УТВЕРЖДЕНО:
Ученым советом Высшей школы сервиса
Протокол № 1 от «29» 09. 2010г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.1.2 Защита пространственной информации

основной профессиональной образовательной программы высшего образования – программы

магистратуры

по направлению подготовки: *43.04.01 Сервис*

направленность (профиль): *Геоинформационный сервис*

Квалификация: *магистр*

Год начала подготовки: 2021

Разработчики:

должность	ученая степень и звание, ФИО
Доцент	***к.т.н., доцент Шайтура С.В.***

Рабочая программа согласована и одобрена директором ОПОП:

должность	ученая степень и звание, ФИО
Доцент высшей школы сервиса	***К.т.н., Шайтура С.В.***

1. Аннотация рабочей программы дисциплины

Дисциплина «Защита пространственной информации» программы магистратуры 43.04.01 «Сервис» профиль «Геоинформационный сервис» относится к вариативной части программы.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК УВ-2 - Способен применять интеллектуальные технологии для обработки и защиты геоданных; в части индикаторов достижения компетенции ПК УВ-2.1. (Осуществляет выбор интеллектуальных технологий и специализированного программного обеспечения для решения задач обработки и защиты геоданных), ПК УВ-2.1. (Применяет интеллектуальные технологии для обработки и защиты геоданных в профессиональной деятельности).

Содержание дисциплины охватывает круг вопросов, связанных с формированием и развитием технологических навыков к обоснованию и разработке технологии, выбору ресурсов и технических средств для реализации процесса защиты геопространственных данных.

Дисциплина включает шесть разделов. Первый раздел «Защита интернет ресурсов» знакомит студентов с основными направлениями деятельности по обеспечению информационной безопасности и защите информации в глобальной сети. Рассматриваются аспекты нормативно-правовой базы, регламентирующей данную деятельность, задачи руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей и, конечно, методов их применения.

Во втором разделе «Защита баз данных» рассматриваются такие вопросы как угрозы безопасности баз данных, политика безопасности, восстановление базы данных.

Третий раздел «Защита серверных операций» включает вопросы системы защиты программного обеспечения, серверные операционные системы и их защита, защита внутренней сети от атак.

Четвертый раздел «Защита сетей и каналов» рассматривает сстратегии защиты информационных систем при работе в Интернет. Защита Интернет сервера. Обеспечение безопасности WEB-серверов. Особенности использования и настойки стандартных картографических серверов. Анализ вариантов реализации картографического Интернет сервера. Вопросы реализации Интернет сервера с помощью базовой геоинформационной системы. Методы защиты ИС, используемой для решения корпоративных задач. Разработка технических средств по защите данных в сетевой геоинформационной системе. Возможности шифрования пакетов на различных сетевых уровнях. Обоснование перечня организационных мероприятий по защите данных в сетевой геоинформационной системе.

Пятый раздел «Защита клиентских операций» посвящен защите информации в персональной ИС массового использования, защите информации в персональной настольной ИС, ккриптографической защите хранимых и обрабатываемых данных в ИС, выбору криптографического алгоритма для защиты персональных ИС.

Шестой раздел «Защита геоинформационных сетей» рассматривает особенности защиты распределенных геопространственных данных: пространственной базы данных, пространственной клиентской части, шифрование пространственных данных.

Общая трудоемкость освоения дисциплины составляет 14 зачетных единиц, 504 часов.

Преподавание дисциплины ведется:

На заочной форме обучения 1 - 2 курсах, с 1 по 3 семестры, и предусматривает проведение учебных занятий следующих видов: лекции (14 ч), в том числе, традиционные лекции с презентацией, практические занятия в форме выполнения практических работ (24 ч.), самостоятельная работа обучающихся (456 ч.), групповые и индивидуальные консультации (12 ч), промежуточная аттестация (4 ч.).

Программой предусмотрены следующие виды контроля:

На заочной форме обучения текущий контроль успеваемости в форме защиты практических работ, тестирования; промежуточная аттестация в форме зачета во 2 семестре и экзамена в 3 семестре.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

№ пп	Индекс компетенции, индикатора	Планируемые результаты обучения (компетенции, индикатора)
1	ПК УВ-2	Способен применять интеллектуальные технологии для обработки и защиты геоданных ПК УВ-2.1. Осуществляет выбор интеллектуальных технологий и специализированного программного обеспечения для решения задач обработки и защиты геоданных ПК УВ-2.1. Применяет интеллектуальные технологии для обработки и защиты геоданных в профессиональной деятельности

3. Место дисциплины (модуля) в структуре ООП:

Дисциплина «Защита пространственной информации» входит в вариативную часть блока Б.1 по направлению 43.03.01 Сервис профиль «Геоинформационный сервис».

Формирование компетенции ПК УВ-2 - Способен применять интеллектуальные технологии для обработки и защиты геоданных *начинается* в дисциплине «Защита пространственной информации» в 1 – 3 семестре.

Компетенция ПК УВ-2 *заканчивает* формироваться при изучении дисциплин: в 4 семестре «Преддипломная практика» в 4 семестре и при выполнении ВКР.

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

Общая трудоемкость дисциплины составляет _14_ зачетных единицы/ 504 акад.часов.

Для заочной формы обучения:

Виды учебной деятельности	Всего	Семестры		
		1	2	3
Контактная работа обучающихся с преподавателем	**48**	**4**	**22**	**22**
в том числе:				
Лекции	14	2	6	6
Практические занятия	24		12	12
Консультации	6	2	2	2
Промежуточная аттестация	4		2	2
Самостоятельная работа	**456**	**140**	**158**	**158**
Форма промежуточной аттестации			**Зачет**	**Экз.**
Общая трудоемкость час	**504**	**144**	**180**	**180**
з.е.	**14**	**4**	**5**	**5**

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
Для заочной формы обучения.

Номер недели семестра	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРС	Виды учебных занятий и формы их проведения					
			Лекции, акад. Часов	Форма проведения лекции	Практические занятия, акад.часов	Форма проведения практического занятия	СРС, акад.часов	Форма проведения СРС
1	**1.** Защита интернет ресурсов	Подходы к построению надежной информационной системы	0.5	Традиционная с презентацией			70	Изучение лекционного материала. Самостоятельное изучение отдельных тем блока. Подготовка к практическим занятиям
1		Межсетевые экраны	0.5					
1		Защита от атак						
1								
1								
1								
1	2. Защита баз данных	Угрозы безопасности баз данных	0.5	Традиционная с презентацией			70	Изучение лекционного материала. Самостоятельное изучение отдельных тем блока. Подготовка к практическим занятиям
1		Политика безопасности	0.5					

Номер недели семестра	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРС	Виды учебных занятий и формы их проведения					
			Лекции, акад. Часов	Форма проведения лекции	Практические занятия, акад.часов	Форма проведения практического занятия	СРС, акад.часов	Форма проведения СРС
1		Восстановление базы данных						
1								
1								
1								
Консультация – 2 часа								
Промежуточная аттестация – зачет – 2 часа								
2	3. Защита серверных операционных систем	Системы защиты программного обеспечения	1	Традиционная с презентацией			79	Изучение лекционного материала. Самостоятельное изучение отдельных тем блока. Подготовка к практическим занятиям
2		Серверные операционные системы	1					
2		Защита внутренней сети от атак	1					
2								
2								

Номер недели семестра	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРС	Виды учебных занятий и формы их проведения					
			Лекции, акад. Часов	Форма проведения лекции	Практические занятия, акад.часов	Форма проведения практического занятия	СРС, акад.часов	Форма проведения СРС
2								
2		ПЗ 1. Оценка уязвимостей активов			4	Практическая работа		
2		Тестирование . (К.т.№1)			1	тестирование		
2		Тестирование. (К.т.№2)			1	Тестирование		
2	4. Защита сетей и каналов	Технологии аутентификации	2	Традиционная с презентацией			79	Изучение лекционного материала. Самостоятельное изучение отдельных тем блока. Подготовка к практическим занятиям
2		Создание виртуальных защищённых сетей	1					
2		ПЗ 2 Оценка угроз активам			4	Практическая работа		
2		Тестирование . (К.т.№3)			1	тестирование		
2		Тестирование. (К.т.№4)			1	Тестирование		
Консультация – 2 часа								
Промежуточная аттестация – экзамен – 2 часа								

Номер недели семестра	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРС	Виды учебных занятий и формы их проведения					
			Лекции, акад. Часов	Форма проведения лекции	Практические занятия, акад.часов	Форма проведения практического занятия	СРС, акад.часов	Форма проведения СРС
3	5 Защита клиентских операционных систем	Классификация операционных систем	1	Традиционная с презентацией			79	Изучение лекционного материала. Самостоятельное изучение отдельных тем блока. Подготовка к практическим занятиям
3		Угрозы информации в информационно-вычислительных системах	1					
3		Защита информации в информационно-вычислительных системах	1					
3		ПЗ 3: Оценка существующих и планируемых средств защиты			4	Практическая работа		
3		Тестирование (К.т.№1)			1	тестирование		
3		Тестирование (К.т.№2)			1	Тестирование		
3	6. Защита геоинформационных сетей	Защита геопространственных баз данных	1	Традиционная с презента-			79	Изучение лекционного материала. Самостоятельное изучение отдельных тем блока.

Номер недели семестра	Наименование раздела	Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРС	Виды учебных занятий и формы их проведения					
			Лекции, акад. Часов	Форма проведения лекции	Практические занятия, акад.часов	Форма проведения практического занятия	СРС, акад.часов	Форма проведения СРС
3		Защита клиентской части информационных систем	1	цией				Подготовка к практическим занятиям
3		Виды шифрования пространственной информации	1					
3		ПЗ 4: Оценка рисков			4	Практическая работа		
3		Тестирование. (К.т.№3)			1	тестирование		
3		Тестирование. (К.т.№4)			1	Тестирование		
Консультация – 2 часа								
Промежуточная аттестация – экзамен – 2 часа								

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

Для самостоятельной работы по дисциплине обучающиеся используют следующее учебно-методическое обеспечение:

№ п/п	Тема, трудоемкость в акад.ч.	Учебно-методическое обеспечение
1	Интеллектуальные информационные системы. Защита интернет ресурсов Заочная форма – 70	1.Информационные технологии и системы: Учеб. Пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. – 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014 2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. – 2-е изд. – М.: Форум: НИЦ ИНФРА-М, 2014. – 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900 3. Душин, В. К. Теоретические основы информационных процессов и систем : Учебник / В. К. Душин. – 5-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. Режим доступа: http://znanium.com/catalog.php?Bookinfo =450784 *Дополнительная литература* 1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670
2	Защита баз данных Заочная форма – 70	1.Информационные технологии и системы: Учеб. Пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. – 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014 2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. – 2-е изд. – М.: Форум: НИЦ ИНФРА-М, 2014. – 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900 3. Душин, В. К. Теоретические основы информационных процессов и систем : Учебник / В. К. Душин. – 5-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. Режим доступа: http://znanium.com/catalog.php?Bookinfo =450784 *Дополнительная литература* 1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670
3	Защита серверных операционных систем, Заочная форма – 79	1.Информационные технологии и системы: Учеб. Пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. – 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014 2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. – 2-е изд. – М.: Форум: НИЦ ИНФРА-М, 2014. – 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900 3. Душин, В. К. Теоретические основы инфор-

		мационных процессов и систем : Учебник / В. К. Душин. – 5-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. Режим доступа: http://znanium.com/catalog.php?Bookinfo =450784 *Дополнительная литература* 1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670
4	Защита сетей и каналов, Заочная форма – 79	1.Информационные технологии и системы: Учеб. Пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. – 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014 2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. – 2-е изд. – М.: Форум: НИЦ ИНФРА-М, 2014. – 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900 3. Душин, В. К. Теоретические основы информационных процессов и систем : Учебник / В. К. Душин. – 5-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. Режим доступа: http://znanium.com/catalog.php?Bookinfo =450784 *Дополнительная литература* 1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670
5	Защита клиентских операционных систем, Заочная форма – 79	1.Информационные технологии и системы: Учеб. Пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. – 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014 2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. – 2-е изд. – М.: Форум: НИЦ ИНФРА-М, 2014. – 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900 3. Душин, В. К. Теоретические основы информационных процессов и систем : Учебник / В. К. Душин. – 5-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. Режим доступа: http://znanium.com/catalog.php?Bookinfo =450784 *Дополнительная литература* 1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670
6	Защита геоинформационных сетей, Заочная форма – 79	1.Информационные технологии и системы: Учеб. Пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. – 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014 2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов.

