АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНСТИТУТ МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СВЯЗЕЙ»
INSTITUTE OF INTERNATIONAL ECONOMIC RELATIONS

Принята на заседании
Учёного совета ИМЭС
(протокол от 26 января 2022 г. № 6)

УТВЕРЖДАЮ
Ректор ИМЭС Ю.И. Богомолова
26 января 2022 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0162B6870090AF03B544352CE01F9DE4C7
Владелец: БОГОМОЛОВА ЮЛИЯ ИГОРЕВНА
Действителен: с 20.01.2023 до 20.04.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

по направлению подготовки
09.03.02 Информационные системы и технологии

Направленность (профиль)
«Информационные системы и сетевые технологии»

Москва – 2022

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 926.

Дисциплина «Информационная безопасность и защита информации» закладывает основы для разработки комплекса мер по обеспечению защиты информационных активов организации путем их идентификации, описания, выявления уязвимостей, угроз, а также рисков, которые могут произойти в случае реализации угроз применительно к имеющимся уязвимостям информационных активов. При этом комплекс мер основывается на соответствующей нормативно-правовой базе, включающий как федеральные законы и документы регулирующих государственных органов, так и стандарты, лучшие практики, отраслевые и локальные документы, а также организационном, аппаратном и программном обеспечении.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в учебные планы по программам подготовки бакалавров по направлению 09.03.02 Информационные системы и технологии и входит в обязательную часть Блока 1.

Дисциплина изучается на 3 курсе в 5 семестре.

Цель и задачи дисциплины

Цель изучения дисциплины - формирование у обучающихся необходимых компетенций для успешного освоения образовательной программы, в частности, ознакомление с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей и, конечно, методов их применения.

Задачи изучения дисциплины:

- сформировать знания, умения и практический опыт осуществления поиска, критического анализа и синтеза информации, применения системного подхода для решения поставленных задач;
- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
- сформировать знания, умения и практический опыт инсталляции программного и аппаратного обеспечения для информационных и

автоматизированных систем в области защиты информации;

- научиться применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой.
- формирование уровня знаний, умений, практического опыта, опыта деятельности в рамках программы подготовки кадров к Цифровой Экономике, построенных на основе Программы «Цифровая экономика России».

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компе-тенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	
Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3	**ОПК-3.1** Знает: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	методы защиты информации;	определять виды активы организации;	подготовки обзоров описания объекта защиты информации; определения и ранжирования активов организации;	Контактная работа: Лекции Лабораторные практикумы Самостоятельная работа
		ОПК-3.2 Умеет: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основные организационные и административные меры обеспечения ЗИ; основные правовые понятия, правовые акты Российской Федерации в области ЗИ, установленные на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	определять ценность каждого актива организации; формулировать требования к обеспечению сотрудниками ЗИ;	разработки политики ИБ организации;	
		ОПК-3.3 Имеет навыки: подготовки обзоров, аннотаций, составления рефератов,	порядок защиты информационных активов; основные	применять нормативные документы в сфере ИБиЗИ при	определения перечня нормативно-правового	

Результаты освоения ООП (содержание компетенций)	Код компе-тенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	
		научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	положения политики ИБ.	определении категории доступа к информации организации, а также для ее защиты на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	обеспечения ИБиЗИ.	
Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5	**ОПК-5.1** Знает: основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем	программные и аппаратные средства для обеспечения защиты информации	выбирать программное и аппаратное обеспечение на рынке обеспечения ИБиЗИ;	инсталляции программных и аппаратных средств обеспечения ИБиЗИ;	Контактная работа: Лекции Лабораторные практикумы Самостоятельная работа
		ОПК-5.2 Умеет: выполнять параметрическую настройку информационных и автоматизированных систем	современные стандарты информационного взаимодействия систем;	выполнять первичную настройку средств обеспечения ИБиЗИ.	сопровождения программных и аппаратных средств обеспечения ИБиЗИ	
		ОПК-5.3 Имеет навыки: инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем	классификацию средств обеспечения ИБиЗИ.	выполнять инсталляцию средств обеспечения ИБиЗИ.	работы по сопровождению ИБиЗИ информационной системы	
Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем	ОПК-7	**ОПК-7.1** Знает: основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем	основные платформы для реализации защиты информации;	осуществлять выбор платформ и инструментальных программно-аппаратных средств для обеспечения ИБиЗИ;	разворачивать инфраструктуру программно-аппаратных средств для обеспечения ИБиЗИ;	Контактная работа: Лекции Лабораторные практикумы Самостоятельная работа
		ОПК-7.2 Умеет: применять современные технологии для реализации информационных систем	основные требования к системе защиты информации;	делать расчет стоимости программно-аппаратных средств для обеспечения ИБиЗИ;	добавлять в системы защиты необходимые компоненты для полной работы.	

