МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол № 11 от «20» июня 2019 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Системы инженерно-технической защиты информации

Б1.В.1.ДВ.07.02 вариативная

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
к.б.н., доцент
/Ф.Т. Байрушин

Для приема: 2019 г.

Уфа 2019 г.

Составитель: Ф.Т. Байрушин

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью протокол от «20» июня 2019 г. №11

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» _____________ 20 _ г.

Заведующий кафедрой ____________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» _____________ 20 _ г.

Заведующий кафедрой ____________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» _____________ 20 _ г.

Заведующий кафедрой ____________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» _____________ 20 _ г.

Заведующий кафедрой ____________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать основные принципы работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);	
	Знать способы организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);	
	Знать основные принципы организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Умения	Уметь выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);	
	Уметь применять методы организации и сопровождения аттестации объекта информатизации по требованиям	ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);	

	безопасности информации		
	Уметь применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Владения (навыки / опыт деятельности)	Владеть навыками установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);	
	Владеть навыками организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);	
	Владеть навыками организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Системы инженерно-технической защиты информации» относится к дисциплинам вариативной части.
Дисциплина изучается на 2,3 курсах в 4,5 семестрах.
Цель изучения дисциплины: формирование у бакалавров целостного представления о системах инженерно-технической защиты информации.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы

обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

КАРТА КОМПЕТЕНЦИИ ПК-1

ПК-1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Этап (уровень) освоения компетенции	**Планируемые результаты обучения** (показатели достижения заданного уровня освоения компетенций)	**Критерии оценивания результатов обучения**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД; эксплуатационные и технико-экономические характеристики программных	Имеет фрагментарные знания о аппаратных средствах вычислительной техники; операционных системах персональных ЭВМ	Знает основные аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности; основные направления политик защиты информации на предприятии	Знает, с небольшими ошибками, аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД; эксплуатационные и технико-экономические характеристики	Знает аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД; эксплуатационные и технико-экономические характеристики программных

	и технических средств защиты информации и обеспечения информационной безопасности; основные направления политик защиты информации на предприятии (организации); возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.;		(организации)	ки программных и технических средств защиты информации и обеспечения информационной безопасности; основные направления политик защиты информации на предприятии (организации); возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.;	и технических средств защиты информации и обеспечения информационной безопасности; основные направления политик защиты информации на предприятии (организации); возможные угрозы информационной безопасности, связанные с аспектами деятельности предприятия (организации), особенностями технологических процессов, организационной структуры и др.
Второй этап (уровень)	Уметь: формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных	Небольшие умения в области выполнения работ по эксплуатации технических и программных средств обеспечения информационной	В целом умеет настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на	Умеет, с небольшими недочетами, формулировать и настраивать политику безопасности распространенных операционных систем, а	Умеет формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных

	вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты**;** выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации;	безопасности и защиты информации	их основе; выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации;	также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты**;** выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты**;** выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации;
Третий этап (уровень)	Владеть: методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации.	Плохо владеет навыками методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации.	При помощи опытных сотрудников способен тестировать. настраивать и применять средства программно-технического обеспечения защиты информации.	Владеет большинством способов оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации.	Владеет методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации.

КАРТА КОМПЕТЕНЦИИ ПК-5

ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

Этап (уровень) освоения компетенции	**Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)**	**Критерии оценивания результатов обучения**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: Правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Имеет фрагментарные знания об основных понятиях о правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	В целом знает об основных правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства, но допускает значительные ошибки	Хорошо знает об основных правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства, но допускает незначительные ошибки	Обладает целостными знаниями об основных правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства.
Второй этап (уровень)	Уметь: Выбирать тип необходимых средств для выявления наличия электронных	Умеет выбирать тип необходимых средств для выявления наличия электронных	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата	Умеет выбирать тип необходимых средств для выявления наличия электронных	Уверенно умеет выбирать тип необходимых средств для выявления наличия