		– 2-е изд. – М.: Форум: НИЦ ИНФРА-М, 2014. – 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900 3. Душин, В. К. Теоретические основы информационных процессов и систем : Учебник / В. К. Душин. – 5-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2014. Режим доступа: http://znanium.com/catalog.php?Bookinfo =450784 *Дополнительная литература* 1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670

7. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции, индикатора	Содержание компетенции, индикатора	Раздел дисциплины, обеспечивающий формирование компетенции, индикатора	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, индикатора обучающийся должен:		
				знать	уметь	владеть
1	ПК УВ-2	Способен применять интеллектуальные технологии для обработки и защиты геоданных				
		ПК УВ-2.1. Осуществляет выбор интеллектуальных технологий и специализированного программного обеспечения для решения задач обработки и защиты геоданных	Все разделы	Знает основные понятия и определения в сфере интеллектуальных технологий, защиты и обработки геоданных	Использует специализированное программное обеспечение в сфере интеллектуальных технологй	Производит выбор интеллектуальных технологий и специализированного программного обеспечения для решения задач обработки и защиты геоданных
		ПК УВ-2.1. Применяет интеллектуальные технологии для обработки и защиты геоданных в профессиональной деятельности		Знает принципы формирования интеллектуальных информационных технологий	Использует интеллектуальные системы для решения задач геомаркетинга	Применяет интеллектуальные технологии для обработки и защиты геоданных в профессиональной деятельности

7.2. Описание показателей и критериев оценивания компетенций на разных этапах их формирования, описание шкал оценивания

Результат обучения по дисциплине	Показатель оценивания	Критерий оценивания	Этап освоения компетенции
Знать основные определения и положения защиты информации; классификацию угроз и уязвимостей существующим информационным системам; основные защитные механизмы; программно-аппаратные средства защиты; руководящие документы регламентирующие безопасность геоинформационных систем. Уметь: классифицировать угрозы безопасности геоинформационным системам; описать процесс принятия решения при выборе технологии защиты информации; разрабатывать и внедрять модели обеспечения безопасности; проводить протоколирование и аудит безопасности; спроектировать комплексную систему безопасности. Владеть: практической работой со специализированным, прикладным программным обеспечением безопасности; умением применять стандарты и разрабатыватьи политику безопасности; методами оценки безопасности; методами подбора экспертных систем для решения различных задач	тестирование	Студент демонстрирует умение применять на основе знаний теоретических основ современных геоинформационных технологии в профессиональной деятельности Студент демонстрирует теоретические знания основ современных геоинформационных технологий. Студент демонстрирует владение навыками применения современных геоинформационных технологии в профессиональной деятельности.	Способен применять интеллектуальные технологии для обработки и защиты геоданных

Технология оценивания знаний обучающихся

Для оценки результатов обучения по дисциплине, т.е. знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы, в университете используются элементы балльно-рейтинговой технологии.

Балльно-рейтинговая технология оценки достижений обучающихся (далее - БРТ) предназначена для повышения объективности и достоверности определения уровня подготовки обучающихся и используется с целью формирования личностно-ориентированного обучения, стимулирования систематической работы обучающихся, раскрытия их творческих способностей, дифференциации оценки знаний и формирования итогового портфолио обучающегося,

отражающего все его достижений за время обучения в Университете.

БРТ позволяет обучающимся:

- понимать систему текущего оценивания по дисциплинам с целью получения по ним итоговых оценок;
- осознать необходимость систематической работы по выполнению учебного плана на основании знания своей текущей рейтинговой оценки по каждой дисциплине и ее изменение из-за освоения материала не в установленные преподавателем сроки;
- своевременно оценить состояние своей работы по изучению дисциплины, выполнению всех видов учебной работы до начала промежуточной аттестации;
- определить свой личный общий рейтинг и сравнить его с рейтингами других обучающихся.

В качестве внутренней шкалы текущих оценок используется 80 балльная оценка обучающихся по трем критериям: посещаемость, текущий контроль успеваемости, активность на учебных занятиях.

Распределение баллов между видами контроля устанавливается в следующем соотношении:

- посещение учебных занятий (до 30 баллов за посещение всех занятий);
- текущий контроль успеваемости (до 50 баллов), в том числе:
  1 задание текущего контроля (0-10 баллов)
  2 задание текущего контроля (0-10 баллов)
  3 задание текущего контроля (0-10 баллов)
  4 задание текущего контроля (0-15 баллов);
  5 бонусные рейтинговые баллы за активность на занятиях по итогам семестра (0-5 баллов).

При этом посещаемость занятий лекционного типа (за исключением поточных, более 100 человек) и занятий семинарского типа оценивается накопительно следующим образом: максимальное количество баллов, отводимых на учет посещаемости (30 баллов), делится на количество лекций (за исключением поточных, более 100 человек) и практических занятий по дисциплине. Полученное значение определяет количество баллов, набираемых обучающимся за посещение одного занятия.

При оценке выполнения заданий текущего контроля в баллах учитывается степень самостоятельности выполненной работы.

При проведении занятий семинарского типа фиксируется учебная активность обучающихся и при определении итогового рейтинга за семестр начислять за нее до 5 рейтинговых бонусных баллов.

Рейтинговые баллы набираются в течение всего периода обучения по дисциплине и фиксируются путем занесения в «Журнал учета посещаемости и текущего контроля успеваемости по дисциплине (модулю), практике» в ЭПОС университета.

Результаты текущего контроля успеваемости учитываются при выставлении оценки в ходе промежуточной аттестации следующим образом.

Оценка «отлично» выставляется только по результатам сдачи экзамена/дифференцированного зачета. Автоматическое проставление оценки «отлично» не допускается.

Если по результатам текущего контроля обучающийся набрал:

71-80 балл - имеет право получить «автоматом» «зачтено» или оценку «хорошо»;

62-70 баллов - имеет право получить «автоматом» «зачтено» или оценку « удовлетворительно»;

51-61 балл - обязан сдавать зачет/экзамен;

50 баллов и ниже — не допуск к зачету/экзамену.

Обучающийся имеет право улучшить оценку в результате непосредственной сдачи экзамена/дифференцированного зачета. Технология выставления итоговой оценки, в том числе перевод в итоговую 5-балльную шкалу оценки определяется следующим образом:

Таблица перевода рейтинговых баллов в итоговую 5 - балльную оценку

Баллы за семестр	Автоматическая оценка		Баллы за зачет/экзамен		Общая сумма баллов	Итоговая оценка
	зачтено	экзамен	min	max		
71-80	зачтено	4 (хорошо)	18	20	89-90	4 (хорошо)
					91-100	5(отлично)
62-70	зачтено	3(удовлетворительно)	15	20	77-90	4 (хорошо)
51-61	Допуск к зачету/экзамену		11	20	62-75	3(удовлетворительно'
					76-81	4 (хорошо)
50 и менее	Не допуск к зачету, экзамену					

Виды средств оценивания, применяемых при проведении текущего контроля и шкалы оценки уровня знаний, умений и навыков при выполнении отдельных форм текущего контроля

Средство оценивания – тестирование

Шкала оценки уровня знаний, умений и навыков при решении тестовых заданий

Критерии оценки	оценка
выполнено верно заданий	«5», если (90 –100)% правильных ответов
	«4», если (70 – 89)% правильных ответов
	«3», если (50 – 69)% правильных ответов
	«2», если менее 50% правильных ответов

Виды средств оценивания, применяемых при проведении промежуточной аттестации и шкалы оценки уровня знаний, умений и навыков при их выполнении

Устный опрос

Шкала оценки уровня знаний, умений и навыков при устном ответе

Оценка	Критерии оценивания	Показатели оценивания
«5»	– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание программного материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; – ответ прозвучал самостоятельно, без наводящих вопросов; – продемонстрирована способность творчески применять знание теории к решению профессиональных задач; – продемонстрировано знание современной учебной и научной литературы; – допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию	– Обучающийся показывает всесторонние и глубокие знания программного материала, – знание основной и дополнительной литературы; – последовательно и четко отвечает на вопросы билета и 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; – подтверждает полное освоение компетенций, предусмотренных программой
«4»	– вопросы излагаются систематизировано и последовательно; – продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; – продемонстрировано усвоение основной литературы. – ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: – а) в изложении допущены небольшие пробелы, не исказившие содержание ответа;	– 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 и в целом

	– б) допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; – в) допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя	подтверждает освоение компетенций, предусмотренных программой
«3»	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – усвоены основные категории по рассматриваемому и дополнительным вопросам; – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; – при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы	– 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; – подтверждает освоение компетенций, предусмотренных программой на минимально допустимом уровне
«2»	– не раскрыто основное содержание учебного материала; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов. – не сформированы компетенции, умения и навыки.	– 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 вопросы или затрудняется с ответом; – не подтверждает освоение компетенций, предусмотренных программой

оценочная шкала устного ответа

Процентный интервал оценки	**оценка**
менее 50%	**2**
51% - 70%	**3**
71% - 85%	**4**
86% - 100%	**5**

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Номер недели семестра	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	Вид и содержание контрольного задания	Требования к выполнению контрольного задания и срокам сдачи
1	*Блок 1.контрольные точки 1,2*	*Тест на выявление уровня освоения теоретических знаний по блоку «*Защита интернет ресурсов*»*	*Контрольная работа. 10 вариантов тестовых заданий. В каждом задании – 5 вопросов, с 5 вариантами ответа, правильный ответ один*
2	*Блок 2. Контрольные точки 3,4*	*Тест на выявление уровня освоения теоретических знаний по блоку «*Защита баз данных*»*	*10 вариантов тестовых заданий В каждом задании – 5 вопросов, с 5 вариантами ответа, правильный ответ один*
3	*Блок 3. Контрольные точки 1,2*	*Тест на выявление уровня освоения теоретических знаний по блоку «*Защита серверных операционных систем*»*	*10 вариантов тестовых заданий В каждом задании – 5 вопросов, с 5 вариантами ответа, правильный ответ один*
4	*Блок 4. контрольные точки 3,4*	*Тест на выявление уровня освоения теоретических знаний по блоку* Защита сетей и каналов*»*	*10 вариантов тестовых заданий В каждом задании – 5 вопросов, с 5 вариантами ответа, правильный ответ один*
5	*Блок 5. Контрольные точки 1,2*	*Тест на выявление уровня освоения теоретических знаний по блоку «*Защита клиентских операционных систем *»*	*10 вариантов тестовых заданий В каждом задании – 5 вопросов, с 5 вариантами ответа, правильный ответ один*
6	*Блок 6. Контрольные точки 3,4*	*Тест на выявление уровня освоения теоретических знаний по блоку «*Защита геоинформационных сетей*»*	*10 вариантов тестовых заданий В каждом задании – 5 вопросов, с 5 вариантами ответа, правильный ответ один*

БЛОК ПЕРВЫЙ «Защита интернет ресурсов»
1 контрольная точка: Вид контрольного задания – защита практических работ.

2 контрольная точка: Вид контрольного задания - тесты

1. Для отправки широковещательных сообщений в данный сетевой сегмент используется адрес …

a) **192.32.64.255**
b) 255.255.255.255
c) 255.255.255.0
d) 0.0.0.0

2. Сеть с адресом 190.25.32.0 принадлежит к классу …

a) A
b) **B**
c) C

3. Команда протокола SMTP, которая служит для указания адреса получателя сообщения, – …

a) HELO
b) **RCPT TO**
c) SEND
d) POST

4. Неверно, что адрес … является корректным MAC-адресом

a) 00457FEB7777
b) **FFFFFFFFFFF**
c) FE6794C76890

5. Протокол … реализует криптографическую защиту на канальном уровне

a) SSL
b) SSH
c) TCP
d) **PPTP**

6. Поле заголовка IP-датаграммы, которое показывает количество преодолеваемых маршрутизаторов, – …

a) Identification
b) Flags
c) IHL
d) **Time to Live**

7. Сообщение «…» относится к протоколу ICMP

a) **Network unreachable**
b) RCVD WILL STATUS
c) Transfer complete
d) PORT command successful

8. Пакет с установленным флагом … в заголовке первым посылается при установлении связи по протоколу TCP

a) **SYN**
b) FYN
c) ACK

9. Один из уровней стека протоколов TCP/IP – …

a) физический

b) канальный
c) **транспортный (transport)**
d) сеансовый

10.Авторизация – это процедура предоставления субъекту ...
a) **определенных полномочий и ресурсов в данной системе**
b) определенного идентификатора
c) определенной ключевой пары

Блок второй «Защита баз данных**»**
3 контрольная точка: Вид контрольного задания – защита практических работ, реферат.
Темы рефератов:

1. Сущность безопасности баз данных
2. Задачи обеспечения информационной безопасности баз данных.
3. Критерии качества баз данных
4. Угрозы информационной безопасности баз данных
5. Источники угроз информации баз данных
6. Классификация угроз информационной безопасности баз данных

4 контрольная точка: Вид контрольного задания - тесты.
Тесты:

1.Наиболее частый случай нарушения безопасности информационной системы – это …
a) атаки извне
b) обиженные сотрудники
c) **ошибки персонала**
d) вирусы

2.Аутентификация – это процедура проверки ...
a) **подлинности заявленного пользователя, процесса или устройства**
b) пользователя по его идентификатору
c) пользователя по его имени

3.S/Key – это протокол аутентификации на основе …
a) многоразовых паролей
b) PIN-кода
c) **одноразовых паролей**

4. Неверно, что к протоколу IP относится такая функция, как …
a) фрагментация
b) маршрутизация
c) **достоверность передачи**

5.Для защиты от прослушивания трафика при помощи сетевого анализатора может использоваться …

a) фильтрация трафика
b) **шифрование передаваемой информации**
c) дополнительная аутентификация

6.Сетевой адаптер, работающий в селективном режиме, игнорирует …
a) фреймы, не содержащие в поле «адрес получателя» адрес данного узла
b) широковещательные фреймы
c) **фреймы, не содержащие в поле «адрес получателя» адрес данного узла, и широковещательные фреймы**

7.Чтобы усилить защиту беспроводной сети, следует …
a) **изменить заводской SSID**
b) повысить уровень сложности паролей пользователей
c) защитить протокол SSNP

8.Трафик между клиентами и серверами во внутренней сети лучше всего защищать при помощи …
a) SAP
b) **SSL**
c) TPC

9.Маршруты типа «…» просматриваются в таблице в первую очередь
a) маршрутизация
b) маршрут к сети
c) маршрут по умолчанию
d) **маршрут к узлу**

10.Управление доступом – это **...**
a) защита персонала и ресурсов
b) реагирование на попытки несанкционированного доступа
c) **способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных)**

Блок третий «Защита серверных операционных систем**»**
1 контрольная точка: Вид контрольного задания – защита практических работ.