Результаты освоения ООП (содержание компетенций)	Код компе-тенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	
		ОПК-7.3 Имеет навыки: владения технологиями, применения инструментальных программно-аппаратных средств реализации информационных систем	процессы создания и эксплуатации системы информационной безопасности.	подбирать компоненты для обеспечения ИБиЗИ.	конструирования информационных систем в части применения инструментальных программно-аппаратных средств	

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности.	8					12				24	Защита отчета по лабораторному практикуму/20 Реферат/10
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	8					14				25	Защита отчета по лабораторному практикуму/20
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	10					14				25	Защита отчета по лабораторному практикуму/20
Тема 4. Защита информации в информационных системах.	10					14				25	Защита отчета по лабораторному практикуму/20 Эссе/10
Всего:	**36**					**54**				**99**	**100**
Контроль, час	**27**										**Экзамен**
Объем дисциплины (в академических часах)	**216**										
Объем дисциплины (в зачетных единицах)	**6**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности.

Основные понятия информационной безопасности (ИБ). Понятие тайны как объекта защиты ИБ. Организация защиты информации (ЗИ). Политика ИБ. Субъекты и средства, представляющие угрозу для ИБ. Субъекты и средства, осуществляющие защиту информации.

Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации.

Основы нормативно-правовой ЗИ. Основные нормативные документы РФ по ЗИ. Защита государственной тайны. Защита коммерческой тайны (КТ). Доктрина ИБ РФ. Государственные органы РФ, отвечающие за нормативно-правовое обеспечение ИБ.

Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации.

Организационная защита информации. Работа с конфиденциальной информацией. Функции службы безопасности. Классификация способов защиты информации. Основные действия по защите информации. Процессы создания и эксплуатации системы информационной безопасности. Типовая модель многорубежной системы защиты информации.

Тема 4. Защита информации в информационных системах.

Основные принципы организации процесса защиты информации. Угрозы информационной безопасности. Средства защиты информации. Защита информации от утечки по техническим каналам. Оценка эффективности системы ИБ. Средства несанкционированного доступа и защиты аудио информации. Средства несанкционированного доступа и защиты видео информации.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков использования профессиональной лексики, закрепление практических профессиональных компетенций, поощрение интеллектуальных инициатив.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое

изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к зачету с оценкой.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции, обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

Получение задания и рекомендаций к выполнению практикума.

Настройка инструментальных средств, необходимых для выполнения практикума.

Выполнение заданий практикума.

Подготовка отчета в соответствии с требованиями.

Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Реферат

Подготовка рефератов направлена на развитие и закрепление у обучающихся навыков самостоятельного глубокого, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации.

Рефераты должны отвечать высоким квалификационным требованиям в отношении научности содержания и оформления.

Темы рефератов, как правило, посвящены рассмотрению одной проблемы. Объем реферата может быть от 12 до 15 страниц машинописного текста, отпечатанного через 1,5 интервала, а на компьютере через 1 интервал (список литературы и приложения в объем

не входят).

Текстовая часть работы состоит из введения, основной части и заключения.

Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает конкретные цели и задачи, которые он собирается решить в ходе своего небольшого исследования.

В основной части подробно раскрывается содержание вопроса (вопросов) темы.

В заключении кратко должны быть сформулированы полученные результаты исследования и даны выводы. Кроме того, заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы.

В список литературы (источников и литературы) обучающийся включает только те документы, которые он использовал при написании реферата.

В приложении (приложения) к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата.

Эссе

Эссе - это самостоятельная письменная работа на тему, предложенную преподавателем. Цель эссе состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей.

Эссе должно содержать: четкое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с использованием концепций и аналитического инструментария, рассматриваемого в рамках дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме. В зависимости от специфики дисциплины формы эссе могут значительно дифференцироваться.

Структура эссе.

1. Титульный лист
2. Введение - суть и обоснование выбора данной темы, состоит из ряда компонентов, связанных логически и стилистически; На этом этапе очень важно правильно сформулировать вопрос, на который вы собираетесь найти ответ в ходе своего исследования.