	средств перехвата информации; Применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе; Разрабатывать организационно-распорядительные документы по вопросам защиты информации;	средств перехвата информации, но не умеет применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе и разрабатывать организационно-распорядительные документы по вопросам защиты информации	информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, но не в полнее умеет разрабатывать организационно-распорядительные документы по вопросам защиты информации	средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, разрабатывать организационно-распорядительные документы по вопросам защиты информации, но допускает незначительные ошибки.	электронных средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, разрабатывать организационно-распорядительные документы по вопросам защиты информации
Третий этап (уровень)	Владеть: Навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Не способен правильно работать с нормативными правовыми актами и не вполне владеет навыками лицензирования в области защиты информации.	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирования систем защиты информации, но без учета требований по сравнительному анализу подсистем по показателям информационной безопасности	Владеет навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирования систем защиты информации, но испытывает незначительные трудности при определении требований и сравнительном анализе подсистем по показателям	Владеет навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирования систем защиты информации, определением требований, сравнительным анализом подсистем по показателям информационной безопасности

				информацион ной безопасно	

КАРТА КОМПЕТЕНЦИИ ПК-6

ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Этап (уровень) освоения компетенции	**Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)**	**Критерии оценивания результатов обучения**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: основные принципы оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Имеет фрагментарные знания об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	В целом знает: об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных, но не знает критерии и меры надежности, возможности и особенности организационно, аппаратных и программных средств безопасности и защиты информации.	Знает: об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации, но допускает незначительные ошибки.	Демонстрирует целостность знания об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
Второй этап (уровень)	Уметь: использовать возможности и особенности организационных, аппаратных и программных средств обеспечения	Умеет использовать возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и	Умеет использовать возможности и особенности организационно, аппаратных и программных средств обеспечения безопасности и	Уверенно использует возможности и особенности организационных, аппаратных и программных средств обеспечения	Уверенно использует возможности и особенности организационных, аппаратных и программных средств обеспечения

	безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	защиты информации.	защиты информации, но не умеет составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности, но допускает незначительные ошибки.	безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.
Третий этап (уровень)	Владеть: навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем	Не способен эксплуатировать современного электронного обор и информационно-коммуникационных технологий.	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, но не использует методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем.	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем, но испытывает незначительные трудности	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	основные принципы работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);	Опрос, практические задания, тестирование
	способы организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);	Опрос, практические задания, тестирование
	основные принципы организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Опрос, практические задания, тестирование
2-й этап Умения	выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);	Опрос, практические задания, тестирование
	применять методы организации и сопровождения аттестации объекта информатизации по требованиям безопасности	ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по	Опрос, практические задания, тестирование

	информации	требованиям безопасности информации (ПК-5);	
	применять навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Опрос, практические задания, тестирование
3-й этап Владения навыками	установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);	Опрос, практические задания, тестирование
	организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);	Опрос, практические задания, тестирование
	организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Опрос, практические задания, тестирование

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины, для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;
от 80 баллов – «отлично».

Устный опрос (аудиторная работа)

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации. Студент излагает содержание вопроса изученной темы и делает доклад по одной из тем.

Примерная тематика занятий

Модуль 1

Основные свойства информации как предмета инженерно-технической защиты
Источники и носители конфиденциальной информации
Виды угроз безопасности информации
Способы и средства инженерной защиты и технической охраны

Модуль 2.

Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки
Способы предотвращения утечки информации по материально-вещественному каналу
Общие положения по инженерно-технической защите информации в организации
Организационные и технические меры по инженерно-технической защите информации в организации

Модуль 3

Принципы построения системы СТЗИ: многозональность и многорубежность
Одноразовые пароли
Ролевое управление доступом
Низкочастотные и высокочастотные излучения технических средств

Модуль 4

Цифровые сертификаты
Шифрование заменой(подстановка
Типовая структура технического канала утечки информации
Система распределения ключей Диффи-Хелмана

Критерии и методика оценивания:

Студенту предлагается 4 задания в каждом из 4 модулей в процессе изучения материала курса. За каждое задание начисляется:

- 1,5 балла, если ответы на вопросы даны верно и достаточно полно.
- 1 балл за неполный ответ,
- 0 баллов если ответ на устный вопрос не дан или дан неверно.

Темы практических занятий

Модуль 1

1. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты (предлагается до 5 видов объектов защиты).
2. – Составление модели поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
3. – Составление модели поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
4. – Определение и анализ условий и факторов, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.
5. – Разработка и анализ методов защиты видовых демаскирующих признаков от технических средств разведок.
6. – Разработка и анализ методов защиты сигнальных демаскирующих признаков от технических средств разведок.
7. – Разработка и анализ методов защиты радиосигналов от перехвата техническими средствами разведок.