2 контрольная точка: Вид контрольного задания - тесты

Тесты:

1. Анализ рисков включает в себя …
a. набор адекватных контрмер, осуществляемый в ходе управления рисками
b. анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности
c. выявление существующих рисков и оценку их величины

d. мероприятия по обследованию безопасности ИС, с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите

2. Информация – это …
a. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
b. совокупность знаний, накопленная человечеством
c. совокупность принципов, методов и форм управления
d. совокупность рефлексий между идеей и материей на макро- и микроуровнях

3. Информационная безопасность, по законодательству РФ, – это …
a. методологический подход к обеспечению безопасности
b. свод норм, соблюдение которых призвано защитить компьютеры и сеть от несанкционированного доступа
c. состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства
d. состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства
e. маркетинг

4. Неверно, что … относят к источникам угроз информационной безопасности
a. человеческий фактор
b. правовые аспекты функционирования ИС
c. стихийные бедствия
d. аппаратные сбои
e. ошибки проектирования и разработки ИС

5. Система защиты информации – это …
a. комплексная совокупность программно-технических средств, обеспечивающая защиту информации
b. совокупность органов и/или исполнителей, а также используемая ими техника защиты информации
c. область информационных технологий
d. разработка стратегии защиты бизнеса компаний

6. Пользователь, (потребитель) информации – это …
a. фирма – разработчик программного продукта, которая занимается ее дистрибьюцией

b. пользователь, использующий совокупность программно-технических средств
c. субъект, пользующийся информацией, в соответствии с регламентом доступа
d. владелец фирмы или предприятия
e. все служащие предприятия

7. Право доступа к информации – это …
a. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
b. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
c. возможность доступа к информации, не нарушающая установленные правила разграничения доступа
d. нарушение установленных правил разграничения доступа
e. лицо или процесс, осуществляющие несанкционированный доступ к информации

8. На компьютерах может применяться локальная политика безопасности …
a. подстановки
b. гаммирования
c. параметров безопасности
d. симметричных криптографических преобразований

9. К основным видам систем обнаружения вторжений относятся … системы
a. активные и пассивные
b. локальные
c. межсетевые
d. синхронные

10. Утилиты скрытого управления позволяют …
a. переименовывать файлы и их расширения
b. вводить новую информацию
c. перезагружать компьютер

Блок четвертый «Защита сетей и каналов**»**
3 контрольная точка: Вид контрольного задания – защита практических работ.

4 контрольная точка: Вид контрольного задания - тесты:

1. Выделяют … уровень стека протоколов TCP/IP

а) физический
б) канальный
в) **сетевой (internet)**
г) сеансовый

2. Наиболее частый случай нарушения безопасности информационной системы – …

а) атаки извне
б) обиженные сотрудники
в) ошибки персонала
г) компьютерные вирусы

3. Авторизация – это процедура предоставления субъекту …

а) определенных полномочий и ресурсов в данной системе
б) определенного идентификатора
в) определенной ключевой пары

4. Аутентификация – это процедура проверки ...

а) подлинности заявленного пользователя, процесса или устройства
б) пользователя по его идентификатору
в) пользователя по его имен

5. Неверно, что к протоколу IP относится такая функция, как …

а) фрагментация
б) маршрутизация
в) достоверность передачи

6. Средства телекоммуникации – это …

а) совокупность средств связи, обеспечивающих передачу данных между ЭВМ и информационными системами, удаленными друг от друга на значительные расстояния;
б) комплекс технических средств передачи информации
в) проводное, оптико-волоконное и беспроводное соединение объектов

7. Неверно, что добавляется IP-заголовок к пакету протокола … из стека TCP/IP

а) ICMP
б) DHCP
в) ARP

8. К средствам технической защиты информации относятся ...

а) аппаратные и программные средства защиты
б) технические средства, предназначенные для предотвращения утечки информации по одному или нескольким техническим каналам
в) межсетевые экраны

9. Неверно, что … является состоянием соединения по протоколу TCP

а) LISTEN

б) SYN-SENT
в) WAIT
г) LAST-ACK

10. Службой TELNET обычно используется порт № …
а) 20
б) 21
в) 22
г) 23

БЛОК ПЯТЫЙ Защита клиентских операционных систем»
1 контрольная точка: Вид контрольного задания – защита практических работ.

2 контрольная точка: Вид контрольного задания - тесты:

11. Операционная система цифровой вычислительной системы предназначена для обеспечения …
a. **определенного уровня эффективности цифровой вычислительной системы за счет автоматизированного управления ее работой и предоставляемого пользователям набора услуг**
b. удобной работы пользователя
c. совмещения различных интерфейсов

12. Современную организацию ЭВМ предложил …
a. Норберт Винер
b. Джон фон Нейман
c. Чарльз Беббидж

13. В системное программное обеспечение входят …
a. языки программирования
b. операционные системы
c. графические редакторы
d. компьютерные игры
e. текстовые редакторы

14. Анализ рисков включает в себя …
a. набор адекватных контрмер, осуществляемый в ходе управления рисками
b. анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС в случае осуществления угрозы безопасности
c. выявление существующих рисков и оценку их величины
d. мероприятия по обследованию безопасности ИС с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите

15. Информация – это …

e. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
f. совокупность знаний, накопленная человечеством
g. совокупность принципов, методов и форм управления
h. совокупность рефлексий между идеей и материей на макро- и микроуровнях

16. Информационная сфера – это …

a. совокупность всех накопленных факторов в информационной деятельности людей
b. сфера деятельности человеко-машинного комплекса в процессе производства информации
c. **совокупность информации и субъектов, осуществляющих сбор, формирование, распространение и использование информации**
d. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
e. сфера, в которой производится и распространяется информация

17. Неверно, что … относят к источникам угроз информационной безопасности

f. человеческий фактор
g. правовые аспекты функционирования ИС
h. стихийные бедствия
i. аппаратные сбои
j. ошибки проектирования и разработки ИС

18. Система защиты информации – это …

a. комплексная совокупность программно-технических средств, обеспечивающих защиту информации
b. совокупность органов и/или исполнителей, а также используемая ими техника защиты информации
c. область информационных технологий
d. разработка стратегии защиты бизнеса компаний

19. Пользователь (потребитель) информации – это …

f. фирма – разработчик программного продукта, которая занимается ее дистрибьюцией
g. пользователь, использующий совокупность программно-технических средств
h. субъект, пользующийся информацией в соответствии с регламентом доступа
i. владелец фирмы или предприятия

j. все служащие предприятия

20.Право доступа к информации – это …

a. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
b. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
c. возможность доступа к информации, не нарушающая установленные правила разграничения доступа
d. нарушение установленных правил разграничения доступа
e. лицо или процесс, осуществляющие несанкционированного доступа к информации

Блок шестой «Защита геоинформационных сетей**»**
3 контрольная точка: Вид контрольного задания – защита практических работ.

4. контрольная точка: Вид контрольного задания - тесты:

1.Санкционированный доступ к информации – это …

a. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
b. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
c. доступ к информации, не нарушающий установленные правила разграничения доступа
d. нарушение установленных правил разграничения доступа
e. лицо или процесс, осуществляющие несанкционированного доступа к информации

2.Несанкционированный доступ к информации – это …

a. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
b. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
c. доступ к информации, не нарушающий установленные правила разграничения доступа, которые служат для регламентации права доступа к компонентам системы
d. **нарушение установленных правил разграничения доступа**
e. лицо или процесс, осуществляющие несанкционированный доступ к информации

3.Идентификация субъекта – это …

a. процедура распознавания субъекта по его идентификатору
b. проверка подлинности субъекта с данным идентификатором
c. установление того, является ли субъект именно тем, кем он себя объявил
d. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
e. установление лиц или процессов, осуществляющих несанкционированный доступ к информации

4.Аутентификация субъекта – это …
a. процедура распознавания субъекта по его идентификатору
b. проверка подлинности субъекта с данным идентификатором
c. установление того, является ли субъект именно тем, кем он себя объявил
d. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
e. установление лиц или процессов, осуществляющих несанкционированный доступ к информации

5.Авторизация субъекта – это …
a. процедура распознавания субъекта по его идентификатору
b. проверка подлинности субъекта с данным идентификатором
c. установление того, является ли субъект именно тем, кем он себя объявил
d. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
e. установление лиц или процессов, осуществляющих несанкционированный доступ к информации

6.Неверно, что … должны быть доступны в нормальной работе пользователя
a. системные утилиты и системные редакторы
b. средства защиты, системные утилиты
c. средства разработки, утилиты
d. средства защиты

7.По существующим правилам разрабатывать, производить защиты информации может только предприятие, имеющее …
a. лицензию
b. сертификат
c. начальный капитал
d. аккредитацию

8.В стандартной политике безопасности установка программных продуктов непосредственно пользователем корпоративной рабочей станции …

a. разрешена
b. разрешена, за исключением компьютерных игр
c. разрешена, но только с устного согласия сотрудника ИТ-отдела
d. запрещена

9.Под доступностью информации понимается …

f. возможность за приемлемое время получить требуемую информационную услугу
g. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
h. защита от несанкционированного доступа к информации

10.Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) …

a. влечет во всех случаях уголовную ответственность
b. влечет только наложение административного штрафа
c. не влечет за собой уголовной ответственности
d. влечет уголовную ответственность и наложение административного штрафа

Контрольные вопросы к зачету 2 семестр

1. Подходы к построению надежной информационной системы
2. Межсетевой экран – инструмент реализации политики безопасности.
3. Технические аспекты обеспечения безопасности
4. Программное обеспечение и конфигурация
5. Разработка и коррекция правил политики безопасности
6. Проблема информационной безопасности Internet
7. Правовые основы деятельности по защите информации от несанкционированного доступа
8. Режимы защиты информации
9. Компьютерные атаки. Защитита от атак
10. Классификация компьютерных атак
11. Защита от компьютерных атак
12. Безопасность TCP/IP
13. Инструментальные средства изучения защищенности информационных систем
14. Сущность безопасности баз данных
15. Задачи обеспечения информационной безопасности баз данных.
16. Критерии качества баз данных
17. Угрозы информационной безопасности баз данных
18. Источники угроз информации баз данных
19. Классификация угроз информационной безопасности баз данных
20. Классификация систем защиты программного обеспечения.
21. Достоинства и недостатки основных систем защиты.
22. Системы защиты от несанкционированного доступа
23. Программно-аппаратные средства защиты с электронными ключами.

24. Показатели эффективности систем защиты
25. Серверные операционные системы ведущих производителей
26. Проблемы информационной безопасности сетей
27. Анализ угроз сетевой безопасности.
28. Обеспечение информационной безопасности сетей
29. Угрозы и уязвимости проводных корпоративных сетей
30. Угрозы и уязвимости беспроводных сетей
31. Аутентификация, авторизация и администрирование действий пользователей.
32. Методы аутентификации, использующие пароли и PIN коды.
33. Строгая аутентификация.
34. Биометрическая аутентификация пользователя.
35. Функции МЭ.
36. Особенности функционирования МЭ на различных уровнях модели OSI.
37. Схемы сетевой защиты на базе МЭ.
38. Проблемы безопасности МЭ.
39. Концепция построения виртуальных защищенных сетей VPN.
40. VPN решения для построения защищенных сетей.
41. Достоинства применения технологий VPN.
42. Протоколы формирования защищенных каналов на канальном уровне.
43. Протоколы формирования защищенных каналов на сеансовом уровне.
44. Защита беспроводных сетей
45. Архитектура средств безопасности IPSec.
46. Защита передаваемых данных с помощью протоколов AH и ESP.
47. Протокол управления криптоключами IKE.
48. Особенности реализации средств IPSec.
49.