При работе над введением могут помочь ответы на следующие вопросы: «Надо ли давать определения терминам, прозвучавшим в теме эссе?», «Почему тема, которую я раскрываю, является важной в настоящий момент?», «Какие понятия будут вовлечены в мои рассуждения по теме?», «Могу ли я разделить тему на несколько более мелких подтем?».

3. Основная часть - теоретические основы выбранной проблемы и изложение основного вопроса.

Данная часть предполагает развитие аргументации и анализа, а также обоснование их, исходя из имеющихся данных, других аргументов и позиций по этому вопросу. В этом заключается основное содержание эссе и это представляет собой главную трудность. Поэтому важное значение

имеют подзаголовки, на основе которых осуществляется структурирование аргументации; именно здесь необходимо обосновать (логически, используя данные или строгие рассуждения) предлагаемую аргументацию/анализ. Там, где это необходимо, в качестве аналитического инструмента можно использовать графики, диаграммы и таблицы.

В зависимости от поставленного вопроса анализ проводится на основе следующих категорий:

Причина — следствие, общее — особенное, форма — содержание, часть — целое, постоянство — изменчивость.

Хорошо проверенный способ построения любого эссе — использование подзаголовков для обозначения ключевых моментов аргументированного изложения: это помогает посмотреть на то, что предполагается. Такой подход поможет следовать точно определенной цели в данном исследовании. Эффективное использование подзаголовков - не только обозначение основных пунктов, которые необходимо осветить. Их последовательность может также свидетельствовать о наличии или отсутствии логичности в освещении темы.

4. Заключение - обобщения и аргументированные выводы по теме с указанием области ее применения и т.д. Методы, рекомендуемые для составления заключения: повторение, иллюстрация, цитата, впечатляющее утверждение. Заключение может содержать такой очень важный, дополняющий эссе элемент, как указание на применение исследования, не исключая взаимосвязи с другими проблемами.

Навигация для обучающихся по самостоятельной работе в рамках изучения дисциплины

Наименование темы	**Вопросы, вынесенные на самостоятельное изучение**	**Формы самостоят. работы**	**Форма текущего контроля**
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	Основные понятия информационной безопасности (ИБ). Понятие тайны как объекта защиты ИБ. Организация защиты информации (ЗИ).	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму Подготовка реферата	Реферат Защита отчета по лабораторному практикуму
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	Доктрина ИБ РФ. Государственные органы РФ, отвечающие за нормативно-правовое обеспечение ИБ.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по	Защита отчета по лабораторному практикуму

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоят. работы	Форма текущего контроля
		практикуму	
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	Процессы создания и эксплуатации системы информационной безопасности. Типовая модель многорубежной системы защиты информации.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Защита отчета по лабораторному практикуму
Тема 4. Защита информации в информационных системах	Угрозы информационной безопасности. Средства несанкционированного доступа и защиты аудио информации. Средства несанкционированного доступа и защиты видео информации.	Работа с литературой, включая ЭБС, Ресурсами информационно-коммуникационной сети «Интернет» Подготовка к лабораторному практикуму, подготовка отчета по практикуму Подготовка эссе	Эссе Защита отчета по лабораторному практикуму

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

2. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

Дополнительная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

2. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. – Москва :

Издательский дом Высшей школы экономики, 2015. – 574 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

3. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

4. Смирнов, В.И. Защита информации / В.И. Смирнов ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2017. – 67 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

5. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка
1.	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
2.	Специализированный сайт по тематике информационной безопасности	http://all-ib.ru/
3.	Официальный сайт Institute of Electrical and Electronics Engineers (IEEE)	http://www.ieee.org/index.html
4.	Официальный сайт компании Infowatch	http://www.infowatch.ru/
5.	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
6.	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/
7.	Официальный сайт журнала «Информационная безопасность»	http://www.itsec.ru/main.php

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория (Лаборатория информационно-коммуникационных технологий), оборудованная:
комплекты специализированной учебной мебели, мультимедийный проектор, экран, доска классная, принтер, компьютер преподавателя и компьютеры обучающихся с выходом в сеть «Интернет», доступом в электронную информационно-образовательную среду.