Модуль 2

1. – Разработка и анализ методов защиты электрических сигналов от перехвата техническими средствами разведок.
2. – Разработка и анализ методов защиты материальных и вещественных демаскирующих признаков от технических средств разведок.
3. – Анализ возможностей технических средств наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
4. – Анализ возможностей технических средств наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
5. – Анализ возможностей технических средств перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.
6. – Анализ возможностей технических средств съема конфиденциальной речевой информации с использованием вторичных переизлучателей.
7. – Анализ возможностей технических средств съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.

Модуль 3

1. – Анализ возможностей технических средств съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.
2. – Анализ возможностей технических средств подслушивания, методы и средства противодействия средствам подслушивания.
3. – Анализ возможностей технических средств демаскирующих признаков веществ, методы и средства нейтрализации (утилизации) отходов производства.
4. – Анализ возможностей технических средств контроля, обнаружения, уничтожение закладных устройств, порядок проведения поисковых мероприятий на предлагаемом объекте (до 5 объектов).
5. – Анализ возможностей технических средств контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения поисковых мероприятий (до 5 видов линий и их архитектур построения).
6. – Анализ возможностей технических средств контроля, обнаружения, уничтожение закладных устройств в телефонных линиях связи, порядок проведения поисковых мероприятий (до 5 видов линий и их архитектур построения).

7. – Анализ возможностей технических средств контроля, обнаружения, уничтожение 11 закладных устройств, в электросетях, цепях заземления, порядок проведения поисковых мероприятий.

Модуль 4

1. – Моделирование вербального объекта защиты, возможных угроз безопасности информации для оптических каналов утечки информации в видимом и ИК диапазонах, разработка способов, методов и технических средств защиты информации.
2. – Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации.
3. – Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустикорадиоэлектронных каналов утечки информации, разработка методов и технических средств защиты информации.
4. – Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-оптических каналов утечки информации, разработка методов и технических средств защиты информации.
5. – Моделирование вербального объекта защиты, где производится обработка информации с использованием СВТ (АС), возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.
6. – Моделирование вербального объекта защиты, где производится обработка информации с использованием технических средств обработки информации, возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.
7. – Моделирование вербального объекта защиты, возможных угроз безопасности информации для материально-вещественных каналов утечки информации, разработка методов и технических средств защиты информации.

Критерии и методика оценивания:

Студенту предлагается 7 заданий в каждом из 4 модулей в процессе изучения материала курса. За каждое задание начисляется:

Критерии и методика оценивания:

- 2 балла выставляется студенту, если практическое задание решено верно, показано уверенное владение учебным материалом;

- 1 балл выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок, получен верный ответ, нет определенной логической последовательности, неточно используется специализированная терминология;

- 0 баллов выставляется студенту, если студент не дал ни одного правильного ответа

Типовые тесты

Модуль 1

1. Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

2. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;

4. Под replay-атакой понимается:
1. модификация передаваемого сообщения
2. повторное использование переданного ранее сообщения
3. невозможность получения сервиса законным пользователем

5. Уровень секретности - это
1. ответственность за модификацию и НСД информации
2. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

6. Что такое несанкционированный доступ (нсд)?
1. Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2.Создание резервных копий в организации
3. Правила и положения, выработанные в организации для обхода парольной защиты
4. Вход в систему без согласования с руководителем организации

7 К посторонним лицам нарушителям информационной безопасностиотносится:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.

8. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
1. Безопасная OECD
2. ISO\IEC
3. OECD
4. CPTED

9. Перехват, который осуществляется путем использования оптической техники называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. К внутренним нарушителям информационной безопасности относится:
1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

11. Анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности – это?
1. Протоколирование
2. Экранирование
3. Аудит

12. Хронологически упорядоченная совокупность записей результатов деятельности субъектов АС, достаточная для восстановления, просмотра и анализа последовательности действий с целью контроля конечного результата – это?
1. Политика безопасности
2. Журнал аудита
3. Регистрационный журнал

13. К какому классу межсетевых экранов относится CISCO PIX?
1. Межсетевые экраны экспертного уровня
2. Шлюзы прикладного уровня

14. Активный перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;

5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

15. Защита информации от утечки это деятельность по предотвращению:
    1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
    2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
    3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
    4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
    5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

