Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский университет Государственной противопожарной службы МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Научная специальность
2.3.6 Методы и системы защиты информации, информационная безопасность

Подготовка научных и научно-педагогических кадров в адъюнктуре (аспирантуре)

Санкт-Петербург

1. Цель и задачи дисциплины «Методы и системы защиты информации, информационная безопасность»

Цель изучения дисциплины: формирование системы теоретических знаний и умений, необходимых для успешной профессиональной деятельности в сфере науки, техники и технологии, охватывающие совокупность проблем, связанных с разработкой, совершенствованием и применением методов и средств защиты информации, а также обеспечением информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз.

Перечень компетенций, формируемых в процессе изучения дисциплины «Методы и системы защиты информации, информационная безопасность»

Таблица 1

Компетенции	Содержание
ОПК-7	способность формулировать научные задачи, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность
ОПК-11	способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности
ПК-6	способность исследовать научные основы теории и методологии обеспечения информационной безопасности и защиты информации
ПК-7	способность исследовать методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида
ПК-8	способность исследовать методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса
ПК-9	способность исследовать способы повышения противодействия угрозам нарушения информационной безопасности для любого вида информационных систем
ПК-10	способность проводить анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.

Задачами изучения дисциплины является:

– формирование системы научного знания предметной области в составе:

1) методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях;

2) специфика и механизм научно-исследовательской деятельности, ее методологический инструментарий;

3) основные положения образовательных программ высшего образования, основные задачи в области обеспечения информационной безопасности;

4) основные тенденции развития в соответствующей области науки;

5) основные этапы организации работы коллектива в области профессиональной деятельности;

6) основные положения образовательных программ высшего образования для ведения преподавательской деятельности;

7) фундаментальные основы системного анализа, оптимизации, управления, принятия решений и обработки информации применительно к сложным системам;

8) основные принципы построения защищенных распределенных компьютерных систем;

9) основные подходы к разработке защищенного программного обеспечения;

10) существующие подходы и методы построения моделей нарушителей информационной безопасности;

11) основные принципы отладки программ, архитектуры и интерфейсы прикладного программирования операционных систем;

– приобретение умения:

1) анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши / проигрыши реализации этих вариантов;

2) использовать методологическую культуру в научных исследованиях профессиональных проблем;

3) разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;

4) использовать современную вычислительную технику и специализированное программное обеспечение в научно-исследовательской работе;

5) самостоятельно определять порядок выполнения работ;

6) использовать положения основных образовательных программ в ходе осуществления преподавательской деятельности;

7) разрабатывать методы и алгоритмы решения задач оптимизации, управления, принятия решений и обработки информации;

8) разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении;

9) применять инструментальные средства отладки и дизассемблирования программного кода;

10) проектировать архитектуру защищенных систем, выявлять атаки,

описывать природу атаки, ее признаки и методы обнаружения;

11) разрабатывать быстрые вычислительные алгоритмы для криптографических приложений;

– овладение:

1) навыками анализа методологических проблем, возникающих при решении исследовательских и практических задач, в том числе в междисциплинарных областях;

2) способностью самостоятельной научно-исследовательской деятельности с использованием ранее полученных знаний в конкретной области;

3) навыками разработки частных методик исследования научно-исследовательских задач в области обеспечения информационной безопасности;

4) навыками использования программных средств и работы в компьютерных сетях, использования ресурсов Интернет;

5) основными методами, способами и средствами получения, хранения, переработки информации, навыками синхронного восприятия и документирования мультимедийной информации на иностранных языках;

6) способностью самостоятельной организации работы коллектива исполнителей;

7) навыками преподавательской деятельности по основным образовательным программам высшего образования;

8) навыками системного подхода к решению прикладных задач для повышения эффективности функционирования объектов исследования и разработки;

9) навыками и средствами проектирования систем обеспечения информационной безопасности, объектов информатизации на базе компьютерных систем в защищенном исполнении;

10) основными методами верификации программ, способами настройки систем обнаружения компьютерных атак;

11) способами создания сигнатур обнаруженных атак, навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем;

12) навыками использования систем компьютерной математики для решения профессиональных задач.