Тесты к зачету (2 семестр)

11. Для отправки широковещательных сообщений в данный сетевой сегмент используется адрес …

e) **192.32.64.255**
f) 255.255.255.255
g) 255.255.255.0
h) 0.0.0.0

12. Сеть с адресом 190.25.32.0 принадлежит к классу …

d) A
e) **B**
f) C

13. Команда протокола SMTP, которая служит для указания адреса получателя сообщения, – …

e) HELO
f) **RCPT TO**
g) SEND
h) POST

14. Неверно, что адрес … является корректным MAC-адресом

d) 00457FEB7777
e) **FFFFFFFFFFFF**
f) FE6794C76890

15.Протокол … реализует криптографическую защиту на канальном уровне
e) SSL
f) SSH
g) TCP
h) **PPTP**

16.Поле заголовка IP-датаграммы, которое показывает количество преодолеваемых маршрутизаторов, – …
e) Identification
f) Flags
g) IHL
h) **Time to Live**

17.Сообщение «…» относится к протоколу ICMP
e) **Network unreachable**
f) RCVD WILL STATUS
g) Transfer complete
h) PORT command successful

18.Пакет с установленным флагом … в заголовке первым посылается при установлении связи по протоколу TCP
d) **SYN**
e) FYN
f) ACK

19.Один из уровней стека протоколов TCP/IP – …
e) физический
f) канальный
g) **транспортный (transport)**
h) сеансовый

20.Авторизация – это процедура предоставления субъекту ...
d) **определенных полномочий и ресурсов в данной системе**
e) определенного идентификатора
f) определенной ключевой пары

21.Наиболее частый случай нарушения безопасности информационной системы – это …
e) атаки извне
f) обиженные сотрудники
g) **ошибки персонала**

h) вирусы

22.Аутентификация – это процедура проверки ...
d) **подлинности заявленного пользователя, процесса или устройства**
e) пользователя по его идентификатору
f) пользователя по его имени

23.S/Key – это протокол аутентификации на основе …
d) многоразовых паролей
e) PIN-кода
f) **одноразовых паролей**

24. Неверно, что к протоколу IP относится такая функция, как …
d) фрагментация
e) маршрутизация
f) **достоверность передачи**

25.Для защиты от прослушивания трафика при помощи сетевого анализатора может использоваться …
d) фильтрация трафика
e) **шифрование передаваемой информации**
f) дополнительная аутентификация

26.Сетевой адаптер, работающий в селективном режиме, игнорирует …
d) фреймы, не содержащие в поле «адрес получателя» адрес данного узла
e) широковещательные фреймы
f) **фреймы, не содержащие в поле «адрес получателя» адрес данного узла, и широковещательные фреймы**

27.Чтобы усилить защиту беспроводной сети, следует …
d) **изменить заводской SSID**
e) повысить уровень сложности паролей пользователей
f) защитить протокол SSNP

28.Трафик между клиентами и серверами во внутренней сети лучше всего защищать при помощи …
d) SAP
e) **SSL**
f) TPC

29.Маршруты типа «…» просматриваются в таблице в первую очередь
e) маршрутизация
f) маршрут к сети
g) маршрут по умолчанию

h) **маршрут к узлу**

30. Управление доступом – это ...
d) защита персонала и ресурсов
e) реагирование на попытки несанкционированного доступа
f) **способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных)**

31. Реакция ОС Windows на FIN-сканирование в случае закрытого порта – …
a) посылка пакета с флагами RST+ACK
b) **молчание**
c) посылка пакета с флагами SYN+ACK

32. Команда … является командой протокола FTP
a) **RNTO**
b) DIR
c) LS
d) GET

33. Маршрут … просматривается в таблице маршрутизации в первую очередь
a) к сети
b) по умолчанию
c) **к узлу**

34. Неверно, что… является характеристикой протокола UDP
a) наличие в заголовке поля «Контрольная сумма»
b) работа без установления соединения
c) **техника плавающего окна**

35. Набор данных, позволяющий поставить открытый ключ с объектом, имеющим соответствующий закрытый ключ, носит название «…»
a) модуль доступа
b) **цифровой сертификат**
c) конструктивный сертификат

36. Когда пользователь входит в домен, вводя реквизиты своей учетной записи, происходит …
a) **идентификация**
b) **аутентификация**
c) терминализация

37. Для централизованной аутентификации можно использовать …
a) **RADIUS**
b) RETAIL

c) CONNECT

38.Возможна атака … на DNS
a) **footprinting**
b) IP spoofing
c) fishing

39.IP-заголовок не добавляется к пакету протокола … из стека TCP/IP
a) ICMP
b) DHCP
c) **ARP**

40.Неверно, что … является состоянием соединения по протоколу TCP
a) LISTEN
b) SYN-SENT
c) WAIT
d) **LAST-ACK**

1. Выделяют … уровень стека протоколов TCP/IP
а) физический
б) канальный
в) **сетевой (internet)**
г) сеансовый

2. Наиболее частый случай нарушения безопасности информационной системы – …
а) атаки извне
б) обиженные сотрудники
в) ошибки персонала
г) компьютерные вирусы

3. Авторизация – это процедура предоставления субъекту …
а) определенных полномочий и ресурсов в данной системе
б) определенного идентификатора
в) определенной ключевой пары

4. Аутентификация – это процедура проверки ...
а) подлинности заявленного пользователя, процесса или устройства
б) пользователя по его идентификатору
в) пользователя по его имен

5. Неверно, что к протоколу IP относится такая функция, как …
а) фрагментация

б) маршрутизация
в) достоверность передачи

6. Средства телекоммуникации – это …

а) совокупность средств связи, обеспечивающих передачу данных между ЭВМ и информационными системами, удаленными друг от друга на значительные расстояния;

б) комплекс технических средств передачи информации

в) проводное, оптико-волоконное и беспроводное соединение объектов

7. Неверно, что добавляется IP-заголовок к пакету протокола … из стека TCP/IP

а) ICMP
б) DHCP
в) ARP

8. К средствам технической защиты информации относятся ...

а) аппаратные и программные средства защиты

б) технические средства, предназначенные для предотвращения утечки информации по одному или нескольким техническим каналам

в) межсетевые экраны

9. Неверно, что … является состоянием соединения по протоколу TCP

а) LISTEN
б) SYN-SENT
в) WAIT
г) LAST-ACK

10. Службой TELNET обычно используется порт № …

а) 20
б) 21
в) 22
г) 23

21. Операционная система цифровой вычислительной системы предназначена для обеспечения …

d. **определенного уровня эффективности цифровой вычислительной системы за счет автоматизированного управления ее работой и предоставляемого пользователям набора услуг**
e. удобной работы пользователя
f. совмещения различных интерфейсов

22. Современную организацию ЭВМ предложил …

d. Норберт Винер
e. Джон фон Нейман
f. Чарльз Беббидж

23. В системное программное обеспечение входят …
f. языки программирования
g. операционные системы
h. графические редакторы
i. компьютерные игры
j. текстовые редакторы

24. Анализ рисков включает в себя …
e. набор адекватных контрмер, осуществляемый в ходе управления рисками
f. анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС в случае осуществления угрозы безопасности
g. выявление существующих рисков и оценку их величины
h. мероприятия по обследованию безопасности ИС с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите

25. Информация – это …
i. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
j. совокупность знаний, накопленная человечеством
k. совокупность принципов, методов и форм управления
l. совокупность рефлексий между идеей и материей на макро- и микроуровнях

26. Информационная сфера – это …
f. совокупность всех накопленных факторов в информационной деятельности людей
g. сфера деятельности человеко-машинного комплекса в процессе производства информации
h. **совокупность информации и субъектов, осуществляющих сбор, формирование, распространение и использование информации**
i. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
j. сфера, в которой производится и распространяется информация

27. Неверно, что … относят к источникам угроз информационной безопасности
k. человеческий фактор
l. правовые аспекты функционирования ИС
m. стихийные бедствия

n. аппаратные сбои
o. ошибки проектирования и разработки ИС

28. Система защиты информации – это …
a. комплексная совокупность программно-технических средств, обеспечивающих защиту информации
b. совокупность органов и/или исполнителей, а также используемая ими техника защиты информации
c. область информационных технологий
d. разработка стратегии защиты бизнеса компаний

29. Пользователь (потребитель) информации – это …
k. фирма – разработчик программного продукта, которая занимается ее дистрибьюцией
l. пользователь, использующий совокупность программно-технических средств
m. субъект, пользующийся информацией в соответствии с регламентом доступа
n. владелец фирмы или предприятия
o. все служащие предприятия

30. Право доступа к информации – это …
a. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
b. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
c. возможность доступа к информации, не нарушающая установленные правила разграничения доступа
d. нарушение установленных правил разграничения доступа
e. лицо или процесс, осуществляющие несанкционированного доступа к информации

Вопросы к экзамену (3 семестр)

1. Понятие об архитектуре аппаратных средств
2. Классификация программных средств.
3. Принципы работы вычислительной системы
4. Классификация операционных систем
5. Угрозы безопасности информации в информационно-вычислительных системах
6. Структуризация методов обеспечения информационной безопасности.
7. Требования профиля защиты
8. Защита геопространственных баз данных
9. Защита клиентской части информационных систем
10. Виды шифрования пространственной информации
11. Стенография

12. Использование технологии цепочки блоков для защиты геопространственных данных

Тесты к экзамену (3 семестр)

31. Санкционированный доступ к информации – это …

f. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
g. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
h. доступ к информации, не нарушающий установленные правила разграничения доступа
i. нарушение установленных правил разграничения доступа
j. лицо или процесс, осуществляющие несанкционированного доступа к информации

32. Несанкционированный доступ к информации – это …

f. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
g. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
h. доступ к информации, не нарушающий установленные правила разграничения доступа, которые служат для регламентации права доступа к компонентам системы
i. **нарушение установленных правил разграничения доступа**
j. лицо или процесс, осуществляющие несанкционированный доступ к информации

33. Идентификация субъекта – это …

f. процедура распознавания субъекта по его идентификатору
g. проверка подлинности субъекта с данным идентификатором
h. установление того, является ли субъект именно тем, кем он себя объявил
i. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
j. установление лиц или процессов, осуществляющих несанкционированный доступ к информации

34. Аутентификация субъекта – это …

f. процедура распознавания субъекта по его идентификатору
g. проверка подлинности субъекта с данным идентификатором
h. установление того, является ли субъект именно тем, кем он себя объявил
i. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
j. установление лиц или процессов, осуществляющих несанкционированный доступ к информации

35. Авторизация субъекта – это …
f. процедура распознавания субъекта по его идентификатору
g. проверка подлинности субъекта с данным идентификатором
h. установление того, является ли субъект именно тем, кем он себя объявил
i. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
j. установление лиц или процессов, осуществляющих несанкционированный доступ к информации

36. Неверно, что … должны быть доступны в нормальной работе пользователя
e. системные утилиты и системные редакторы
f. средства защиты, системные утилиты
g. средства разработки, утилиты
h. средства защиты

37. По существующим правилам разрабатывать, производить защиты информации может только предприятие, имеющее …
e. лицензию
f. сертификат
g. начальный капитал
h. аккредитацию

38. В стандартной политике безопасности установка программных продуктов непосредственно пользователем корпоративной рабочей станции …
e. разрешена
f. разрешена, за исключением компьютерных игр
g. разрешена, но только с устного согласия сотрудника ИТ-отдела
h. запрещена

39. Под доступностью информации понимается …
a. возможность за приемлемое время получить требуемую информационную услугу
b. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
c. защита от несанкционированного доступа к информации

40. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) …
e. влечет во всех случаях уголовную ответственность
f. влечет только наложение административного штрафа
g. не влечет за собой уголовной ответственности

h. влечет уголовную ответственность и наложение административного штрафа

7.4. Содержание занятий семинарского типа.

Типовые практические задания

ПРАКТИЧЕСКАЯ РАБОТА № 1

Вид практического занятия: Практическая работа.
Тема и содержание занятия: Оценка уязвимостей активов
Цель занятия:
1.Ознакомиться с основными уязвимостями информационных активов.
2. Изучить методы деления информации по уязвимостям
3. Освоить методику и приобрести исследовательские навыки по оценке уязвимостей информационных активов.
Практические навыки:

В данном пункте необходимо провести идентификацию уязвимостей окружающей среды, организации, процедур, персонала, менеджмента, администрации, аппаратных средств, программного обеспечения или аппаратуры связи, которые могли бы быть использованы источником угроз для нанесения ущерба активам и деловой деятельности организации, осуществляемой с их использованием.

Оценка должна проводиться для активов, определенных в п.п. (e) п.1.2.1.

При проведении оценки рекомендуется руководствоваться требованиями стандарта ГОСТ Р ИСО/МЭК ТО 13335-3-2007 (Приложение D).

Пункт должен содержать:

а) Описание процедуры оценки уязвимости активов, при этом должно быть отражено, что является основанием для проведения такой оценки, как часто проводится оценка, кто проводит оценку, какие при этом используются методики, в какой форме представляются результаты оценки.