Помещение для самостоятельной работы обучающихся – аудитория, оборудованная:
комплекты специализированной учебной мебели, мультимедийный проектор, экран, доска классная, компьютеры с выходом в сеть «Интернет»

и доступом в электронную информационно-образовательную среду.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

- Windows (зарубежное, возмездное);
- MS Office (зарубежное, возмездное);
- Adobe Acrobat Reader (зарубежное, свободно распространяемое);
- КонсультантПлюс: «КонсультантПлюс: Студент» (российское, свободно распространяемое);
- 7-zip – архиватор (зарубежное, свободно распространяемое);
- Comodo Internet Security (зарубежное, свободно распространяемое);
- MySQL for Windows – реляционная система управления базами данных (зарубежное, свободно распространяемое);
- Apache NetBeans – свободная интегрированная среда разработки приложений (IDE) на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада и ряда других (зарубежное, свободно распространяемое);
- Android Studio – разработка мобильных приложений (зарубежное, свободно распространяемое)

электронно-библиотечная система:

- Электронная библиотечная система (ЭБС) «Университетская библиотека ONLINE» http://biblioclub.ru/.
- Образовательная платформа «Юрайт». Для вузов и ссузов. Электронная библиотечная система (ЭБС) https://urait.ru/

современные профессиональные баз данных:

- Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.
- Портал Единое окно доступа к образовательным ресурсам http://window.edu.ru/

информационные справочные системы:

- Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
- Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/).

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	20-15 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 14-10 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 9-6 – работа и отчет выполнены в срок, в основном самостоятельно, использованы соответствующие формулы; определены соответствующие спецификации, имеются ошибки в расчетах; выбраны совместимые комплектующие необходимые, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 5 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.
2.	Реферат	10-9 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 8-7 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 6-5 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.
3.	Эссе	10-9 – грамотное использование компьютерной

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
		терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 8-7 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 6-5 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания к лабораторным практикумам

Лабораторный практикум № 1. Общие проблемы безопасности. Основные положения теории информационной безопасности

Задание 1

1. Придумайте, компанию, для которой вы будете разрабатывать нормативное и административно-организационное обеспечение информационной безопасности. Это может быть:

- вымышленная компания;
- компания, где вы работаете;
- компания, по которой планируете выполнять дипломный проект;
- компания, где вы проходили практику;
- компания, описание и данные по которой вы использовали в рамках другого курса;

2. Приведите краткое описание компании:

- название, организационно-правовая форма, учредители
- краткая история компании (год основания, основные этапы развития)
- сфера деятельности
- миссия
- количество сотрудников
- организационная структура (представить в виде рисунка)
- способы ведения бизнеса
- основные конкуренты и конкурентная стратегия
- основные поставщики и потребители (клиенты)
- цели компании на ближайшие год (не менее 5 целей), три года (не менее 5 целей), пять лет (не менее 5 целей).

Задание 2

Определить основные активы компании, и занести данные в соответствующую таблицу. Количество активов каждого вида определяется особенностями компании и должно соответствовать

информационным потокам компании, а также используемым программным и техническим средствам для их обработки.

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная	Качественная
Информационные активы						
Активы программного обеспечения						
Физические активы						

Задание 3

Провести ранжирование активов по пятибалльной шкале по степени их значимости для компании, выявить наиболее ценные активы. Данные представить в виде таблицы.

Наименование актива	Ценность актива (ранг)

Задание 4

Разработка политики информационной безопасности

1. Ознакомьтесь с прилагаемыми нормативными документами для разработки политики информационной безопасности (ИБ), а также учебным фрагментом политики ИБ компании «Ин Техно» (в фрагменте представлена общая политика ИБ без указания конкретных деталей, сроков, ответственных лиц и так далее).

2. Разработайте проект политики ИБ для вашей организации. При этом следует акцентировать внимание на следующих аспектах:

- цели политики ИБ;
- основные принципы;
- на кого будет распространяться эта политика;
- выделение групп пользователей
- выделение основных видов информационных ресурсов;
- определение уровней доступа (атрибутов безопасности) к информации:
  - открыто (О)
  - конфиденциально (К)
  - секретно (С),
  - совершенно секретно (СС)
  - особая важность (ОВ)
- определение политики в отношении паролей, в честности:
  - повторяемость / неповторяемость паролей
  - количество паролей, хранимое системой
  - максимальный срок действия пароля

– минимальный срок действия пароля

– минимальная длина пароля

– соответствие требованиям сложности

– параметры блокировки учетных записей (пороговое значение блокировки, время блокировки, сброс счетчика блокировки)

- определение политики в отношении доступа к ресурсам сети Internet, в частности:

– использование доступа к сети Internet в личных целях

– ведение «белого» или «черного» списка сайтов

– временной интервал доступа сети Internet

– объем скачиваемой и загружаемой информации

– возможности использования ресурсов сети Internet различными группами пользователей

– использование почтовых и иных сервисов

– контроль за использованием ресурсов сети Internet

- что разрешено, а что запрещено различным группам пользователей;
- рекомендации для пользователей.