2. Перечень планируемых результатов обучения дисциплины «Методы и системы защиты информации, информационная безопасность», соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты обучения дисциплины «Методы и системы защиты информации, информационная безопасность»	**Планируемые результаты освоения образовательной программы**
В результате освоения дисциплины **«Методы и системы защиты информации, информационная безопасность»** обучающийся должен **демонстрировать способность и готовность решать следующие профессиональные задачи**	В результате освоения образовательной программы обучающийся должен **владеть** компетенциями
в области научно-исследовательской деятельности:	
оценивание степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности; исследование научных основ теории и методологии обеспечения информационной безопасности и защиты информации; исследование методов, аппаратно-программных и организационных средств защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида; исследование методов, моделей и средств выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса; исследование способов повышения противодействия угрозам нарушения информационной безопасности для любого вида информационных систем; анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	ОПК-7, ОПК-11, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10
в области преподавательской деятельности	
систематизация, классификация, интерпретация и визуализация: методов, аппаратно-программных и организационных средств защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида; методов, моделей и средств выявления и идентификации угроз нарушения информационной безопасности объектов различного вида и класса; способов повышения противодействия угрозам нарушения информационной безопасности для любого вида информационных систем; рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	ОПК-7, ОПК-11, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10

3. Место дисциплины «Методы и системы защиты информации, информационная безопасность»

Дисциплина относится к образовательному компоненту по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» по программе подготовки научных и научно-педагогических кадров в аспирантуре (адъюнктуре).

4.Структура и содержание дисциплины «Методы и системы защиты информации, информационная безопасность»

Дисциплина изучается на 3 курсе по очной (5 семестр) и на 2-3 курсе по заочной форме обучения.

Общая трудоемкость дисциплины по очной и заочной формам обучения составляет 6 ЗЕ (216 часов).

4.1. Объем дисциплины «Методы и системы защиты информации, информационная безопасность» и виды учебной работы

для очной формы обучения 3 года

Вид учебной работы	Всего часов	3 курс 5 семестр
Общая трудоемкость дисциплины в часах	216	216
Контактные часы (всего)	76	76
В том числе:		
Лекции	32	32
Практические занятия	34	34
Семинарские занятия	10	10
Самостоятельная работа (всего)	104	104
Экзамен	36	36

Для заочной формы обучения 4 года

Вид учебной работы	Всего часов	2 курс	3 курс
Общая трудоемкость дисциплины в часах	216	108	108
Контактные часы (всего)	26	10	16
В том числе:			
Лекции	12	6	6
Практические занятия	12	4	8
Семинарские занятия	2		2
Самостоятельная работа (всего)	181	98	83
Экзамен	9		9

4.2. Разделы дисциплины «Методы и системы защиты информации, информационная безопасность»

очная форма обучения

№ п/п	Наименование разделов, тем	Всего часов	Количество часов по видам занятий				
			Лекции	Семинары	Практические занятия	Экзамен	Самостоятельная работа
1	2	3	4	5	6	7	8
5 семестр							
Раздел 1. Теория, методология и актуальные вопросы обеспечения информационной безопасности и защиты информации							
1	Актуальные вопросы обеспечения информационной безопасности и защиты информации	16	2	2			12
2	Теория и методология обеспечения информационной безопасности и защиты информации	18	2		4		12
Раздел 2. Анализ элементов системы обеспечения информационной безопасности							
3	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса	10	2		2		6
4	Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности	10	2	4			4
5	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения	10	2		2		6
Раздел 3. Методы и средства защиты информации и обеспечения информационной безопасности							
6	Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида	12	2		4		6

№ п/п	Наименование разделов, тем	Всего часов	Количество часов по видам занятий				
			Лекции	Семинары	Практические занятия	Экзамен	Самостоятельная работа
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
7	Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности	6	2				4
Раздел 4. Идентификация, аутентификация и авторизация							
8	Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа	14	2		4		8
Раздел 5. Противодействие угрозам нарушения информационной безопасности							
9	Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем	12	2		4		6
10	Модели и методы формирования комплексов средств противодействия угрозам безопасности информации и нарушения информационной безопасности для различного вида объектов защиты	8	2				6
11	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет	12	2		4		6
Раздел 6. Оценка информационной безопасности							
12	Модели и методы оценки защищенности информации и информационной безопасности объекта	10	2		4		4
13	Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты	8	2		2		4
Раздел 7. Менеджмент информационной безопасности							

№ п/п	Наименование разделов, тем	Всего часов	Количество часов по видам занятий				
			Лекции	Семинары	Практические занятия	Экзамен	Самостоятельная работа
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
14	Модели и методы управления информационной безопасностью	10	2				8
15	Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления	12	2		4		6
Раздел 8. Системы документооборота и средства зашиты циркулирующей в них информации							
16	Системы документооборота и средства зашиты циркулирующей в них информации	12	2	4			6
Экзамен		36				36	
Всего		**216**	**32**	**10**	**34**	**36**	**104**