16.Длина исходного ключа у алгоритма шифрования DES (бит)
56
128
64
256

17.Компьютер — это:
а) устройство для работы с текстами;
б) электронное вычислительное устройство для обработки чисел;
в) устройство для хранения информации любого вида;
г) многофункциональное электронное устройство для работы с информацией;
д) устройство для обработки аналоговых сигналов.
е) другое

18. Постоянное запоминающее устройство служит для:
а) хранения программ начальной загрузки компьютера и тестирования его узлов;
б) хранения программы пользователя во время работы;
в) записи особо ценных прикладных программ;
г) хранения постоянно используемых программ;
д) постоянного хранения особо ценных документов.
е) другое

19. Процесс хранения информации на внешних носителях принципиально отличается от процесса хранения информации в оперативной памяти:
а) тем, что на внешних носителях информация может храниться после отключения питания компьютера;
б) объемом хранимой информации;
в) различной скоростью доступа к хранимой информации;
г) возможностью защиты информации;
д) способами доступа к хранимой информации.
е) другое

20. Манипулятор “мышь” — это устройство:

а) модуляции и демодуляции;
б) считывания инфоромации;
в) долговременного хранения информации;
г) ввода информации;
д) для подключения принтера к компьютеру.
е) другое

21. С использованием команды MD в MS DOS создается:
а) текстовый файл;
б) командный файл;
в) пустой каталог;
г) совокупность каталогов;
д) файл IO.SYS.
е) другое

22. Одной из основных характеристик компьютера является быстродействие, которое характеризуется:

а) количеством операций в секунду;
б) количеством выполняемых одновременно программ;
в) временем организации связи между АЛУ и ОЗУ;
г) количеством вводимых символов;
д) количеством подключенных устройств;
е) другое

23. Имя и тип файла разделяются между собой:
а) символом “ . ”;
б) символом “ - ”;
в) пробелом
г) символом “*”
д) символом « _ »
е) другое

24Скорость работы компьютера зависит от:
а) тактовой частоты обработки информации в процессоре;
б) наличия или отсутствия подключенного принтера;
в) организации интерфейса операционной системы;
г) объема внешнего запоминающего устройства;
д) объема обрабатываемой информации.
е) другое

25 Во время исполнения прикладная программа хранится:
а) в видеопамяти;
б) в процессоре;
в) в оперативной памяти;
г) на жестком диске;
д)в ПЗУ.
е) другое

Модуль 2

1.Компьютер — это:
а) устройство для работы с текстами;
б) электронное вычислительное устройство для обработки чисел;

в) устройство для хранения информации любого вида;
г) многофункциональное электронное устройство для работы с информацией;
д) устройство для обработки аналоговых сигналов.
е) другое

2. Постоянное запоминающее устройство служит для:
а) хранения программ начальной загрузки компьютера и тестирования его узлов;
б) хранения программы пользователя во время работы;
в) записи особо ценных прикладных программ;
г) хранения постоянно используемых программ;
д) постоянного хранения особо ценных документов.
е) другое

3. Процесс хранения информации на внешних носителях принципиально отличается от процесса хранения информации в оперативной памяти:
а) тем, что на внешних носителях информация может храниться после отключения питания компьютера;
б) объемом хранимой информации;
в) различной скоростью доступа к хранимой информации;
г) возможностью защиты информации;
д) способами доступа к хранимой информации.
е) другое

4. Манипулятор “мышь” — это устройство:
а) модуляции и демодуляции;
б) считывания инфоромации;
в) долговременного хранения информации;
г) ввода информации;
д) для подключения принтера к компьютеру.
е) другое

5. С использованием команды MD в MS DOS создается:
а) текстовый файл;
б) командный файл;
в) пустой каталог;
г) совокупность каталогов;
д) файл IO.SYS.
е) другое

6. Одной из основных характеристик компьютера является быстродействие, которое характеризуется:

а) количеством операций в секунду;
б) количеством выполняемых одновременно программ;
в) временем организации связи между АЛУ и ОЗУ;
г) количеством вводимых символов;
д) количеством подключенных устройств;
е) другое

7. Имя и тип файла разделяются между собой:
а) символом “ . ”;
б) символом “ - ”;
в) пробелом

г) символом “*”
д) символом « _ »
е) другое

8Скорость работы компьютера зависит от:
а) тактовой частоты обработки информации в процессоре;
б) наличия или отсутствия подключенного принтера;
в) организации интерфейса операционной системы;
г) объема внешнего запоминающего устройства;
д) объема обрабатываемой информации.
е) другое