Политика ИБ должна отвечать на следующие вопросы

1. Насколько возможно использование Интернет в личных целях?
2. Ограничивать ли работу в Интернет в нерабочее время?
3. Как решаются вопросы конфиденциальности корпоративной информации?
4. Какое место занимают вопросы безопасности в политике ИБ?
5. На кого распространяется эта политика?
6. Какие права оставляет за собой организация?
7. Какие юридические аспекты необходимо учитывать?
8. Прочие вопросы.

Лабораторный практикум № 2. Нормативно-правовые аспекты информационной безопасности и защиты информации.

Задание 1

Провести оценку уязвимости активов. Данные представить в виде таблицы (либо таблиц, т.к. удобнее сформировать отдельную таблицу для каждого типа активов). С примерами типовых уязвимостей можно ознакомиться в приложении D стандарта ГОСТ Р ИСО/МЭК 27005-2010.

Активы **Группа уязвимостей и содержание уязвимости**	**Актив 1**	**Актив 2**	**Актив 3**	**…**	**Актив N**
Аппаратные средства					
Программные средства					

Сеть					
Персонал					
Место функционирования организации					
Организация					

Задание 2

Определить перечень информационных активов, обязательное ограничение доступа, к которым регламентируется действующим законодательством РФ, а также отнесенных компанией к коммерческой тайне. Данные представить в виде таблицы.

№ п/п	Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, №№ статей

Лабораторный практикум № 3. Административно-организационные аспекты информационной безопасности и защиты информации.

Задание 1

Проведите оценку угроз активам. Данные представить в виде таблицы.

Группа угроз/ Содержание угроз	Актив 1	Актив 2	Актив 3	…	Актив N
1. Угрозы, обусловленные преднамеренными действиями					
2. Угрозы, обусловленные случайными действиями					
3. Угрозы, обусловленные естественными причинами (природные, техногенные факторы)					

Задание 2

Проведите оценку рисков информационной безопасности Данные представьте в виде таблиц оценки «штрафных баллов» и результатов оценки рисков ИБ (таблица 3.2).

Оценивание рисков производится экспертным путем на основе анализа ценности активов, возможности применения угроз и использования уязвимостей, определенных в предыдущих заданиях. Для

оценивания используется таблица с заранее предопределенными «штрафными баллами» для каждой комбинации ценности активов, уровня угроз и уязвимостей

Пример оценки уровень угроз и уязвимостей («штрафных баллов»)

	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.

Результаты оценки рисков информационной безопасности

Риск	Актив	Ранг риска

Лабораторный практикум № 4. Защита информации в информационных системах.

На основе данных, полученных при выполнении предыдущих заданий и произвольных данных потерях из-за инцидентов информационной безопасности, и затратах на систему ИБ и провести расчет показателей эффективности системы ИБ.

Задание 1.

Рассчитать величину потерь ДО модернизации системы ИБ. Данные представить в таблице 4.1.

Величины потерь (рисков) для критичных информационных ресурсов до/после внедрения/модернизации системы защиты информации

Актив	Угроза	Величина потерь (тыс.руб.)

Задание 2.

Рассчитать объем разового и постоянного ресурса, выделяемого на защиту информации. Данные представить в таблицах Ресурс, выделяемый на защиту информации, может иметь разовый и постоянный характер. Разовый ресурс расходуется на закупку, установку и наладку дорогостоящей техники, постоянный - на заработную плату сотрудникам

службы безопасности и поддержание определенного уровня безопасности, прежде всего, путем эксплуатации технических средств и контроля эффективности защиты.

Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия				
п\п	**Выполняемые действия**	**Среднечасовая зарплата специалиста (руб.)**	**Трудоемкость операции (чел.час)**	**Стоимость, всего (тыс.руб.)**
Стоимость проведения организационных мероприятий, всего				
Мероприятия инженерно-технической защиты				
№ п/п	**Номенклатура ПиАСИБ, расходных материалов**	**Стоимость, единицы (тыс.руб)**	**Кол-во (ед.измерения)**	**Стоимость, всего (тыс.руб.)**
Стоимость проведения мероприятий инженерно-технической защиты				
Объем разового ресурса, выделяемого на защиту информации				

Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п\п	**Выполняемые действия**	**Среднечасовая зарплата специалиста (руб.)**	**Трудоемкость операции (чел.час)**	**Стоимость, всего (тыс.руб.)**
Стоимость проведения организационных мероприятий, всего				
Мероприятия инженерно-технической защиты				
№ п/п	**Номенклатура ПиАСИБ, расходных материалов**	**Стоимость, единицы (тыс.руб)**	**Кол-во (ед.измерения)**	**Стоимость, всего (тыс.руб.)**
Стоимость проведения мероприятий инженерно-технической защиты				
Объем постоянного ресурса, выделяемого на защиту информации				

Задание 3.

Рассчитать величину потерь ПОСЛЕ модернизации системы ИБ. Данные представить в таблице 4.1.

Задание 4.

Рассчитать показатели экономической эффективности системы ИБ. Пусть

$R_{\sum}$ - суммарное значение ресурса, выделенного на защиту информации *за год*

$R_{ср}$ – реальные среднегодовые потери из-за инцидентов информационной безопасности (потери ДО модернизации)

$R_{прогн}$ – прогнозируемые потери после модернизации системы ИБ (потери ПОСЛЕ модернизации)

Тогда срок окупаемости затрат на обеспечение ИБ составит:

$$\mathbf{T_{ок} = R_{\sum} / (R_{ср} – R_{прогн})}$$

Задание 5.

Обменяйтесь выполненным практикумом с вашим одногруппником. Проведите условный анализ выполнения основных задач по обеспечению безопасности на основе полученных данных.

Анализ выполнения основных задач по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	**Степень выполнения**

Дополнительно опишите ваши замечания по полученным данным, в частности по оценке информационных активов, рисков, угроз, политики ИБ и так далее.

Примерные темы рефератов:

1. Сравнительный анализ сетевых сканеров.
2. Сравнительный анализ программных межсетевых экранов.
3. Сравнительный анализ аппаратных межсетевых экранов.
4. Сравнительный анализ систем обнаружения атак или вторжений.
5. Международные стандарты в сфере безопасности сетей.
6. Российское законодательство по информационной безопасности и безопасности сетей.
7. Международное законодательство по информационной безопасности и безопасности сетей.
8. Сравнительный анализ производителей аппаратных средств обнаружения и отражения сетевых атак.
9. Сравнительный анализ разработчиков программных средств обнаружения и отражения сетевых атак.
10. Сравнительный анализ комплексных программных средств обеспечения сетевой безопасности.
11. Сравнительный анализ комплексных аппаратных средств обеспечения сетевой безопасности.
12. Комплекс программных решений в области информационной безопасности компании Infowatch.
13. Комплекс программных решений в области информационной безопасности Лаборатории Касперского.
14. Комплекс программных решений в области информационной безопасности компании Symantec.

15. Комплекс программных решений в области информационной безопасности компании SearchInform.

Примерные темы эссе:

1. Защита систем трансляции, передачи сообщений и электропитания.
2. Защита помещения от утечки акустической информации через акустоэлектрические преобразователи телефонной цепи и аппарата.
3. Акустопреобразовательные элементы с передачей информативного сигнала радиоизлучением.
4. Акустоэлектрические преобразователи, технические характеристики акустопреобразовательного канала.
5. Криптографическая защита телефонных сообщений.
6. Активные способы защиты телефонных линий.
7. Пассивные способы защиты телефонных линий.
8. Телефонная линия как канал утечки информации, индуктивный и бесконтактный съем информации с телефонной линии.
9. Комбинированные способов технической защиты телефонных линий.
10. Способы технической защиты в IP телефонии.
11. Радиозакладные устройства.
12. Сетевые закладные устройства.
13. Средства и способы обнаружения радиозакладных устройств.
14. Комплексы мониторинга технических каналов утечки информации.
15. Активное противодействие закладным радиоустройствам.
16. Акустические устройства перехвата информации.
17. Защита конфиденциальной акустической информации от несанкционированной аудио записи.
18. Портативные средства аудиозаписи, способы и средства противодействия.
19. Переносные средства аудиозаписи, способы и средства противодействия.
20. Способы и средства проверки звукоизоляции помещений.
21. Средства контроля эффективности акустической защиты.
22. Аппаратно-программные комплексы виброакустическмих измерений.
23. Пассивные способы защиты акустической информации.
24. Активные способы защиты акустической информации.
25. Комплексные системы защиты акустической информации.
26. Защита конфиденциальной информации от несанкционированной видео записи.
27. Портативные средства видеозаписи, способы и средства противодействия.
28. Переносные средства видеозаписи, способы и средства противодействия.
29. Технические каналы утечки информации.