заочная форма обучения

№ п/п	Наименование разделов, тем	Всего часов	Количество часов по видам занятий				
			Лекции	Семинары	Практические занятия	Экзамен	Самостоятельная работа
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
2 курс							
Раздел 1. Теория, методология и актуальные вопросы обеспечения информационной безопасности и защиты информации							
1	Актуальные вопросы обеспечения информационной безопасности и защиты информации	14	2				12
2	Теория и методология обеспечения информационной безопасности и защиты информации	12					12
Раздел 2. Анализ элементов системы обеспечения информационной безопасности							

№ п/п	Наименование разделов, тем	Всего часов	Количество часов по видам занятий				
			Лекции	Семинары	Практические занятия	Экзамен	Самостоятельная работа
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
3	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса	14	2				12
4	Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности	12					12
5	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения	16			2		14
Раздел 3. Методы и средства защиты информации и обеспечения информационной безопасности							
6	Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида	14	2				12
7	Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности	12					12
Раздел 4. Идентификация, аутентификация и авторизация							
8	Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа	14			2		12
	Итого за 2 курс	**108**	**6**		**4**		**98**

3 курс							
Раздел 5. Противодействие угрозам нарушения информационной безопасности							
9	Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем	12	2				10
10	Модели и методы формирования комплексов средств противодействия угрозам безопасности информации и нарушения информационной безопасности для различного вида объектов защиты	10					10
11	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет	12			2		10
Раздел 6. Оценка информационной безопасности							
12	Модели и методы оценки защищенности информации и информационной безопасности объекта	14	2		2		10
13	Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты	12			2		10
Раздел 7. Менеджмент информационной безопасности							
14	Модели и методы управления информационной безопасностью	12	2				10
15	Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления	15			2		13
Раздел 8. Системы документооборота и средства зашиты циркулирующей в них информации							
16	Системы документооборота и средства зашиты циркулирующей в них информации	12		2			10
Экзамен		9				9	
Итого за 3 курс		**108**	**6**	**2**	**8**	**9**	**83**
Всего		**216**	**12**	**2**	**12**	**9**	**181**

4.3. Содержание учебной дисциплины

РАЗДЕЛ 1. ТЕОРИЯ, МЕТОДОЛОГИЯ И АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Тема 1. Актуальные вопросы обеспечения информационной безопасности и защиты информации

Источники актуальных вопросов информационной безопасности и защиты информации: научные форумы и диссертационные исследования по специальности 2.3.6 и смежным отраслям знания. Эволюция проблематики в сфере информационной безопасности и защиты информации: основные тенденции и закономерности.

Семинарское занятие. Установление трендов информационной безопасности и защиты информации. Выбор темы реферата.

Самостоятельная работа. Реферирование материалов ИНФОФОРУМА и ИБРР (РИ).

Рекомендуемая литература:

основная: [1 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [1, 5]

Тема 2. Теория и методология обеспечения информационной безопасности и защиты информации

Основные термины и определения в сфере информационной безопасности и защиты информации. «Ландшафт» информационной безопасности: взаимодействие базовых элементов теории. Принципы обеспечения информационной безопасности. Абстрактная модель системы защиты информации: основные понятия. Основы формальной теории защиты информации: монитор безопасности, модель разграничения доступа. Классификация и взаимосвязь моделей безопасности.

Практическое занятие. Решение задач по моделям: HRU, TAM, TAKE-GRANT, Белла-Лападулы.

Самостоятельная работа. Модели дискреционного доступа. Модели мандатного доступа. Ролевые модели доступа. Модели безопасности информационных потоков.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [1 –3, 5, 9]

РАЗДЕЛ 2. АНАЛИЗ ЭЛЕМЕНТОВ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса

Классификационные признаки и известные классификации угроз нарушения информационной безопасности. Методы идентификации угроз нарушения информационной безопасности. Базовая модель угроз. Средства выявления угроз нарушения информационной безопасности.

Практическое занятие. Написание частных моделей угроз информационной безопасности.

Самостоятельная работа. Типовые модели нарушителей информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [3, 10, 24]

Тема 4. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности

Назначение, цели и задачи аудита информационной безопасности компании. Принципы и формы проведения аудита информационной безопасности. Целевые системы нормативов для проведения аудита. Методология мониторинга безопасности информационных систем на основе модели адаптивной защиты.

Семинарское занятие. Основные стадии аудита: планирование, моделирование, тестирование, анализ, разработка предложений, документирование. Методы аудита: экспертно-аналитические, экспертно-инструментальные, моделирование действий злоумышленника.