9 Во время исполнения прикладная программа хранится:
а) в видеопамяти;
б) в процессоре;
в) в оперативной памяти;
г) на жестком диске;
д)в ПЗУ.
е) другое

10Для подключения компьютера к телефонной сети используется:
а) модем;
б) факс;
в) сканер;
г) принтер;
д) монитор.
е) другое

11Расширение имени файла, как правило, характеризует:
а) время создания файла;
б) объем файла;
в) место, занимаемое файлом на диске;
г) тип информации, содержащейся в файле;
д) место создания файла.
е) другое

12 Команда COPY предназначена для копирования в MS DOS:
а) файлов и каталогов;
б) только текстовых файлов;
в) только каталогов;
г) только командных файлов;
д) утилит MSDOS.
е) другое

13 . Максимальная длина двоичного кода, который может обрабатываться или передаваться процессором целиком:
а) Кэш;
б) BIOS;
в) Разрядность;
г) Тактовая частота
д) Контроллер;
е) другое

14 . В какой из последовательностей единицы измерения информации указаны в порядке возрастания:

а)байт, килобайт, мегабайт, бит;
б)килобайт, байт, бит, мегабайт;
в)байт, мегабайт, килобайт, гигабайт;
г)мегабайт, килобайт, гигабайт, байт;
д)байт, килобайт, мегабайт, гигабайт. е) другое.

15 .Винчестер предназначен для:

а) подключения периферийных узлов к магистрали;
б) управления работой ЭВМ по заданной программе;
в)хранения информации;

16 Память, используемая для хранения ьольших объемов информации:

а) оперативная память;
б) гибкий магнитный диск;
в) постоянная память (ПЗУ);

17 Микропроцессор имеет в своем составе:

а) устройство ввода;
б) внутренние регистры;
в) арифметико-логическое устройство;

18. Как называется умышленно искаженная информация?
а)Дезинформация
б)Информативный поток
в) Достоверная информация
г) Перестает быть информацией
19. Как называется информация, к которой ограничен доступ?
а Конфиденциальная
б Противозаконная
в Открытая
г Недоступная
20. Какими путями может быть получена информация?
а. проведением, покупкой и противоправным добыванием информации научных исследований
б. захватом и взломом ПК информации научных исследований
в. добыванием информации из внешних источников и скремблированием информации научных исследовании
г. захватом и взломом защитной системы для информации научных исследований
21. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
а. защищенные КС
б.небезопасные КС
в. Само достаточные КС
г.Саморегулирующиеся КС
22.Основной документ, на основе которого проводится политика информационной безопасности?
а. программа информационной безопасности

Б. регламент информационной безопасности
в. политическая информационная безопасность
г. Протекторат
В зависимости от формы представления информация может быть разделена на?
а. Речевую, документированную и телекоммуникационную
б. Мысль, слово и речь
в. цифровая, звуковая и тайная
г. цифровая, звуковая
23. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации
а. Информационным процессам
б. Мыслительным процессам
в. Машинным процессам
г. Микропроцессам
24.Что называют защитой информации?
а. Все ответы верны
б. Называют деятельность по предотвращению утечки защищаемой информации
в. Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
г. Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
25. Под непреднамеренным воздействием на защищаемую информацию понимают?
а. Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
б. Процесс ее преобразования, при котором содержание информации изменяется на ложную
в. Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
г. Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Модуль 3

1.Шифрование информации это
а. Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
б. Процесс преобразования, при котором информация удаляется
в. Процесс ее преобразования, при котором содержание информации изменяется на ложную
г. Процесс преобразования информации в машинный код

2.Основные предметные направления Защиты Информации?
а. охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
б. Охрана золотого фонда страны
в.Определение ценности информации
г. Усовершенствование скорости передачи информации

3. Государственная тайна это
а. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
б. ограничения доступа в отдельные отрасли экономики или на конкретные производства
в. защищаемые банками и иными кредитными организациями сведения о банковских операциях

г. защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

4. Коммерческая тайна это….
а. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
б. ограничения доступа в отдельные отрасли экономики или на конкретные производства
в.. защищаемые банками и иными кредитными организациями сведения о банковских операциях
г. защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

5.Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
а. Тайна связи
б. Нотариальная тайна
в. Адвокатская тайна
г. Тайна страхования

6.Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

7.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
а. управление доступом
б. конфиденциальность
в. аутентичность
г. целостность

8. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

9.Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных
а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

10. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

11.Какая из перечисленных атак на поток информации является пассивной:
а. перехват.
б. имитация.
в. модификация.
г. фальсификация.
д. прерывание.