б) Перечень уязвимостей с указанием оценки степени вероятности возможной реализации отмеченных уязвимостей, например "высокая", "средняя" или "низкая", сведенный в таблицу 5

Следует обратить внимание на то что, в указанной таблице уязвимости сгруппированы по областям существования/возникновения. Один и тот же информационный актив может присутствовать в нескольких разделах таблицы. Иными словами, один и тот же информационный актив может иметь несколько уязвимостей.

Таблица 5

Результаты оценки уязвимости активов

Группа уязвимостей Содержание уязвимости	Актив №1	Актив №2	Актив №3	Актив №4	Актив №5	Актив №6	Актив №7
1. Среда и инфраструктура							
Уязвимость 1.1.	**низкая**						
…		**высокая**					
Уязвимость 1.n							
2. Аппаратное обеспечение							
Уязвимость 2.1.							
…							
Уязвимость 2.n					**средняя**		
3. Программное обеспечение							
Уязвимость 3.1.							
…							
Уязвимость 3.n							
4. Коммуникации							
Уязвимость 4.1.							
…							
Уязвимость 4.n							
5. Документы (документооборот)							
Уязвимость 5.1.							
…							
Уязвимость 5.n							
6.Персонал							
Уязвимость 6.1.							
…							
Уязвимость 6.n							
7. Общие уязвимые места							
Уязвимость 7.1.							
…							
Уязвимость 7.n							

ПРАКТИЧЕСКАЯ РАБОТА № 2

Вид практического занятия: Практическая работа.
Тема и содержание занятия: Оценка угроз активам.
Цель занятия:
1.Получить навыки оценки угроз информационным активам
Практические навыки:

Перед началом выполнения данного пункта необходимо уяснить, что **угроза – это** потенциальная причина инцидента, который может нанести ущерб системе или организации, а инцидент, (**инцидент информационной безопасности)** – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность организации или информационную безопасность.

В основе угроз может лежать как природный, так и человеческий фактор; они могут реализовываться случайно или преднамеренно.

В ходе выполнения пункта источники как случайных, так и преднамеренных угроз должны быть идентифицированы, а вероятность их реализации - оценена.

Следует учесть, что, с одной стороны, важно не упустить из виду ни одной возможной угрозы, так как в результате возможно нарушение функционирования или появление уязвимостей системы обеспечения безопасности информационных технологий, а с другой не акцентировать внимание на заведомо маловероятных угрозах.

Исходные данные для оценки угроз следует получать от владельцев или пользователей активов, служащих отделов кадров, специалистов по разработке оборудования и информационным технологиям, а также лиц, отвечающих за реализацию защитных мер в организации.

При формировании перечня угроз рекомендуется руководствоваться требованиями стандарта ГОСТ Р ИСО/МЭК ТО 13335-3-2007 (Приложение С).

Также полезно использование каталогов угроз (наиболее соответствующих нуждам конкретной организации или виду ее деловой деятельности).

После идентификации источника угроз (кто и что является причиной угрозы) и объекта угрозы (какой из элементов системы может подвергнуться воздействию угрозы) необходимо оценить вероятность реализации угрозы. При этом следует учитывать:

- частоту появления угрозы (как часто она может возникать согласно статистическим, опытным и другим данным), если имеются соответствующие статистические и другие материалы;

- мотивацию, возможности и ресурсы, необходимые потенциальному нарушителю и, возможно, имеющиеся в его распоряжении; степень привлекательности и уязвимости активов

системы информационных технологий с точки зрения возможного нарушителя и источника умышленной угрозы;

- географические факторы - такие как наличие поблизости химических или нефтеперерабатывающих предприятий, возможность возникновения экстремальных погодных условий, а также факторов, которые могут вызвать ошибки у персонала, выход из строя оборудования и послужить причиной реализации случайной угрозы.

После завершения оценки угроз составляют перечень идентифицированных угроз, активов или групп активов, подверженных этим угрозам, а также определяют степень вероятности реализации угроз с разбивкой на группы высокой, средней и низкой вероятности.

Пункт должен содержать:

а) описание процедуры оценки угроз активам, при этом должно быть отражено, что является основанием для проведения такой оценки, как часто проводится оценка, кто проводит оценку, какие при этом используются методики, в какой форме представляются результаты оценки.

Таблица 6

Результаты оценки угроз активам

Группа угроз Содержание угроз	Актив №1	Актив №2	Актив №3	Актив №
1. Угрозы, обусловленные преднамеренными действиями				
Угроза 1.1.	**средняя**			
…		**высокая**		
Угроза 1.n				
2. Угрозы, обусловленные случайными действиями				
Угроза 2.1.				
…				
Угроза 2.n				
3. Угрозы, обусловленные естественными причинами (природные, техно				
Угроза 3.1.				
…				
Угроза 3.n				

ПРАКТИЧЕСКАЯ РАБОТА № 3

Вид практического занятия Практическая работа.

Тема и содержание: Оценка существующих и планируемых средств защиты

Цель занятия:

1. Получить навыки оценки существующих и планируемых средств защиты

Практические навыки:

Для защиты информации, составляющей коммерческую тайну, её владелец создает собственную систему защиты информации. Законодательно структура такой системы не закреплена.

Задачи по защите информации, в зависимости от возможностей и масштабов организации, может выполнять как профильное структурное подразделение, входящее в штатную структуру предприятия (для крупных компаний), так и сотрудники, уполномоченные руководством для проведения мероприятий по защите информации параллельно с выполнением основных функциональных обязанностей.

Защита информации может осуществляться также в рамках абонентского обслуживания.

Вне зависимости от того, на кого возложены организация и выполнение мероприятий по защите информационных активов, **данный пункт должен содержать:**

а) данные о подразделении (должностных лицах), на которых возложены задачи по защите информации: организационную структуру подразделения и функционал. Информация должна детализировать данные по п.1.1.1. с точки зрения обеспечения информационной безопасности..

б) техническую архитектуру – состав и взаимодействие аппаратных средств, используемых (даже частично) для обработки информационных активов, подлежащих защите. Схему (Рис.2) и таблицу описания технических характеристик;

в) программную архитектуру – программное обеспечение, используемое (даже частично) для обработки информационных ресурсов, подлежащих защите Схему (Рис.3) и таблицу описания технических характеристик;

г) описание как минимум одной из подсистем инженерно-технических средств защиты информации: системы видеонаблюдения, системы контроля и управления доступом, системы периметровой охраны, внедрение и/или модернизация которой предусмотрено темой дипломного проекта. Схемы (Рис.4-7) и таблицу описания технических характеристик.