Самостоятельная работа. Инструментальные средства проведения активного аудита информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [22]

Тема 5. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения

Категорирование и оценка критичности информационных активов. Идентификация и категорирование угроз. Технология обработки рисков информационной безопасности. Методы количественной и качественной оценки

рисков информационной безопасности. Идентификация и категорирование уязвимостей. Анализ уязвимости процессов переработки информации: скомпрометированные процессы и процессы, обладающие недекларированными возможностями.

Практическое занятие. Определение величины рисков нарушения информационной безопасности.

Самостоятельная работа. Инструментальные средства анализа рисков информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [21]

РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 6. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида

Методы обеспечения безопасности информации: препятствование, управление доступом, маскировка, регламентация, принуждение, побуждение. Классификация аппаратно-программных средства защиты информационных систем и ресурсов. Встроенные сервисы безопасности и специализированные средства идентификации/аутентификации, контроля доступа, обеспечения целостности, протоколирования, аудита, экранирования. Организационные средства защиты информационных систем и ресурсов: политики, инструкции, предписания и регламенты.

Практическое занятие. Установка и настройка программного средства защиты от НСД.

Самостоятельная работа. Назначение, основные функциональные возможности и устройство типового аппаратно-программного модуля доверенной загрузки.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [10, 11]

Тема 7. Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности

Принципы создания новых средств защиты информации и обеспечения информационной безопасности. Принципы совершенствования существующих средств защиты информации и обеспечения информационной безопасности. Известные технические, математические и организационные решения по

созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Самостоятельная работа. Частные технические, математические и организационные решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [3]

РАЗДЕЛ 4. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ

Тема 8. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа

Понятие идентификации, аутентификации и авторизации. Технологии идентификации: кодовая, радиочастотная, биометрическая, смарт-карточная. Технологии аутентификации: однофакторная и многофакторная, одноразовые и многоразовые пароли, цифровые сертификаты. Администрирование доступа субъектов к ресурсам системы. Системы разграничения доступа: требования к реализации диспетчера доступа и представление матрицы управления доступом.

Практическое занятие. Настройка программного средства СКУД.

Самостоятельная работа. Назначение, основные функциональные возможности и устройство типовой СКУД.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [7]

РАЗДЕЛ 5. ПРОТИВОДЕЙСТВИЕ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем

Основания классификации моделей противодействия угрозам нарушения информационной безопасности: этап противодействия, вид среды взаимодействия, тип нарушителя, способ формализации, цель моделирования. Иерархия и характеристика моделей противодействия угрозам нарушения информационной безопасности по уровню абстракции.

Практическое занятие. Теоретико-игровое моделирование противодействия угрозам нарушения информационной безопасности.

Самостоятельная работа. Модели пространственно-временного распределения ресурсов для обеспечения информационной безопасности в условиях вероятностного риска.

Рекомендуемая литература:
основная: [2 – 4]
дополнительная: [1, 2]
нормативно-правовые акты: [4, 18–20]

Тема 10. Модели и методы формирования комплексов средств противодействия угрозам безопасности информации и нарушения информационной безопасности для различного вида объектов защиты

Способы совместного применения средств противодействия угрозам нарушения информационной безопасности: межмодульное взаимодействие, комплексирование, интеграция. Централизованная и распределенная архитектура организации взаимодействия средств противодействия. Функциональная, структурная и потоковая модели формирования комплексов средств противодействия.

Самостоятельная работа. Методы комплексирования средств противодействия.

Рекомендуемая литература:
основная: [2 – 4]
дополнительная: [1, 2]
нормативно-правовые акты: [4, 18 – 20]

Тема 11. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет

Общеархитектурные и специальные механизмы сетевой защиты. Методы реализации стандартизованных механизмов сетевой защиты. Генерация новых механизмов сетевой защиты; метод доверенной маршрутизации. Средства информационного противодействия угрозам нарушения информационной безопасности в сетях общего пользования.

Практическое занятие. Администрирование программного межсетевого экрана.

Самостоятельная работа. Назначение, основные функциональные возможности и устройство типового межсетевого экрана.

Рекомендуемая литература:
основная: [2 – 4]
дополнительная: [1, 2]
нормативно-правовые акты: [8, 11, 23–25]

РАЗДЕЛ 6. ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 12. Модели и методы оценки защищенности информации и информационной безопасности объекта

Методологические подходы к оценке информационной безопасности. Критерии и показатели определения требуемого уровня защищенности объекта.

Методы, используемые для оценки защищенности информации и информационной безопасности: экспертный опрос, нечеткая логика, решение задач на графах, нормативные и стандартизированные методики.

Практическое занятие. Решение типовых задач оценки защищенности информации и информационной безопасности объекта: определение а) требуемого и текущего количества установленных средств защиты, б) требуемой и текущей меры структурной защищенности объекта, в) оптимального расположения точек контроля на графе объекта, г) определения оптимального уровня всех точек контроля через анализ структурной защищенности.

