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1. Моделирование автоматизированных систем	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	10
	Тема 2. Теоретические основы информационного управления	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка выступления и презентации для семинара-дискуссии	См. раздел 7 РПД	9
	Тема 3. Анализ и синтез систем обеспечения и систем управления информационной безопасностью автоматизированных систем	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	12
	Тема 4. Основы теории конфликт	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	11
	Тема 5. Моделирование автоматизированных систем управления в условиях риска	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка выступления и презентации для семинара-дискуссии	См. раздел 7 РПД	11
	Тема 6. Проблема измерения и оценивания информационной безопасности автоматизированных систем	Подготовка к аудиторным занятиям	Проработка лекционных вопросов Подготовка устных сообщений	См. раздел 7 РПД	10

6.2. Методические указания по организации самостоятельной работы аспирантов

Самостоятельная работа предполагает:

- подготовку к лекциям;
- подготовку к собеседованиям на практических занятиях.

Подготовка к лекциям предполагает проработку конспектов предшествующих лекций, работу с нормативными документами, основной и дополнительной литературой. Подготовка к собеседованию предполагает повторение пройденного материала, приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины, подготовку сообщений к семинарам, круглым

столам, дискуссиям.

6.3. Материалы для проведения текущего и промежуточного контроля знаний

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий Собеседование	Тема 1-6	ОПК-1, 3; ПК-4, 5, 7
2	Промежуточный Экзамен	Тема 1-6	ОПК-1, 3; ПК-4, 5, 7

Вопросы для собеседования

Тема 1. Моделирование автоматизированных систем

1. Методы управления и их характеристики.
2. Информационное управление, характеристики и методы. Объекты информационного управления и их характеристики.
3. Процессная модель автоматизированной системы.
4. Вероятностные модели автоматизированной системы.
5. Модели автоматизированной системы на основе цепей Маркова.
6. Модель автоматизированной системы с использованием сетей Петри.

Тема 2. Теоретические основы информационного управления

1.Основные проблемы и задачи теоретического исследования информационного управления.

2.Основные положения информационно-логического подхода.

3.Основные положения системно-логического подхода.

4.Основные положения структурного подхода.

5.Стратегии информационного управления с использованием сценарного подхода.

6.Моделирование и формирование сценариев информационного управления.

Тема 3. Анализ и синтез систем обеспечения и систем управления информационной безопасностью автоматизированных систем

1.Уязвимости, угрозы, риски, рисковые события, негативные последствия, ущербы.

2.Риск-ориентированный подход к обеспечению информационной безопасности.

3.Идентификация событий информационной безопасности.

4.Предварительный анализ событий информационной безопасности.

5.Накопление знаний о событиях информационной безопасности.

6.Общая модель обеспечения информационной безопасности автоматизированной системы. Механизмы и методы защиты.

7.Модели и методы синтеза систем обеспечения информационной безопасности. Модели и методы синтеза систем управления информационной безопасностью.

Тема 4. Основы теории конфликта

1.Системное исследование конфликта.

2.Функциональные пространства и переменные.

3.Классификация конфликтов.

4.Абстрактный конфликт.

5.Реальный конфликт.

6.Причины конфликта.

7.Неопределённость и самоорганизация.

8.Решение конфликта.

Тема 5. Моделирование автоматизированных систем в условиях риска

1.Модель управления риском.

2.Основные методы моделирования автоматизированных систем в условиях риска. Модели на основе марковских случайных процессов.

3.Модели на основе теории игр.

4.Модели на основе сетей Петри.

5.Графовая форма представления информационных моделей.

6.Методы имитационного моделирования автоматизированных систем в условиях риска.

Тема 6. Проблема измерения и оценивания информационной безопасности автоматизированных систем

1.Методы оценки автоматизированных систем.

2.Принципы функциональной декомпозиции автоматизированных систем.

3.Модель оценки информационной безопасности на основе оценки процессов.

4.Оценка информационной безопасности на основе модели зрелости процессов.

5.Риск-ориентированная оценка информационной безопасности.

6.Процесс функциональной декомпозиции автоматизированных систем.

7.Использование функциональной декомпозиции для проведения оценки информационной безопасности автоматизированных систем.