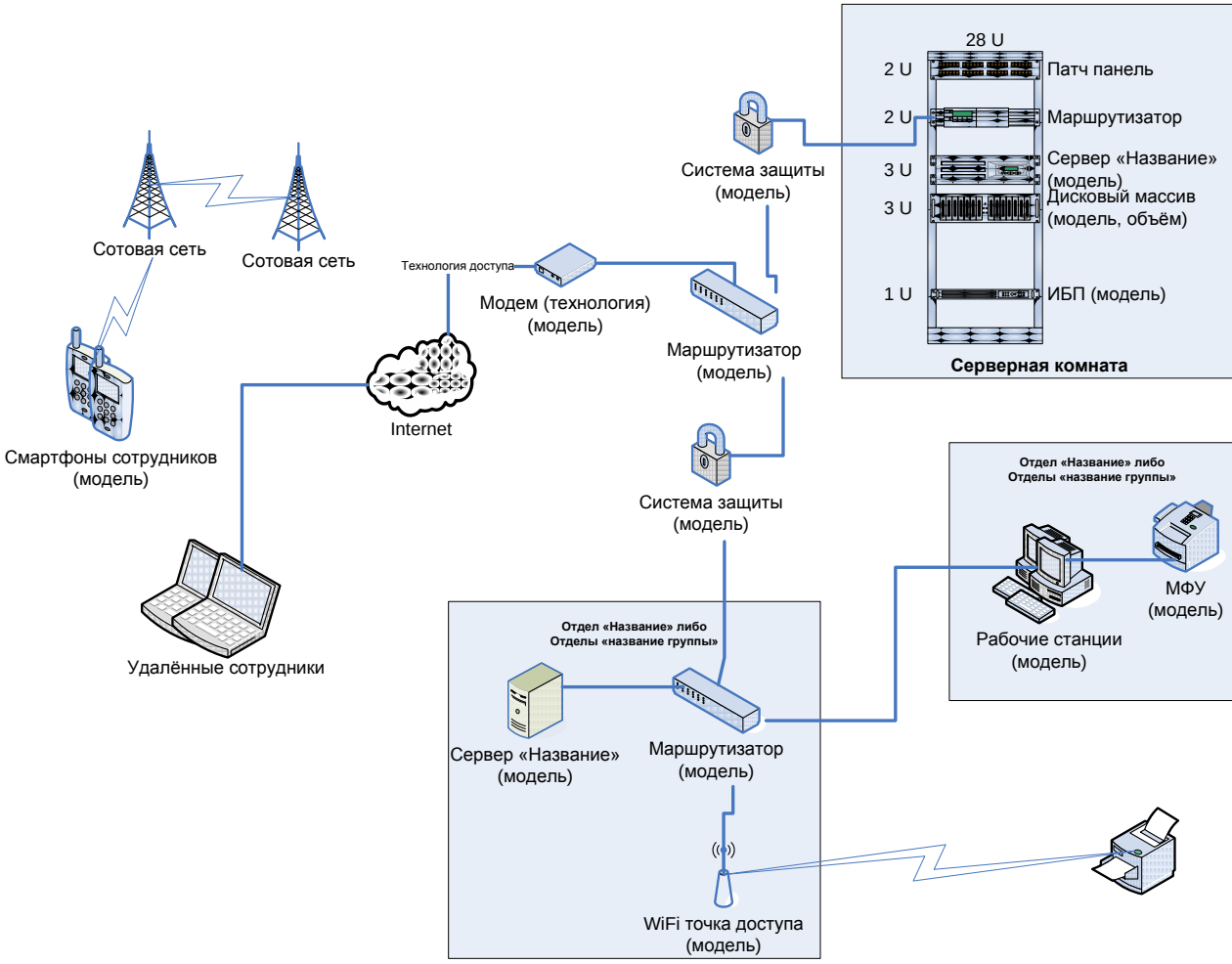

Рис.2. Пример технической архитектуры предприятия

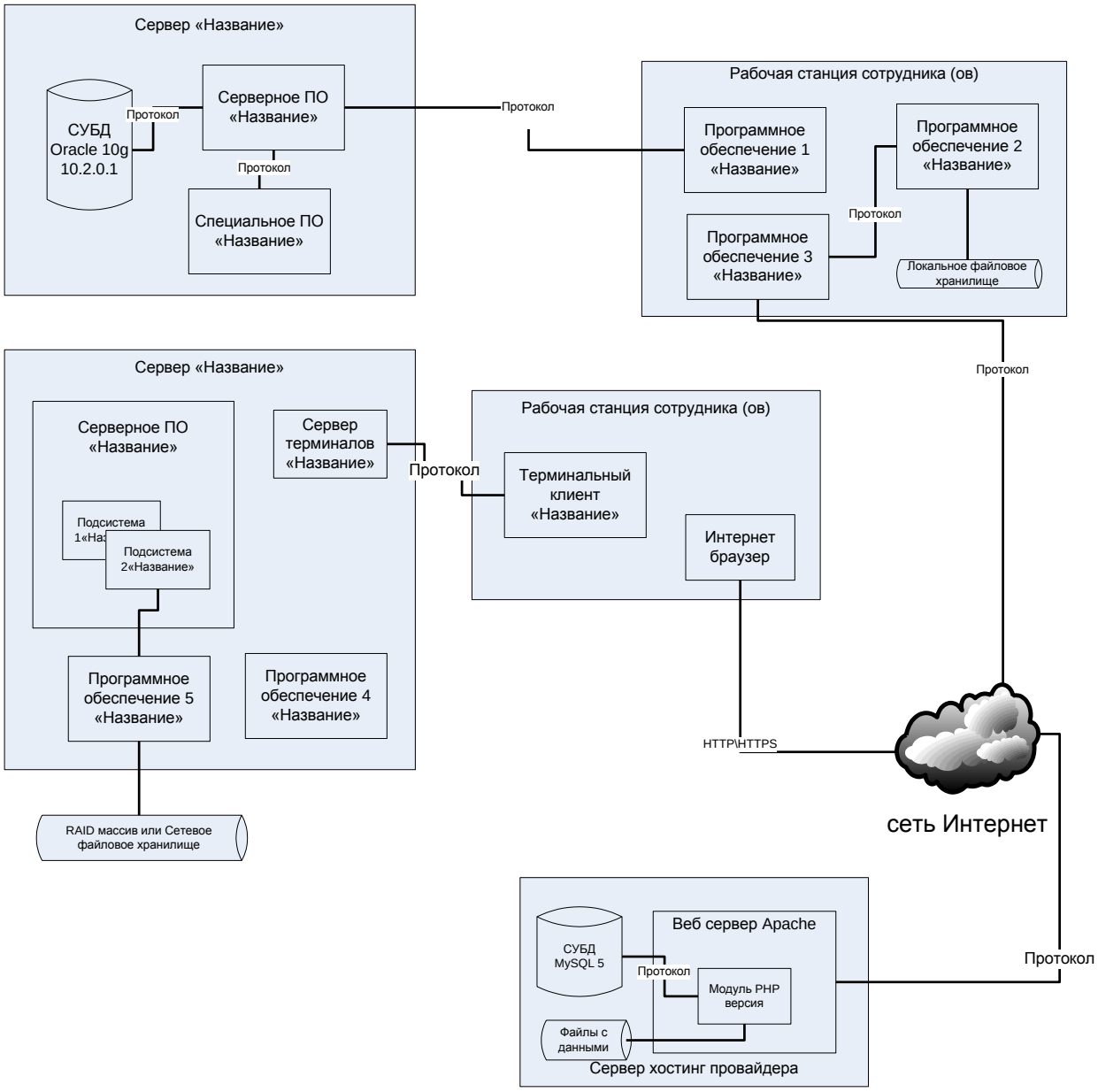

Рис.3. Пример программной архитектуры предприятия

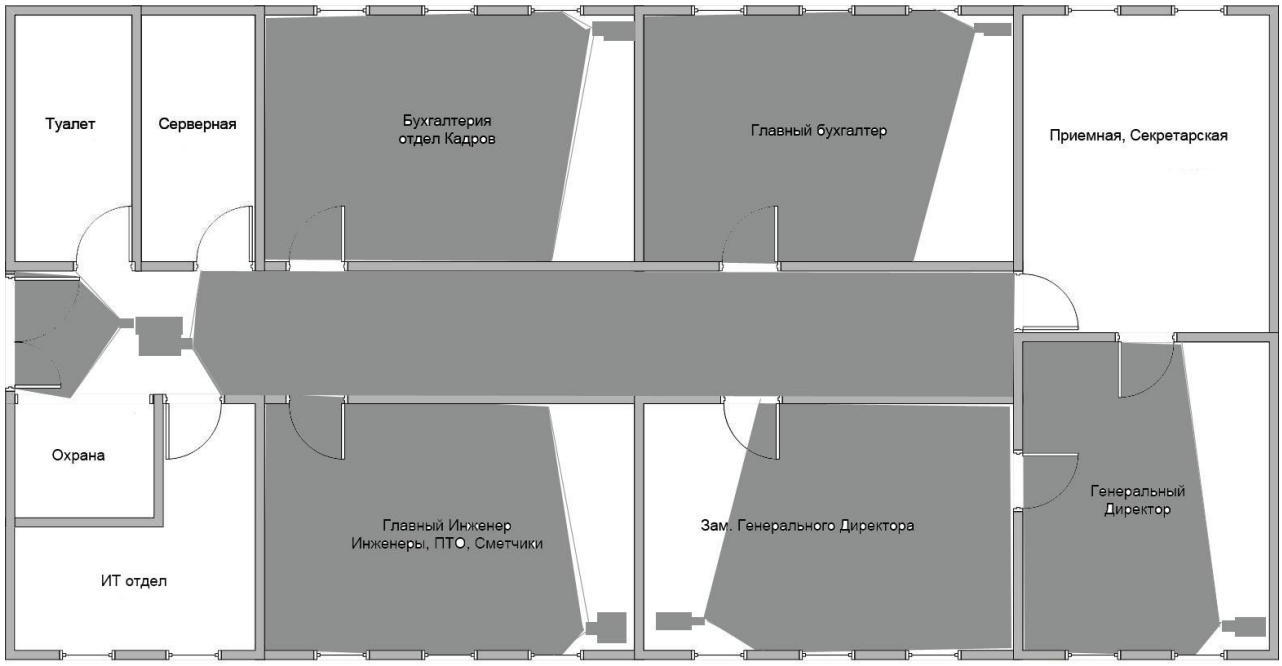

Рис.4. Расположение камер охранного видеонаблюдения.

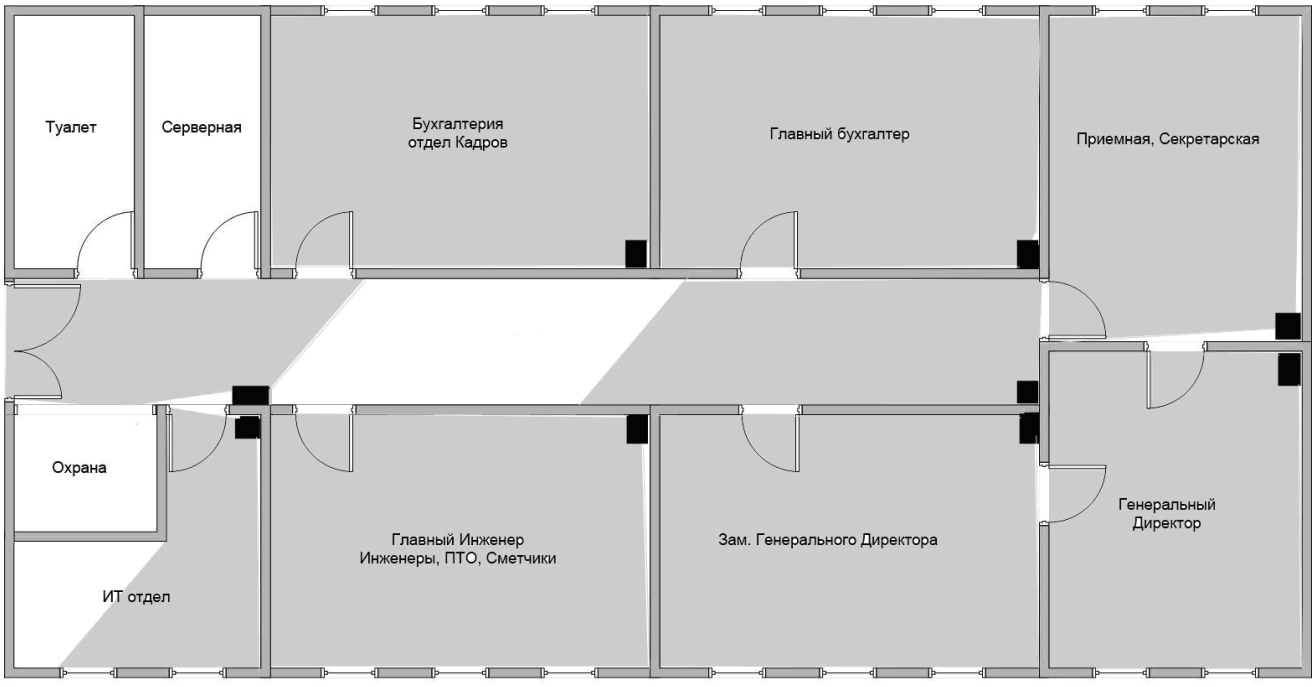

Рис.5. Расположение датчиков движения

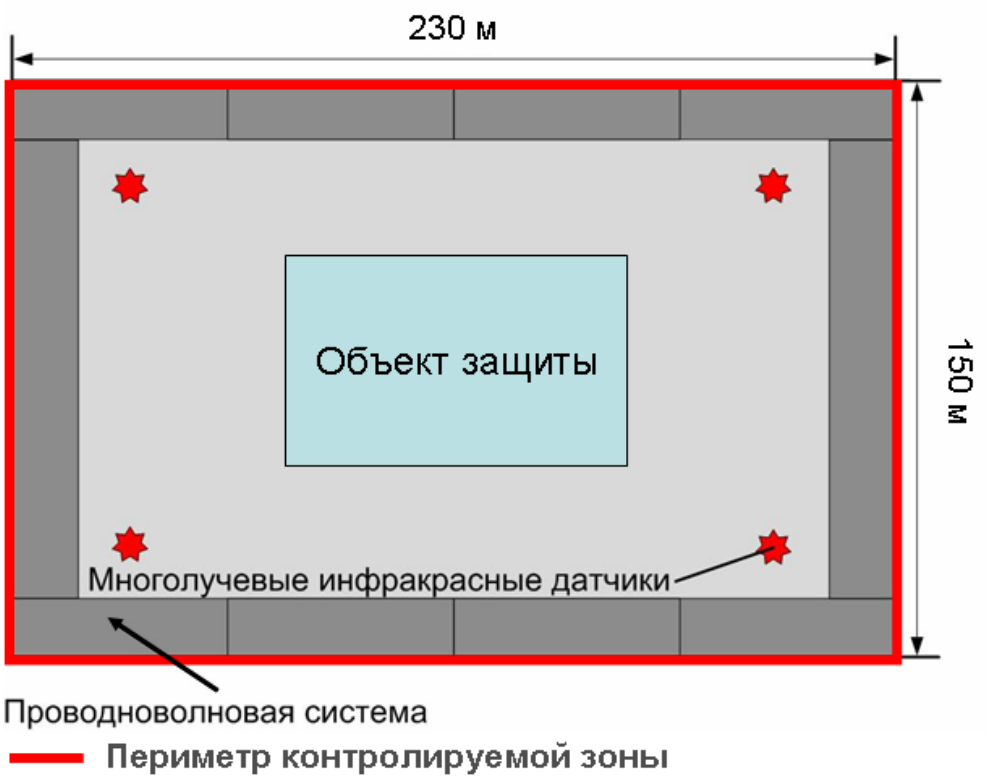

Рис. 6. Расположение систем контроля периметра (вариант 1)

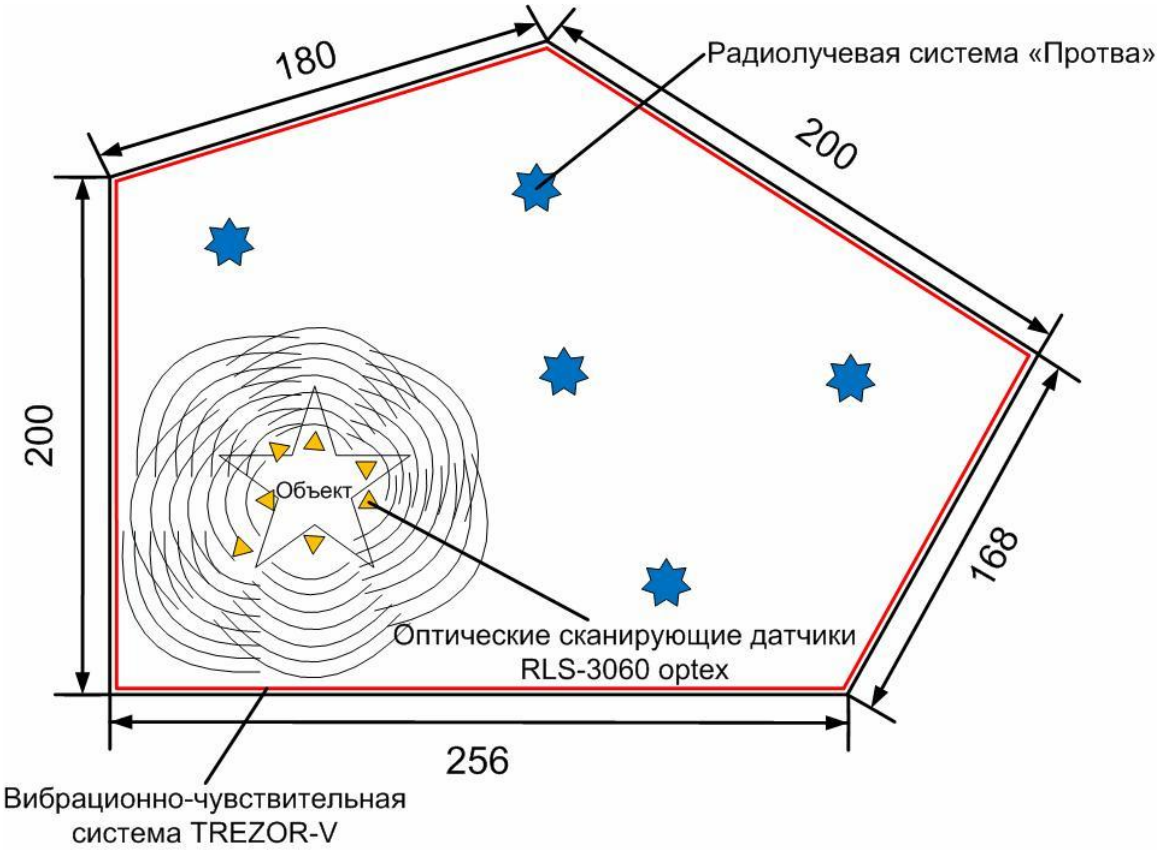

Рис. 7 Расположение систем контроля периметра (вариант 2)

г) результаты оценки действующей системы безопасности информации, отражающие, насколько полно выполняются однотипные объективные функции при решении задач обеспечения защиты информации. Если некоторые задачи решаются не в полном объеме, следует указать, как предусмотренные мероприятия выполняются в действительности. Результаты обследования внести в Таблицу 7.