Самостоятельная работа. ГОСТ Р ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Часть 2. Функциональные компоненты безопасности. Часть 3. Компоненты доверия к безопасности. ГОСТ Р ИСО/МЭК 18045. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК ТО 19791. Оценка безопасности автоматизированных систем.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [12–14, 17]

Тема 13. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты

Инфраструктурная безопасность vs информационная безопасность бизнес-процессов. Введение меры в пространство количественных, качественных показателей и критериев эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты; формулирование интегрального показателя. Методы оценки качества и эффективности комплексной системы обеспечения информационной безопасности: вероятностный, оценочный, экспертный.

Практическое занятие. Аналитическое и имитационное моделирование для получения значений частных и интегрального показателя оценки эффективности системы обеспечения информационной безопасности.

Самостоятельная работа. Метод анализа иерархий Т. Саати применительно к задачам оценки эффективности систем (комплексов) обеспечения информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [12 – 14, 17]

РАЗДЕЛ 7. МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 14. Модели и методы управления информационной безопасностью

Архитектура системы обеспечения информационной безопасности. Виды моделей управления информационной безопасностью; процессная модель. Основные принципы создания системы управления информационной безопасностью. Стандартизованная процедура внедрения системы управления информационной безопасностью. Сертификация системы управления информационной безопасностью.

Самостоятельная работа. ГОСТ Р ИСО/МЭК 13335. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. ГОСТ Р ИСО/МЭК 27001. Системы менеджмента информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [10, 11, 16, 18–21]

Тема 15. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления

Назначение, цели и задачи политики обеспечения информационной безопасности. Типовая структура политики обеспечения информационной безопасности. Механизмы формирования политики обеспечения информационной безопасности. Типовые мероприятия политики обеспечения информационной безопасности. Ответственность за реализацию и нарушение политики обеспечения информационной безопасности. Профилактика нарушений политики обеспечения информационной безопасности.

Практическое занятие. Написание политики безопасности для типового объекта информатизации.

Самостоятельная работа. Порядок расследования инцидентов информационной безопасности.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [10, 11, 15, 16, 18 – 21]

РАЗДЕЛ 8. ПРИКЛАДНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 16. Системы документооборота и средства зашиты циркулирующей в них информации

Понятие документа и системы документооборота. Феномен электронного обмена документальной информацией. Модель электронного документа и его свойства; дуализм электронного документа. Организация защищенного документооборота. Механизмы и средства программно-аппаратной защиты информации в электронной среде.

Семинарское занятие. Защита электронных документов.

Самостоятельная работа. Системы защищенного электронного документооборота.

Рекомендуемая литература:

основная: [2 – 4]

дополнительная: [1, 2]

нормативно-правовые акты: [25]

5. Методические рекомендации по организации изучения дисциплины «Методы и системы защиты информации, информационная безопасность»

При реализации программы дисциплина «Методы и системы защиты информации, информационная безопасность» используются такие виды занятий: лекция, практическое занятие, семинарское занятие.

Лекция: составляет основу теоретического обучения и должна давать систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Практическое занятие: практическое занятие проводится в целях: выработки практических умений и приобретения навыков, закрепления пройденного материала по соответствующей теме.

Семинарские занятия имеют целью углубленное изучение дисциплины, привитие обучающимся навыков самостоятельного поиска и анализа учебной информации, формирование и развитие у них научного мышления, умения активно участвовать в творческой дискуссии, делать правильные выводы, аргументировано излагать и отстаивать свое мнение. На такие занятия могут быть вынесены для обсуждения доклады (сообщения), тематика которых должна раскрывать часть учебного вопроса, детализировать или иллюстрировать обсуждаемый на занятии материал. Для подготовки докладов (сообщений) заблаговременно назначаются докладчики, им персонально ставятся задачи, уточняются содержание и методика изложения материала. Рекомендации по подготовке докладов могут включаться в задание к практическому занятию.

Реферат является важнейшим элементом самостоятельной работы обучающихся при обучении в адъюнктуре. Основной целью реферата является создание и развитие навыков исследовательской работы, умения работать с

научной литературой, в том числе периодическими изданиями, делать на основе их изучения выводы и обобщения.

Консультация проводится перед экзаменом с целью обобщения материала по всей дисциплине и ответа на наиболее трудные вопросы, возникающие у обучающихся при изучении дисциплины.

Самостоятельная работа: направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим учебным занятиям, к экзамену.