Примерный перечень вопросов и заданий к экзамену

1. Методы управления и их характеристики.
2. Информационное управление, характеристики и методы.
3. Объекты информационного управления и их характеристики.
4. Процессная модель автоматизированной системы.
5. Вероятностные модели автоматизированной системы.
6. Модели автоматизированной системы на основе цепей Маркова.
7. Модель автоматизированной системы с использованием сетей Петри.
8. Основные проблемы и задачи теоретического исследования информационного управления.
9. Основные положения информационно-логического подхода.
10. Основные положения системно-логического подхода.
11. Основные положения структурного подхода.
12. Стратегии информационного управления с использованием сценарного подхода.
13. Моделирование и формирование сценариев информационного управления.
14. Уязвимости, угрозы, риски, рисковые события, негативные последствия, ущербы.
15. Риск-ориентированный подход к обеспечению информационной безопасности.
16. Идентификация событий информационной безопасности.
17. Предварительный анализ событий информационной безопасности.
18. Накопление знаний о событиях информационной безопасности.
19. Общая модель обеспечения информационной безопасности автоматизированной системы.
20. Механизмы и методы защиты.
21. Модели и методы синтеза систем обеспечения информационной безопасности. Модели и методы синтеза систем управления информационной безопасностью.
22. Системное исследование конфликта.
23. Функциональные пространства и переменные. Классификация конфликтов.

24. Абстрактный конфликт. Реальный конфликт.
25. Причины конфликта.
26. Неопределённость и самоорганизация. Решение конфликта.
27. Модель управления риском.
28. Основные методы моделирования автоматизированных систем в условиях риска.
29. Модели на основе марковских случайных процессов.
30. Модели на основе теории игр.
31. Модели на основе сетей Петри.
32. Графовая форма представления информационных моделей.
33. Методы имитационного моделирования автоматизированных систем в условиях риска.
34. Методы оценки информационной безопасности автоматизированных систем.
35. Принципы функциональной декомпозиции автоматизированных систем.
36. Модель оценки информационной безопасности на основе оценки процессов.
37. Оценка информационной безопасности на основе модели зрелости процессов.
38. Риск-ориентированная оценка информационной безопасности.
39. Процесс функциональной декомпозиции автоматизированных систем.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) основная литература

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2
http://znanium.com/bookread2.php?book=405000
2. Обеспечение информационной безопасности бизнеса/В.В.Андрианов, С.Л.Зефиров, В.Б.Голованов, Н.А.Голдуев. – М.: Альпина Паблишерс, 2011. – 373с.
http://znanium.com/bookread2.php?book=556539

б) дополнительная литература

1. Шапкин А.С., Шапкин В.А. Теория риска и моделирование рисковых ситуаций: Учебник. - М.: Издательско-торговая корпорация «Дашков и К», 2009. – 880с.
http://znanium.com/bookread2.php?book=450763
2. Уродовских В.Н. Управление рисками предприятия: Учеб.пособие. – М.: Вузовский учебник: ИНФРА-М, 2011.-168с.
http://znanium.com/bookread2.php?book=201227

в) программное обеспечение и Интернет-ресурсы

1. Офисный пакет LibreOffice https://ru.libreoffice.org/
2. http://www.security-science.com/
3. www.elibrary.ru,
4. www.springerlink.com
5. http://www.scirp.org/journal/jis/
6. https://sites.google.com/site/ijcsis/

8. Материально-техническое обеспечение дисциплины (модуля)

Учебная аудитория для проведения лекционных, практических занятий, текущей и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный.

Программное обеспечение ноутбука лекционных аудиторий:

- лицензионное программное обеспечение:

- «Microsoft Windows» (подписка DreamSpark/Microsoft Imagine Standart); регистрационный номер 00037FFEBACF8FD7, договор № СД-130712001 от

12.07.2013, продлен до 2020г.;
- свободно распространяемое программное обеспечение:
    - офисный пакет LibreOffice
    - файловый менеджер FreeCommander
    - программа просмотра pdf-документов Sumatra PDF Reader.

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных
2015-2016	пр-л №1 от 30.9.15	Без изменений			
2016-2017	пр-л №1 от 8.09.16	Без изменений			
2017-2018	пр-л №1 от 31.08.17	Обновлен раздел 7	12, 13		