Таблица 7

Анализ выполнения основных задач
по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	**Степень выполнения**
обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной;	
организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;	
организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;	
предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;	
выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;	
обеспечение режима безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне;	
обеспечение охраны территории, зданий помещений, с защищаемой информацией.	

ПРАКТИЧЕСКАЯ РАБОТА № 4

Вид практического занятия: Практическая работа.
Тема и содержание: Оценка рисков
Цель занятия:
1. Ознакомиться с методами оценки рисков
Практические навыки:

На заключительном этапе анализа риска должна быть проведена суммарная оценка риска. Активы, имеющие ценность и характеризующиеся определенной степенью уязвимости, всякий раз подвергаются риску в присутствии угроз.

Оценка риска представляет собой оценку соотношения потенциальных негативных воздействий на деловую деятельность в случае нежелательных инцидентов и уровня оцененных угроз и уязвимых мест. Риск фактически является мерой незащищенности системы и связанной с ней организации. Величина риска зависит от:

- ценности активов;

- угроз и связанной с ними вероятности возникновения опасного для активов события;
- легкости реализации угроз в уязвимых местах с оказанием нежелательного воздействия;
- существующих или планируемых средств защиты, снижающих степень уязвимости, угроз и нежелательных воздействий.

Задача анализа риска состоит в определении и оценке рисков, которым подвергается система информационных технологий и ее активы, с целью определения и выбора целесообразных и обоснованных средств обеспечения безопасности. При оценке рисков рассматривают несколько различных его аспектов, включая воздействие опасного события и его вероятность.

Многие методы предлагают использование таблиц и различных комбинаций субъективных и эмпирических мер. В настоящее время нельзя говорить о правильном или неправильном методе анализа риска. Важно, чтобы организация пользовалась наиболее удобным и внушающим доверие методом, приносящим воспроизводимые результаты. Ниже приведены несколько примеров методов, основанных на применении таблиц:

Пример 1

Суть подхода заключается в определении наиболее критичных активов в организации с точки зрения рисков ИБ по «штрафным баллам». Оценивание рисков производится экспертным путем на основе анализа ценности активов, возможности реализации угроз и использования уязвимостей, определенных в предыдущих пунктах. Для оценивания предлагается, например, таблица с заранее предопределенными «штрафными баллами» для каждой комбинации ценности активов, уровня угроз и уязвимостей (табл. 8).

Таблица 8

	Уровни угрозы	Низкая			Средняя			Высокая		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Ценность активов	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

В случае определения уровня уязвимости из результатов аудита или самооценки для различных процессов и при наличии экспертных оценок уровня соответствующих угроз и ценности активов можно получить меру риска ИБ для каждого процесса.

Однако такой подход не приводит к интерпретации результатов аудита или самооценки ИБ, ориентированной на бизнес, на бизнес-процессы.

Если оставить за границей анализа угрозы, слабо поддающиеся управлению со стороны системы обеспечения ИБ, и оценить риски по степени влияния уязвимостей на бизнес-процессы, то можно получить оценки рисков бизнес-процессов на основе оцененного профиля процессов.

Пример 2

Для такого оценивания может быть применена таблица, (Таблица 9)в которой строками являются уровни степени влияния уязвимости на бизнес-процессы , столбцами — уровни уязвимостей.

Таблица 9

Уровень уязвимости / Степень влияния уязвимости на бизнес-процессы	Высокий	Средний	Малый	Очень малый
Высокая	64	32	16	8
Средняя	32	16	8	4
Малая	16	8	4	2
Очень малая	8	4	2	1

То есть уровень уязвимости бизнес-процесса показывает (отображает) степень влияния на конкретный бизнес-процесс организации уязвимости, а уровень уязвимости отражает величину отклонения оцененного профиля от рекомендованного (целевого профиля).

Таким образом, столбец в таблице 9 есть характеристика бизнеса, а строка — характеристика уязвимости. Чем больше оцененный профиль отличается от рекомендованного, тем больше величина (уровень) уязвимости.

Предопределенные «штрафные баллы» меры риска бизнес-процессов могут отражать историю инцидентов, связанных с бизнес-процессами, и их последствия, если таковая история имеется. С другой стороны, баллы могут быть внесены в таблицу экспертным способом.

Далее для оценки рисков каждый реализуемый в организации бизнес-процесс рассматривается экспертами и относится ими к одному из 4 классов (столбец табл. 9). Фактически при этом оценивается степень влияния ИБ на каждый конкретный бизнес-процесс.

Понятно, что если процесс имеет сильную стохастическую составляющую, связанную с его природой (например, невозврат кредита, курс валют и т.д.), то влияние ИБ на этот процесс существенно меньше, чем на детерминированный процесс, в котором потери в основном возникают при фальсификации и манипулировании информацией.

Каждый бизнес-процесс может классифицироваться в целом по профилю либо по каждому показателю профиля. (Профиль – наименование совокупности информационного актива, уязвимости, угроз, состояния средств защиты информации). В последнем случае будет получена более точная оценка. Если бизнес-процессы классифицированы экспертами по каждому показателю профиля, то он получает пару координат в таблице 9 и для него может быть определено количество «штрафных баллов» путем их выборки из таблицы и суммирования.

Если бизнес-процессы классифицированы в целом по профилю, то нет необходимости рассматривать далее каждый показатель профиля в отдельности — достаточно взять разницу между значением рекомендованного профиля и средним значением оцененного профиля. По ее величине будет выбран один из столбцов таблицы 9, каждому бизнес-процессу будет присвоен «штрафной балл» из соответствующей для него степени влияния этого столбца. Далее «штрафные баллы» всех бизнес-процессов организации суммируются и получается интегральная оценка в «штрафных баллах» для организации.

После этого вычисляются значения двух характеристических точек для бизнес-процессов организации на оси «штрафных баллов».

Первая характеристическая точка отображает состояние, когда оцененный профиль совпадает с рекомендованным, т.е. соответствует столбцу «очень малый» таблицы 10. При этом окажется, что даже при полной реализации рекомендованного профиля будет ненулевое количество «штрафных баллов». Эта величина отображает остаточный риск, и он будет тем больше, чем больше бизнес-процессов отнесено к высокому уровню зависимости от ИБ.

Вторая характеристическая точка определяется при условии максимального отклонения оцененного и рекомендованного профиля, то есть для ее подсчета используется столбец «высокий» таблицы 9.

Как размещаются эти точки на оси «штрафных баллов», показано на рисунке 8. Как видно из рисунка , на оси образовалось три интервала:

- [0; 1-я характеристическая точка];
- [1-я характеристическая точка; интегральная оценка];
- [интегральная оценка; 2-я характеристическая точка].

Кроме того, представляют также интерес интервалы [0; интегральная оценка] и [0; 2-я характеристическая точка].

Суждение о величине риска ИБ для организации выносится на основе сопоставления длин указанных интервалов. Они же используются и для прогноза состояния информационной безопасности, которое изменяется вследствие изменчивости структуры активов и бизнес-процессов организации и ее деятельности по совершенствованию защитных мер, что приводит к изменению указанных точек на оси «штрафных баллов».

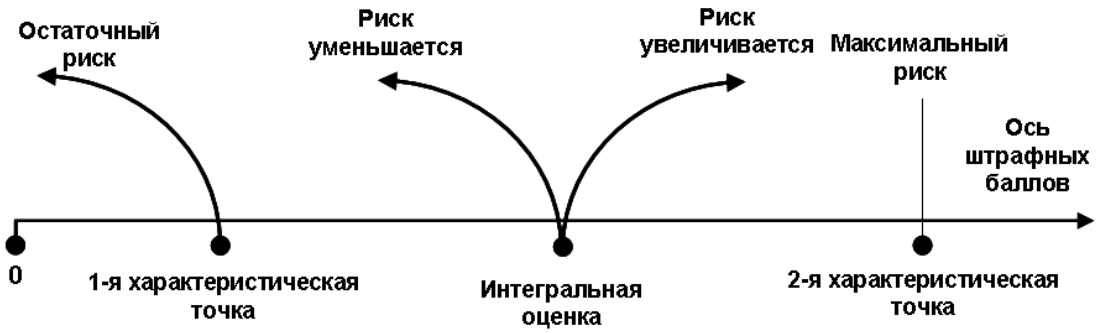

Рис. 8. Размещение характеристических точек на оси штрафных баллов

На рисунке 9 представлена взаимосвязь основных понятий информационной безопасности: «владелец», «актив», «угроза», «уязвимость» и, наконец «риск». Именно величина риска является тем интегрированным показателем, который позволяет владельцу актива принять адекватное решение для определению перечня мер по уменьшению уязвимостей активов.

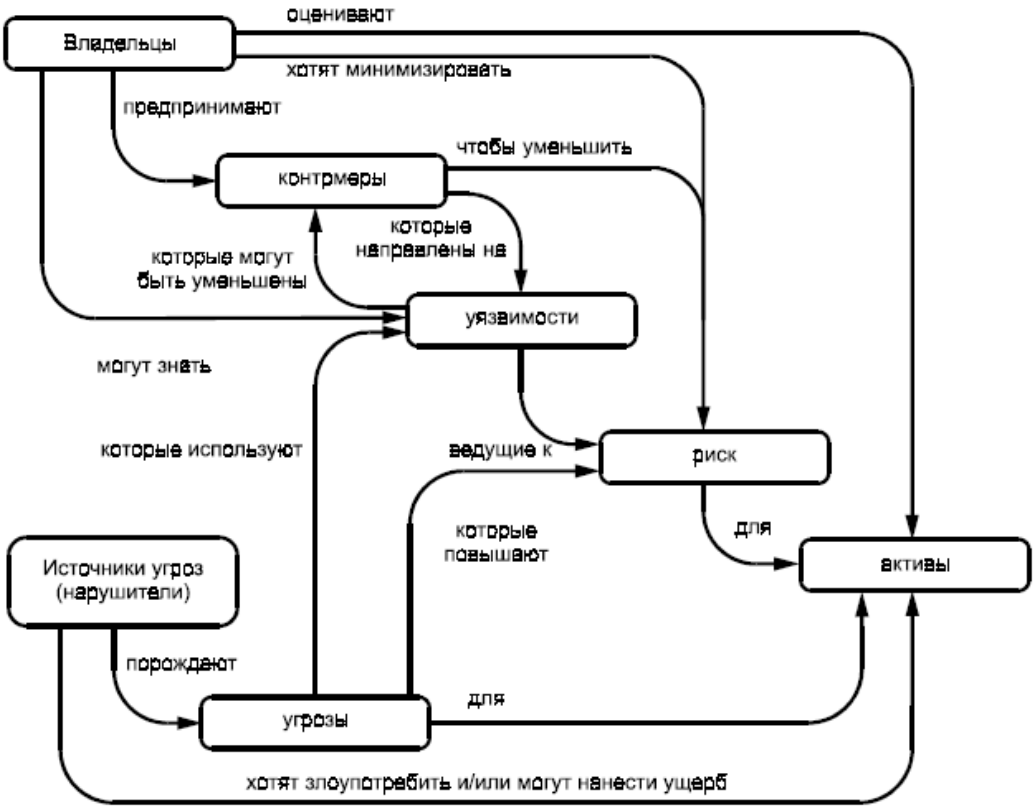

Рис.9. Основные понятия информационной безопасности и их взаимосвязь

Данный пункт должен включать

а) обоснование выбора методики оценки риска;

б) описание проведения процедуры оценки рисков, с указанием:

- должностных лиц, участвующих в оценке;
- способов (форм) представления исходной информации;
- способов (форм) представления результатов оценки рисков

в) результаты проведения оценки риска, проведенные с учетом ценности информационных активов (п.1.2.1.), наличия уязвимостей (п.1.2.2.), степени угроз (п.1.2.3) и состояния действующей в организации системы защиты информации (п.1.2.4.).

г) определить (при наличии) приемлемые риски, обосновать данное решение.

Результаты проведения оценки целесообразно свести в таблицу, которая должна содержать риски наиболее ценным информационным активам, ранжированные в порядке убывания.

Таблица 10

Результаты оценки рисков информационным активам организации

Риск	Актив	Ранг риска

Следует обратить особое внимание на то, что именно результаты оценки рисков являются основанием для:

- выбора и формулировки задач по обеспечению информационной безопасности предприятия (п.1.3.);
- выбора защитных мер (п.1.4.);

Ситуационные задачи к зачеьу за 2 семестр

Задание 1.

Провести анализ сервера аутентификации Kerberos и ответить на следующие вопросы:

1. От чего защищает и от чего не защищает Kerberos.
2. Возможности Kerberos.
3. Форматы данных в системе Kerberos.
4. Типы пересылаемых сообщений.

- Обмен с сервером начальной аутентификации
- Обмен с сервером выдачи билетов
- Аутентификационный обмен клиент/сервер
- Защищенные сообщения
- Конфиденциальные сообщения
- Пересылка удостоверений

5. База данных Kerberos

Задание 2.