30. Технические средства информационной разведки и промышленного шпионажа.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Процедура оценивания	Шкала и критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета, включающего в себя: Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающимся принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними; Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности; Задание №3 – задание на проверку умений и навыков, полученных в результате освоения дисциплины	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые формулы, использована профессиональная лексика. Задача решена правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо)–** ответ в целом правильный, логически выстроен, приведены необходимые формулы, использована профессиональная лексика. Ход решения задачи правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно)–** ответ в основном правильный, логически выстроен, приведены не все необходимые формулы, использована профессиональная лексика. Задача решена частично. **-Менее 50 (неудовлетворительно)**– ответы на теоретическую часть неправильные или неполные. Задача не решена

Типовые задания для проведения промежуточной аттестации обучающихся

Задания на знания

1. Содержание понятий «информационная безопасность» и «безопасность информации». Направления обеспечения безопасности информации. Виды информации с точки зрения организации их защиты. Действия, приводящие к незаконному овладению конфиденциальной информацией.

2. Виды информации, доступ к которой должен быть органичен. Законодательно закрепленные виды тайн. Перечень и содержание информации, относящийся к различным видам тайн (государственная тайна, коммерческая тайна, сведения, затрагивающие неприкосновенность частной жизни и так далее).

3. Основные цели и задачи защиты информации. Компоненты

системы защиты информации. Основные направления деятельности по защите информации. Уровни информационной безопасности. Виды информационных активов организации, порядок определения их стоимости и ранжирования по уровню ценности. Организация защиты информационных активов организации.

4. Цели, задачи, основные разделы и их содержание документа «Политика информационной безопасности». Требования к «Политике информационной безопасности».

5. Уровни нормативно-правовой защиты в сфере информационной безопасности. Структура правовых актов по защите информации. Виды деятельности по защите информации и обеспечению информационной безопасности, подлежащие обязательному лицензированию.

6. Законодательство Российской Федерации в сфере информационной безопасности и защиты информации (основные нормативные документы и их содержание). Виды преступлений в сфере информационных технологий и ответственность за них.

7. Основные нормативные документы по защите государственной тайны и их содержание. Перечень сведений, отнесенных к государственной тайне и порядок их защиты.

8. Основные нормативные документы по защите коммерческой тайны и их содержание. Требования к информации, содержащей коммерческую тайну. Примерный перечень сведений, которые можно отнести к коммерческой тайне и порядок их защиты.

9. Основные составляющие национальных интересов и угроз информационной безопасности Российской Федерации в информационной сфере согласно Доктрине информационной безопасности Российской Федерации.

10. Цели и задачи организационной защиты информации. Направления организационной защиты информации и их практическая реализация.

11. Порядок работы с конфиденциальной информацией. Виды грифов конфиденциальной информации. Порядок работы с конфиденциальными документами.

12. Цели и задачи службы безопасности. Организация работы службы безопасности.

13. Перечень и содержание способов противодействия информационным угрозам.

14. Перечень и содержание основных действий по защите информации.

15. Основные требования к системе обеспечения информационной безопасности и защиты информации.

16. Виды и содержание угроз информационной безопасности.

17. Классификация, возможности и назначение средств инженерно-технической защиты информации.

18. Назначение, возможности и практическое применение средств поиска, обнаружения, детальных измерений, активного и пассивного

противодействия грозам информационной безопасности.

19. Назначение, возможности и практическое применение физических средств защиты информации.

20. Назначение, возможности и практическое применение аппаратных средств защиты информации.

21. Назначение, возможности и практическое применение программных средств защиты информации.

22. Основные факторы и виды утечки информации по техническим каналам (указать технические каналы утечки и их характеристики).

23. Средства и способы защиты информации от утечки по визуально-оптическому и акустическому каналам**.**

24. Средства и способы защиты информации от утечки по электромагнитному и радио каналам.

25. Виды ресурсов, выделяемых на обеспечение информационной безопасности и защиты информации. Порядок расчета срока окупаемости мероприятий по информационной безопасности и защите информации.