12.Технические каналы утечки информации делятся на…
а. Все перечисленное
б. Акустические и виброакустические
в. Электрические
г. Оптические

13. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

14. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

15. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

16.Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

17.По сведениям Media и PricewaterhouseCoopers, на чью долю приходится 60% всех инцидентов IT-безопасности?
а. Хакерские атаки
б. Различные незаконные проникновения
в. Инсайдеры
г. Технические компании

18. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?
а. Индивидуальный подход к защите
б. Комплексный подход к защите
в. Смешанный подход к защите
г. Рациональный подход к защите

19.Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
а. Информационная безопасность
б. Защитные технологии
в. Заземление
г. Конфиденциальность

20.Можно выделить следующие направления мер информационной безопасности
а. Правовые
б. Организационные
в. Все ответы верны
г. Технические

21.Что можно отнести к правовым мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
б. охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
г. охрану вычислительного центра, установку сигнализации и многое другое

22.Что можно отнести к организационным мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
б.Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
г. Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
д.Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

23.Что можно отнести к техническим мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
б. Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
г. Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов.

24. Потенциальные угрозы, против которых направлены технические меры защиты информации
а. Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
а. Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения
б. Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
в. Потери информации из-за не достаточной установки сигнализации в помещении.
г. Процессы преобразования, при котором информация удаляется

25.Шифрование информации это
а. Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
б. Процесс преобразования, при котором информация удаляется
в. Процесс ее преобразования, при котором содержание информации изменяется на ложную
г. Процесс преобразования информации в машинный код

Модуль 4

1.Для подключения компьютера к телефонной сети используется:
а) модем;
б) факс;
в) сканер;
г) принтер;
д) монитор.
е) другое

2.Расширение имени файла, как правило, характеризует:
а) время создания файла;
б) объем файла;
в) место, занимаемое файлом на диске;
г) тип информации, содержащейся в файле;
д) место создания файла.
е) другое

3. Команда COPY предназначена для копирования в MS DOS:
а) файлов и каталогов;

б) только текстовых файлов;
в) только каталогов;
г) только командных файлов;
д) утилит MS DOS.
е) другое
4 . Максимальная длина двоичного кода, который может обрабатываться или передаваться процессором целиком:
а) Кэш;
б) BIOS;
в) Разрядность;
г) Тактовая частота
д) Контроллер;
е) другое

5. В какой из последовательностей единицы измерения информации указаны в порядке возрастания:
а)байт, килобайт, мегабайт, бит;
б)килобайт, байт, бит, мегабайт;
в)байт, мегабайт, килобайт, гигабайт;
г)мегабайт, килобайт, гигабайт, байт;
д)байт, килобайт, мегабайт, гигабайт. е) другое.

6 .Винчестер предназначен для:

а) подключения периферийных узлов к магистрали;
б) управления работой ЭВМ по заданной программе;
в)хранения информации;

7 Память, используемая для хранения ьольших объемов информации:

а) оперативная память;
б) гибкий магнитный диск;
в) постоянная память (ПЗУ);

8. Микропроцессор имеет в своем составе:

а) устройство ввода;
б) внутренние регистры;
в) арифметико-логическое устройство;

9.Что можно отнести к правовым мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
б. охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов,

установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
г. охрану вычислительного центра, установку сигнализации и многое другое

10.Что можно отнести к организационным мерам ИБ?
а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
б.Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
в. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
г. Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
д.Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.
11. Под replay-атакой понимается:
1. модификация передаваемого сообщения
2. повторное использование переданного ранее сообщения
3. невозможность получения сервиса законным пользователем

12. Уровень секретности - это
1. ответственность за модификацию и НСД информации
2. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

6. Что такое несанкционированный доступ (нсд)?
1. Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2.Создание резервных копий в организации
3. Правила и положения, выработанные в организации для обхода парольной защиты
4. Вход в систему без согласования с руководителем организации

13К посторонним лицам нарушителям информационной безопасностиотносится:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.

14. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
1. Безопасная OECD
2. ISO\IEC
3. OECD
4. CPTED

15.. Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

16. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

17. Анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности – это?