Провести анализ операционной системы Windows Server 2016 и ответить на следующие вопросы:

1. Опишите основные Механизмы повышения безопасности ОС Windows Server 2016 – мастер настройки безопасности (Security Configuration Wizard, SCW) и групповую политику Active Directory.
2. Опишите параметры шаблонов безопасности и дополнительные меры для политик уровня домена в трех средах
3. Опишите базовую политику для используемых серверов (MSBP) для серверных ролей,
4. Опишите роль файлового сервера для повышения безопасности компьютеров.

5. Опишите роль сервера печати (как повысить безопасность сервера печати под управлением Windows Server 2016.
6. Опишите роль веб-сервера. Почему для обеспечения всесторонней безопасности веб-узлов и приложений требуется защитить весь сервер IIS (в том числе каждый веб-узел и приложение, которое находится на сервере IIS) от клиентских компьютеров в среде.
7. Опишите роль сервера IAS (серверы проверки подлинности в Интернете (Internet Authentication Server, IAS))
8. Опишите роль сервера для служб сертификации
9. Опишите роль граничного сервера

Задание 3.

Провести анализ операционной системы LINUX и ответить на следующие вопросы:

1. Что представляет собой ОС Linux и ASPLinux в частности. Назовите основные характеристики и отличительные особенности от исследуемых Вами ранее операционных систем.
2. Как и чем обеспечивается безопасность в ОС Linux, перечислите основные механизмы и средства обеспечения безопасности ОС Linux.
3. Как осуществляется управление учетными записями пользователей и управление учетными записями групп в ОС Linux.
4. Как осуществляются идентификация и аутентификация пользователей в ОС Linux.
5. Как осуществляется регистрация событий доступа к объектам файловой системы ОС Linux.
6. Что представляет собой резервное копирование ОС Linux, перечислите методы хранения избыточных копий данных в ОС Linux.
7. Что представляет собой защищенная оболочка SSH ОС Linux.

Задание 4.

Выбрать операционную систему отвечающую интересам компании.
(ОБОСНУЙТЕ)

Осуществить подбор программного обеспечения вычислительных систем.
общее (системное) программное обеспечение (ОПО);
специальное программное обеспечение (СПО).
(ОБОСНУЙТЕ)

Осуществить подбор прикладных программ общего назначения, обслуживающие (сервисные) программы (утилиты)
программы-упаковщики (архиваторы);
антивирусные программы;
программы резервирования;
программы диагностики компьютера;
программы оптимизации дисков;
программы динамического сжатия дисков.
(ОБОСНУЙТЕ)

Осуществить подбор инструментальных программных средств.
компиляторы и интерпретаторы;
автономные отладчики (дебагеры, от англ. Debug «удаление насекомых»);

интегрированные оболочки;
средства создания приложений типа клиент-сервер и т. п.
(ОБОСНУЙТЕ)

Разработать ПОЛИТИКУ БЕЗОПАСНОСТИ компании исходя из выбранных Вами операционной системы и программно-аппаратных средств

Представить модель политики безопасности компании.

Представить форму технико-экономического обоснования создания и развития безопасности информационной системы, а также плана проведения мероприятий.

Варианты компаний:

1. Компания имеет 5 представительств, все пять в разных странах. Имеет 5 представительств в каждом от 50-100 чел. Головная компания 1000 чел в России. Отдел продаж в региональное представительство, административный отдел и отдел обработки данных. Направление деятельности компании - транснациональные грузовые перевозки.
2. Компания имеет одно представительство в России, которое является компанией, купленной годом ранее, занимающееся разработкой ПО. Головная компания до 500 чел. Представительство - до 300 чел. (Разные бренды). 2 домена – 2 бренда
3. Компания имеет головной офис со штатом 300 чел. Занимается продажей сотовых телефонов. По всей России 2000-3000 представительств – магазинах, есть упр. Менеджер (локальный отд. продаж) и тарифный отдел и отд. логистики.
4. Компания – 100 чел. Сфера деятельности аутсорсинг, услуги администрирования. Клиенты в большинстве стран мира. Компания обеспечивает полную поддержку инфраструктуры клиента.
5. Компания состоит из 3-х филиалов на территории РФ. ЦО в Москве. Численность ЦО 100 чел., в филиалах 20 чел. Занимается производством и разработкой средств аутентификации. Производство в филиалах, ЦО выполняет только административные действия.
6. Компания - холдинг с центральным офисом в г. Москве. Занимается созданием и разработкой интернет сайтов и в неё входит ещё 4 компании, находящиеся в 4 странах мира. В каждой компании до 50 человек.

Ситуационные задачи к экзамену за 3 семестр

1. Приведите наиболее популярные в России антивирусные программы и их классификацию. Сделайте сравнительный анализ антивирусных продуктов, отмечая различные аспекты (оперативность, ресурсоёмкость, эффективность и т.д.).
2. Дайте характеристику и оценку следующим технологиям защиты от программ-шпионов и вирусов предлагаемых компанией Microsoft:
   - Защитник Windows (Windows Defender).
   - Windows Live Safety Center.
   - Средство удаления вредоносных программ (Malicious Software Removal Tool).
   - Windows Live OneCare.
   - Microsoft Client Protection.

! Ответы обосновать и представить по установленной форме

8. Перечень основной и дополнительной учебной литературы; перечень ресурсов информационно-телекоммуникационной сети «Интернет», перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

8.1.Основная литература

1.Информационные технологии и системы: Учеб. пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2014. - 352 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=374014

2.Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - 2-е изд. - М.: Форум: НИЦ ИНФРА-М, 2014. - 448 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=435900

3 Информационные технологии: разработка информационных моделей и систем: Учеб. пос. / А.В.Затонский - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014 Режим доступа http://znanium.com/catalog/product/400563

8.2.Дополнительная литература

1. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015 режим доступа http://znanium.com/catalog.php?bookinfo=492670

2. 2. Введение в геоинформационные системы: Учебное пособие / Блиновская Я.Ю., Задоя Д.С., - 2-е изд. - М.:Форум, НИЦ ИНФРА-М, 2021. Режим доступа https://znanium.com/catalog/document?id=375221

1. Моделирование систем и процессов: Учебное пособие / Н.Г. Чикуров. - М.: ИЦ РИОР: НИЦ Инфра-М, 2013. - 398 с. http://znanium.com/catalog.php?bookinfo=392652

2. 2. Дистанционное зондирование земли: Учебное пособие / Владимиров В., Дмитриев Д.Д., Дубровская О.А. – Красноярск: Сиб.федер.ун-т, 2014. – 196 с. Режим доступа https://znanium.com/catalog/document?id=119753

3.Формирование современной международно-правовой концепции исследования и использования космического пространства: Монография / Капустин А.Я., Авхадеев В.Р, Головина А.А. и др. – М.: Институт законодательства и сравнительного правоведения при правительстве российской Федерации: ИНФРА-М,2021.-264 с. Режим доступа https://znanium.com/catalog/document?id=373112

4.Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е.Артемьев. – М.:ИНФРА-М., 2021. – 188 с. Режим доступа https://znanium.com/catalog/document?id=373448

5.ЛЕБЕДЕВ С.В., НЕСТЕРОВ Е.М. Пространственное ГИС-моделирование геоэкологических объектов в ARCGIS: Учебник. – СПБ:ИЗД-ВО РГПУ ИМ. А.И. ГЕРЦЕНА, 2018. – 260 С. Режим доступа HTTPS://ZNANIUM.COM/CATALOG/DOCUMENT?ID=362192

6.Геоэкология: учебное пособие / И.Ю.Григорьева. – М.: ИНФРА-М, 2021. – 270 с. https://znanium.com/catalog/document?id=365605

7.Кузнецов О.Ф. Основы геодезии и топография местности: учебное пособие –М.:Инфра-Инженерия, 2020 – 286 с. Режим доступа https://znanium.com/catalog/document?id=361688

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Microsoft Windows;
2. Microsoft Office;

3. Построение пространственных моделей территорий и объектов (РЕКОД-Модель).
4. Свободная географическая информационная система с открытым кодом QGIS 2.18
5. Геоинформационный портал ГИС-Ассоциация [информационно-справочная система]: http://www.gisa.ru/
6. Электронный атлас Москвы [информационно-справочная система]: http://atlas.mos.ru
7. Геопортал Роскосмоса [профессиональная база данных]: https://gptl.ru/
8. Сообщество специалистов в области ГИС и ДЗЗ [профессиональная база данных]: http://gis-lab.info/
9. Портал Открытых Данных Российской Федерации [профессиональная база данных]: https://data.gov.ru/
10. Геоинформационный портал Россия космическая [информационно-справочная система]: http://russpace.makd.ru/

8.4. Перечень программного обеспечения, современных профессиональных баз данных и информационных справочных системам

1. Microsoft Windows
2. Microsoft Office
3. База данных государственной статистики Федеральной службы государственной статистики
   http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/
4. База социологических данных Всероссийского центра изучения общественного мнения https://wciom.ru/database/ –
5. Справочно-правовая система Консультант + http://www.consultant.ru
6. Построение пространственных моделей территорий и объектов (РЕКОД-Модель)
7. Свободная географическая информационная система с открытым кодом QGIS 2.18

9. Методические указания для обучающихся по освоению дисциплины

Процесс изучения дисциплины предусматривает контактную работу с преподавателем (работа на лекциях и практических занятиях) и самостоятельную (самоподготовка к лекциям и практическим занятиям) работу обучающегося.

В качестве основных форм организации учебного процесса по дисциплине «Защита пространственной информации» по предлагаемой методике обучения выступают лекционные и практические занятия (с использованием интерактивных технологий обучения), а также самостоятельная работа обучающихся.

Теоретические занятия (лекции) организуются по потокам. На лекциях излагаются темы дисциплины, предусмотренные рабочей программой, акцентируется внимание на наиболее принципиальных и сложных вопросах дисциплины, устанавливаются вопросы для самостоятельной проработки. При проведении лекций планируется использование интерактивных форм изложения материала в виде проблемных лекций с использованием мультимедийных технологий в виде презентаций. Конспект лекций является базой при подготовке к практическим занятиям, к экзаменам, а также самостоятельной научной деятельности.

- *Традиционная лекция с презентацией* - подразумевает традиционное изложение учебного материала посредством акцентуации основных смысловых доминант; лекция сопровождается презентацией;

Практические занятия по дисциплине «Защита пространственной информации» проводятся в форме выполнения практических работ с целью приобретения практических навыков в решении задач по стандартизации и управлению качеством в сфере государственного муниципального управления.

Практические занятия способствуют более глубокому пониманию теоретического материала учебного курса, а также развитию, формированию и становлению различных уровней составляющих профессиональной компетентности студентов.

Целью самостоятельной (внеаудиторной) работы обучающихся является обучение навыкам работы с научно-теоретической, периодической, научно-технической литературой и технической документацией, необходимыми для углубленного изучения дисциплины «Защита пространственной информации», а также развитие у них устойчивых способностей к самостоятельному изучению и изложению полученной информации.

Основными задачами самостоятельной работы обучающихся являются:

– овладение фундаментальными знаниями;
– наработка профессиональных навыков;
– приобретение опыта творческой и исследовательской деятельности;
– развитие творческой инициативы, самостоятельности и ответственности студентов.

Самостоятельная работа студентов по дисциплине «Теоретические основы рабочих процессов объектов профессиональной деятельности» обеспечивает:

– закрепление знаний, полученных студентами в процессе лекционных и практических занятий;
– формирование навыков работы с периодической, научно-технической литературой и технической документаций;

Самостоятельная работа является обязательной для каждого обучающегося.

10. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю):

Учебные занятия по дисциплине «Защита пространственной информации» проводятся в следующих оборудованных учебных кабинетах:

Вид учебных занятий по дисциплине	Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий с перечнем основного оборудования
Занятия лекционного типа, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	учебная аудитория, специализированная учебная мебель ТСО: видеопроекционное оборудование/переносное видеопроекционное оборудование доска
Занятия семинарского типа	Инновационно- образовательный центр космических услуг Специализированная учебная мебель ТСО: Видеопроекционное оборудование Интерактивный стол Creority Touch для использования с программным комплексом РЕКОД-МОДЕЛЬ (разработчик - ОАО "Научно-производственная корпорация "Рекод"), рабочие станции, РЕКОД-Модель - построение пространственных моделей территорий и объектов Лицензионное программное обеспечение: в соответствии с рабочей программой
Самостоятельная работа обучающихся	помещение для самостоятельной работы, специализированная учебная мебель, ТСО: видеопроекционное оборудование, автоматизированные рабочие места студентов с возможностью выхода в информационно-телекоммуникационную сеть "Интернет", доска; Помещение для самостоятельной работы в читальном зале На-

	учно-технической библиотеки университета, специализированная учебная мебель автоматизированные рабочие места студентов с возможностью выхода информационно-телекоммуникационную сеть «Интернет», интерактивная доска