Задания на умения

1. Нарушение целостности данных, как правило, вызвано реализацией внешних или внутренних угроз? Обоснуйте ответ.

2. Нарушение конфиденциальности данных, как правило, вызвано реализацией внешних или внутренних угроз? Обоснуйте ответ.

3. Как соотносятся между собой понятия уязвимости и угроз? Обоснуйте ответ.

4. Как соотносятся между собой понятия угроз и рисков? Обоснуйте ответ.

5. В чем заключается отличие между разглашением и утечкой информации? Обоснуйте ответ.

6. Какими способами может быть реализовано противоправное преднамеренное овладение конфиденциальной информацией? Обоснуйте ответ.

7. Каким образом может происходить бесконтрольный выход конфиденциальной информации за пределы организации? Обоснуйте ответ.

8. В чем заключается отличие между служебной и профессиональной тайной? Обоснуйте ответ.

9. Что относится к информационным активам организации, и какие информационные активы являются наиболее ценным для организаций, осуществляющих различные виды деятельности (3-4 примера)? Обоснуйте ответ.

10. Какие сведения не могут составлять коммерческую тайну? Обоснуйте ответ.

11. Какие предъявляются требования к информации, составляющей коммерческую тайну? Обоснуйте ответ.

12. В чем заключается отличие между деятельностью ФСБ и ФСТЭК в сфере нормативно-правового регулирования защиты информации?

Обоснуйте ответ.

13. В чем заключается отличие между правами собственности, владения и распоряжения информацией? Обоснуйте ответ.

14. Какая информация в соответствии с федеральными законами РФ ограничивается или запрещается к распространению? Обоснуйте ответ.

15. Какая информация в соответствии с федеральными законами РФ подлежит предоставлению или распространению? Обоснуйте ответ.

16. В чем заключается отличие между передачей и разглашением коммерческой тайны? Обоснуйте ответ.

17. В чем заключается отличие между предупреждением и выявлением угроз? Обоснуйте ответ.

18. В чем заключается отличие между выявлением и обнаружением угроз? Обоснуйте ответ.

19. Какие требования предъявляются к системе защиты информации? Обоснуйте ответ.

20. В чем заключается отличие между активными и пассивными средствами защиты информации? Обоснуйте ответ.

21. В чем заключается отличие между каналом передачи и каналом утечки информации? Обоснуйте ответ.

22. В чем заключается отличие между физическими и аппаратными средствами защиты информации? Обоснуйте ответ.

23. В чем заключается отличие между программными средствами собственной защиты и в составе вычислительной системы? Обоснуйте ответ.

24. Что легче: локализовать или обнаружить канал утечки информации? Обоснуйте ответ.

25. В чем заключается отличие между разовым и постоянным ресурсом, выделяемым на защиту информации? Обоснуйте ответ.

Задания на навыки

Задание № 1.

Исходя из анализа описания предприятия определить и ранжировать его основные активы. Результаты представить в виде таблиц.

Задание № 2.

Исходя из анализа предложенной политики информационной безопасности, определить ее упущения и слабые места.

Задание № 3.

Исходя из анализа описания предприятия определить перечень информационных активов, обязательное ограничение доступа к которым регламентируется действующим законодательством РФ, а также отнесенных к коммерческой тайне.

Задание № 4.

Исходя из анализа описания предприятия и его основных активов определить соответствующие уязвимости. Результаты представить в виде таблицы.

Задание № 5.

Исходя из анализа потенциальных каналов утечки информации, являющейся конфиденциальной, а также представляющей коммерческую либо государственную тайну определить перечень мер по предотвращению возможной утечки (включая установку аппаратных и программных средств).

Задание № 6.

Исходя из анализа описания, программной и технической архитектуры предприятия определить возможные каналы утечки информации, являющейся коммерческой тайной.

Задание № 7.

Исходя из анализа описания предприятия и его основных активов, определить соответствующие угрозы. Результаты представить в виде таблицы.

Задание № 8.

Исходя из анализа описания предприятия и его основных активов, уязвимостей и угроз определить и ранжировать соответствующие риски. Результаты представить в виде таблицы.

Задание № 9.

По представленным данным о затратах на систему обеспечения информационной безопасности провести расчет показателей ее экономической эффективности.

Задание № 10.

Исходя из анализа описания программной и технической архитектуры предприятия, определить комплекс средств инженерно-технической защиты информации необходимый для существенного повышения уровня ее защиты.