1. Протоколирование
2. Экранирование
3. Аудит

18. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений

19.Какая из перечисленных атак на поток информации является пассивной:

а. перехват.
б. имитация.
в. модификация.
г. фальсификация.
д. прерывание.

20.Технические каналы утечки информации делятся на…

а. Все перечисленное
б. Акустические и виброакустические
в. Электрические
г. Оптические

21. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

22. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

а. Акустические и виброакустические
б. Электрические
в. Оптические

г. Радиоканалы
23. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы
24.Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?
а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы
25.По сведениям Media и PricewaterhouseCoopers, на чью долю приходится 60% всех инцидентов IT-безопасности?
а. Хакерские атаки
б. Различные незаконные проникновения
в. Инсайдеры
г. Технические компании

Критерии и методика оценивания:

Один тестовый вопрос (25 вопросов).

- 0,6 балла выставляется студенту, если ответ правильный;
- 0 баллов выставляется студенту, если ответ неправильный.

Типовые материалы к экзамену

Экзаменационные вопросы:

1 Угрозы безопасности информации и меры по их предотвращению.
2 Видовые демаскирующие признаки объектов в видимом и инфракрасном диапазонах света.
3. Демаскирующие признаки аналоговых сигналов
4. Типовая структура технического канала утечки информации.
5. Концепция и методы технической защиты информации
6. Понятие экранирования. Основные положения
7.Контроль защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.
8.Демаскирующие признаки дискретных сигналов
9.Технический контроль акустической защищенности выделенного помещения.
10.Материально-вещественный канал утечки информации. Способы восстановления информации на магнитных носителях.
11. Аттестация объектов информатизации. Мероприятия по выявлению и оценке свойств каналов утечки .
12.Технический контроль акустической защищенности выделенного помещения.
13.Контроль технических средств и систем .
14.Принципы построения системы ТЗИ: равнопрочность рубежей, непрерывность, подконтрольность и гибкость системы защиты
15.Утечка информации по цепям электропитания
16. Технический контроль акустической защищенности выделенного помещения.
17.Акустический и виброакустический контроль
18.Низкочастотные и высокочастотные излучения технических средств

19.Виды технических каналов утечки информации
20.Оптические каналы утечки информации
21.Скрытие и защита от утечки информации по акустическому и виброакустическому каналам.
22.Анализаторы линий и устройства контроля проводных линий
23.Демаскирующие признаки дискретных сигналов .
24.Электромагнитные излучения распределенных источников.
25.Виды технических каналов утечки информации
26.Оптические каналы утечки информации
27.Принципы построения системы ТЗИ: равнопрочность рубежей, непрерывность, подконтрольность и гибкость системы защиты
28.Утечка информации по цепям электропитания
29.Технический контроль акустической защищенности выделенного помещения.
30.Аттестация объектов информатизации
31.Концепция и методы инженерно-технической защиты информации
32. Понятие экранирования. Основные положения
33.Демаскирующие признаки аналоговых сигналов
34.Типовая структура технического канала утечки информации.
35 Принципы построения системы ТЗИ: многозональность и многорубежность
36.Способы защиты информации с помощью технологии Proximity и смарт-карт
37.Технические каналы утечки информации. Структура и классификация.
38. Электромагнитный канал утечки информации .
39.Методы выявления закладных устройств.
40.Пассивные методы защиты речевой информации от её утечки через ограждающие конструкции. Рекомендации по выбору ограждающих конструкций.
41 Активные методы и средства защиты речевой информации от утечки по техническим каналам, Характеристика генераторов шума.
42.Методы и средства защиты информации в телефонных линиях связи.

Структура экзаменационного билета

Экзаменационный билет состоит из двух теоретических вопросов.

Пример экзаменационного билета:

Федеральное государственное бюджетное образовательное учреждение высшего образования
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт истории и государственного управления

Направление подготовки 10.03.01 «Информационная безопасность»
Дисциплина Системы инженерно-технической защиты информации

1 Угрозы безопасности информации и меры по их предотвращению.
2 Видовые демаскирующие признаки объектов в видимом и инфракрасном диапазонах света.

Зав. кафедрой УИБ А.С. Исмагилова

Федеральное государственное бюджетное образовательное учреждение высшего образования

Направление подготовки 10.03.01 «Информационная безопасность»
Дисциплина Системы инженерно-технической защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Демаскирующие признаки аналоговых сигналов
2. Типовая структура технического канала утечки информации.