6. Оценочные средства для проведения промежуточных аттестаций обучающихся

6.1. Типовые контрольные вопросы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов к кандидатскому экзамену по дисциплине «Методы и системы защиты информации, информационная безопасность»

1. Эволюция проблематики в сфере информационной безопасности и защиты информации.
2. Основные термины и определения в сфере информационной безопасности и защиты информации.
3. «Ландшафт» информационной безопасности: взаимодействие базовых элементов теории.
4. Принципы обеспечения информационной безопасности.
5. Абстрактная модель системы защиты информации: основные понятия.
6. Основы формальной теории защиты информации: монитор безопасности, модель разграничения доступа.
7. Классификация и взаимосвязь моделей безопасности.
8. Модели дискреционного доступа.
9. Модели мандатного доступа.
10. Ролевые модели доступа.
11. Модели безопасности информационных потоков.
12. Классификационные признаки и известные классификации угроз нарушения информационной безопасности.
13. Методы идентификации угроз нарушения информационной безопасности.
14. Базовая и частные модели угроз информационной безопасности.
15. Типовые модели нарушителей информационной безопасности.
16. Средства выявления угроз нарушения информационной безопасности.
17. Назначение, цели и задачи аудита информационной безопасности компании.

18. Принципы и формы проведения аудита информационной безопасности.
19. Основные стадии аудита: планирование, моделирование, тестирование, анализ, разработка предложений, документирование.
20. Методы аудита: экспертно-аналитические, экспертно-инструментальные, моделирование действий злоумышленника.
21. Инструментальные средства проведения активного аудита информационной безопасности.
22. Категорирование и оценка критичности информационных активов.
23. Технология обработки рисков информационной безопасности.
24. Методы количественной и качественной оценки рисков информационной безопасности.
25. Идентификация и категорирование уязвимостей.
26. Анализ уязвимости процессов переработки информации: скомпрометированные процессы и процессы, обладающие недекларированными возможностями.
27. Инструментальные средства анализа рисков информационной безопасности.
28. Методы обеспечения безопасности информации.
29. Классификация аппаратно-программных средства защиты информационных систем и ресурсов.
30. Организационные средства защиты информационных систем и ресурсов.
31. Принципы создания новых средств защиты информации и обеспечения информационной безопасности.
32. Принципы совершенствования существующих средств защиты информации и обеспечения информационной безопасности.
33. Известные технические, математические и организационные решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
34. Понятие идентификации, аутентификации и авторизации.
35. Технологии идентификации: кодовая, радиочастотная, биометрическая, смарт-карточная.
36. Технологии аутентификации: однофакторная и многофакторная, одноразовые и многоразовые пароли, цифровые сертификаты.
37. Системы разграничения доступа: требования к реализации диспетчера доступа и представление матрицы управления доступом.
38. Основания классификации моделей противодействия угрозам нарушения информационной безопасности.
39. Теоретико-игровые модели противодействия угрозам нарушения информационной безопасности.
40. Модели пространственно-временного распределения ресурсов для обеспечения информационной безопасности в условиях вероятностного риска.
41. Способы совместного применения средств противодействия угрозам нарушения информационной безопасности.
42. Общеархитектурные и специальные механизмы сетевой защиты.

43. Средства информационного противодействия угрозам нарушения информационной безопасности в сетях общего пользования.

44. Методологические подходы к оценке информационной безопасности.

45. Критерии и показатели определения требуемого уровня защищенности объекта.

46. Методы, используемые для оценки защищенности информации и информационной безопасности.

47. Методы оценки качества и эффективности комплексной системы обеспечения информационной безопасности.

48. Способы получения значений частных и интегрального показателя оценки эффективности системы обеспечения информационной безопасности.

49. Основные принципы создания и архитектура системы обеспечения информационной безопасности.

50. Процессная модель обеспечения информационной безопасности.

51. Стандартизованная процедура внедрения системы управления информационной безопасностью.

52. Сертификация системы управления информационной безопасностью.

53. Назначение, цели, задачи и типовая структура политики обеспечения информационной безопасности.

54. Ответственность за реализацию и нарушение политики обеспечения информационной безопасности.

55. Профилактика нарушений политики обеспечения информационной безопасности.

56. Порядок расследования инцидентов информационной безопасности.

57. Феномен электронного обмена документальной информацией.

58. Модель электронного документа и его свойства; дуализм электронного документа.

59. Организация защищенного документооборота.

60. Механизмы и средства программно-аппаратной защиты информации в электронной среде.

Примерные темы рефератов по дисциплине

1. Основные тенденции и закономерности в сфере информационной безопасности и защиты информации.

2. Понятие «угрозы» как элемента «ландшафта» информационной безопасности: стандартизованные и авторское определение, «семантическое» дерево.

3. Сравнительный анализ моделей доступа.

4. Классификационные признаки и известные классификации угроз нарушения информационной безопасности.

5. Идентификация и категорирование угроз информационной безопасности.

6. Идентификация и категорирование уязвимостей программного

обеспечения.

7. Классификация аппаратно-программных средства защиты информационных систем и ресурсов.

8. Встроенные сервисы безопасности.

9. Комплексное решение антивирусной защиты.

10. Средства идентификации и аутентификации пользователей мобильных приложений: обзор и сравнительная оценка..

11. Прикладные проблемы авторизации

12. Обзор Российского рынка СКУД.

13. Общеархитектурные механизмы сетевой защиты: обзор и сравнительная оценка.

14. Специальные механизмы сетевой защиты: обзор и сравнительная оценка.

15. Иерархия и характеристика моделей противодействия угрозам нарушения информационной безопасности по уровню абстракции.

16. Критерии оценки устойчивости и непрерывности бизнес-процессов, протекающих в корпоративных информационных системах.

17. Иерархия показателей и критериев эффективности обеспечения информационной безопасности.

18. Оценка затрат на систему информационной безопасности.

19. Стандарты менеджменты информационной безопасности.

20. Типовые мероприятия политики обеспечения информационной безопасности.

21. Ответственность за нарушение политики обеспечения информационной безопасности.

22. Материя и энергия как категории носителей информации

23. Существующие модели защиты электронной информации

24. Системы защищенного электронного документооборота: обзор Российского рынка.

Методика оценивания совокупности знаний, умений и навыков, характеризующих этапы формирования компетенций

В процессе изучения дисциплины процедурами оценивания образовательных достижений обучающихся при завершении этапа формирования компетенций является экзамен.

Промежуточная аттестация: кандидатский экзамен

№	Показатели достижения планируемого уровня компетенций	Шкала оценивания
1	Обучающийся показывает всесторонние и глубокие знания программного материала, знание основной и дополнительной литературы; последовательно и четко отвечает на вопросы билета и	*Оценка «5»* Отлично

	дополнительные вопросы; уверенно ориентируется в проблемных ситуациях; демонстрирует способность применять теоретические знания для анализа практических ситуаций, делать правильные выводы, проявляет творческие способности в понимании, изложении и использовании программного материала.	
2	Обучающийся показывает полное знание программного материала, основной и дополнительной литературы; дает полные ответы на теоретические вопросы билета и дополнительные вопросы, допуская некоторые неточности; правильно применяет теоретические положения к оценке практических ситуаций; демонстрирует хороший уровень освоения материала.	*Оценка «4»* Хорошо
3	Обучающийся показывает знание основного материала в объеме, необходимом для предстоящей профессиональной деятельности; при ответе на вопросы билета и дополнительные вопросы не допускает грубых ошибок, но испытывает затруднения в последовательности их изложения; не в полной мере демонстрирует способность применять теоретические знания для анализа практических ситуаций.	*Оценка «3»* Удовлетворительно
4	Обучающийся имеет существенные пробелы в знаниях основного учебного материала по дисциплине; не способен аргументировано и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на задаваемые комиссией вопросы или затрудняется с ответом.	*Оценка «2»* неудовлетворительно

7. Ресурсное обеспечение дисциплины «Методы и системы защиты информации, информационная безопасность»

7.1 Перечень основной и дополнительной учебной литературы

Основная литература

1. Криптографические методы защиты информации: учебное пособие: [гриф УМО] / Б.Я. Рябко, А.Н. Фионов. – 2-е изд., стер. – М.: Горячая линия - Телеком, 2014. – 229 с.: ил. –ISBN 978-5-9912-0286-2.

2. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. –300 с. (http://192.168.0.15/?19&type=card&cid=ALSFR-a2e62800-d42d-4e9c-9bc9-4c1d7b9f0f55)

3. Синещук, Ю.И. Информационные технологии и защита информации в автоматизированных системах управления МЧС России: учебное пособие для слушателей: [гриф МЧС] / Ю.И. Синещук, С.Н. Терехин, В.В. Духанин; ред. В.С. Артамонов; МЧС России. – СПб.: СПбУ ГПС МЧС России, 2010. – 284 с. – (http://192.168.0.15/?42&type=card&cid=ALSFR-6d86bbe6-aeac-49db-bc2e-068c7a55cb8d)

4. Ярочкин, В.И. Информационная безопасность: учебник для вузов: [гриф Мин. обр.] / В.И. Ярочкин. – 5-е изд. – М.: Академический проект, 2008. – 544 с. (http://192.168.0.15/?48&type=card&cid=ALSFR-7c3626db-06b0-4690-b022-0db0ed774cfd)

Дополнительная литература

1. Грибунин, В.Г. Комплексная система защиты информации на предприятии: учебное пособие: [гриф УМО] / В.Г. Грибунин, В.В. Чудовский. – М.: Академия, 2009. – 416 с.

2. Мельников, В.П. Информационная безопасность и защита информации: учебное пособие: [гриф УМО] / В.П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. – 4-е изд., стер.–М.: Академия, 2009. – 332 с.

Нормативно-правовые акты

1. ФЗ № 149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/364-federalnyj-zakon-ot-27-iyulya-2006-g-n-149-fz.

2. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_50922-2006.

3. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_51275-2006.

4. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_51583-2014.

5. ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_52069.0-2013.

6. ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_52448-2005.

7. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_52633.0-2006.

8. ГОСТ Р 53110-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_53110-2008.

9. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_53114-

2008.

10. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_13335-1-2006.

11. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_%D0%A2%D0%9E_13335-5-2006.

12. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_15408-1-2012.

13. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности»
http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_15408-2-2013.

14. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_15408-3-20133.

15. ГОСТ Р ИСО/МЭК ТО 15446-2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_%D0%A2%D0%9E_15446-2008.

16. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_%D0%A2%D0%9E_18044-2007.

17. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_18045-2013.

18. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы

и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27000-2012.

19. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27002-2012.

20. ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27003-2012.

21. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27005-2010.

22. ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27007-2014.

23. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27033-1-2011.

24. ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27033-3-2014.

25. ГОСТ Р ИСО/МЭК 27034-1-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия» http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A_27034-1-2014.

Доступ к информационно-телекоммуникационной сети «Интернет» как на территории университета, так и вне ее, обеспечивает дисциплину следующими рекомендуемыми к изучению материалами:

Периодические издания

1. Журнал «Защита информации. Инсайд» (официальный сайтhttp://www.inside-zi.ru).

2. Журнал «InformationSecurity. Информационная безопасность» (официальный сайт –http://www.itsec.ru/main.php).

3. Журнал «Проблемы информационной безопасности. Компьютерные системы» (официальный сайт–http://jisp.ru).

7.2. Материально-техническое обеспечение дисциплины «Методы и системы защиты информации, информационная безопасность»

Для проведения и обеспечения занятий используются специальные помещения, представляющие собой учебные аудитории, а также помещения для самостоятельной работы.

Технические средства обучения:

- Мультимедийный проектор,
- Проекционный экран,
- Персональный компьютер.

7.3. Перечень лицензионного программного обеспечения

1. Microsoft Windows Professional, Russian – Системное программное обеспечение. Операционная система. [Коммерческая (Volume Licensing)]; ПО-BE8-834;
2. Microsoft Office Standard (Word, Excel, Access, PowerPoint, Outlook, On-eNote, Publisher) – Пакет офисных приложений [Коммерческая (Volume Licens-ing)]; ПО-D86-664;
3. Adobe Acrobat Reader DC – Приложение для создания и просмотра электронных публикаций в формате PDF [Бесплатная]; ПО-F63-948;
4. MathCad 14 – Программный продукт для выполнения инженерных и математических расчетов [Коммерческая (Full Package Product)]; ПО-6E1-625;
5. MatLab 2009 – Высокоуровневый язык технических расчетов, интерак-тивная среда разработки алгоритмов [Коммерческая (Full Package Product)]; ПО-162-655;
6. Microsoft Project – Программное обеспечение управления проектами и оптимизации управления портфелями [Коммерческая (Full Package Product)]; ПО-0F5-190;
7. Microsoft Visio 2010 – Векторный графический редактор диаграмм и блок-схем [Коммерческая (Full Package Product)]; ПО-ADB-298;
8. Google Chrome – Браузер [Открытая]; ПО-F2C-926.

7.4. Перечень современных профессиональных баз данных и информационных справочных систем

При реализации используются следующие современные профессиональные базы данных (в том числе международные реферативные базы данных научных изданий) и информационные справочные системы, к которым обеспечен доступ:

1. Международная реферативная база данных научных изданий Scopus [Электронный ресурс]. – Режим доступа: https://www.scopus.com/, доступ только после самостоятельной регистрации;
2. Международная реферативная база данных научных изданий Web of Science [Электронный ресурс]. – Режим доступа: https://www.clarivate.ru/products/web-of-science/, доступ только после самостоятельной регистрации;
3. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации;
4. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ;
5. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный доступ.

Авторы: доктор технических наук, профессор Буйневич М.В., кандидат технических наук, доцент Матвеев А.В.