Зав. кафедрой УИБ А.С. Исмагилова

Критерии оценивания результатов экзамена

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний. Студент не смог ответить ни на один дополнительный вопрос.

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Скрипник Д. А. Общие вопросы технической защиты информации: Учебная литература для ВУЗов [Электронный ресурс/ Москва: Национальный Открытый Университет «ИНТУИТ», 2016.- 425 стр. Режим доступа // http:// http://biblioclub.ru/index.php?page=book_red&id=429070&sr=1
2. Голиков А. М. Защита информации от утечки по техническим каналам: учебное пособие[Электронный ресурс] Томский государственный университет систем управления и радиоэлектроники, 2015. -256с. Режим доступа //http:/ http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1

Дополнительная литература

3. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие [Электронный ресурс] Томский государственный университет систем управления и радиоэлектроники, 2015. -256с. Режим доступа //http:/ http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1
4. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие[Электронный ресурс] Москва: Издательский дом Высшей школы экономики, 2015 .-574с. -Режим доступа http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video– Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус),	Лекции, практические занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV(XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера,	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2.Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3.Сисстема централизованного тестирования БашГУ (Moodle).GNU General Public License.

аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **4.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Системы инженерно-технической защиты информации

на 4 семестр

Вид работы	Объем дисциплины 4
Общая трудоемкость дисциплины (ЗЕТ / часов)	108
Учебных часов на контактную работу с преподавателем:	33,2
лекций	16
практических / семинарских	16
лабораторных работ	
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	22 52,8

Форма контроля
Экзамен 4 семестр

на 5 семестр

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	108
Учебных часов на контактную работу с преподавателем:	37,2
лекций	18
практических / семинарских	18
лабораторных работ	
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	36 34,8

Форма контроля
Экзамен 5 семестр

4 семестр

	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
			ЛК	ПР / Сем	ЛР	СРС			
1	2		4	5	6	7	8	9	10
	Модуль 1,2. Объекты информационной защиты		4	4		7	Основная 1, 2. Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Опрос, практические задания, тестирование
2	Основные свойства информации как предмета инженерно-технической защиты		4	4		5	Основная 1, 2.	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, тестирование
3	Источники и носители конфиденциальной информации		4	4		5	Дополнительная 3,4	Выполнение практической работы	Опрос, практические задания, тестирование

	Виды угроз безопасности информации								
4	Способы и средства инженерной защиты и технической охраны		4	4		5	Основная 1, 2.	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, тестирование
	Всего		16	16		22			

5 семестр

	Тема и содержание		Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
			ЛК	ПР / Сем	ЛР	СРС			
1	2		4	5	6	7	8	9	10
5	Модуль 3,4. Способы и средства предотвращения утечки информации через побочные		2	2		8	Основная 1, 2. Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Опрос, практические задания, тестирование

	электромагнитные излучения и наводки								
6	Способы предотвращения утечки информации по материально-вещественному каналу		4	4		7	Основная 1, 2. Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Опрос, практические задания, тестирование
7	Общие положения по инженерно-технической защите информации в организации		4	4		7	Основная 1, 2. Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Опрос, практические задания, тестирование
8	Организационные по инженерно-технической защите информации в организации		4	4		7	Основная 1, 2. Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Опрос, практические задания, тестирование
9	Технические меры по инженерно-технической защите информации в организации		4	4		7	Основная 1, 2. Дополнительная 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Опрос, практические задания, тестирование
	Всего часов		18	18		36			

Приложение 2

Рейтинг – план дисциплины
Системы инженерно-технической защиты информации

Курс 2, семестр 4

Направление подготовки 10.03.01 «Информационная безопасность»

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			0	20
1. Аудиторная работа	1,5	4	0	6
2. Практические работы	2	7	0	14
Рубежный контроль				15
1. Тестовые задания	0,6	25	0	15
Всего			0	35
Модуль 2				
Текущий контроль			0	20
1. Аудиторная работа	1,5	4	0	6
2. Практические работы	2	7	0	14
Рубежный контроль				15
1. Тестовые задания	0,6	25	0	15
Всего			0	35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30

Рейтинг – план дисциплины
Системы инженерно-технической защиты информации

Курс 3, семестр 5

Направление подготовки 10.03.01 «Информационная безопасность»

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3				

Текущий контроль			0	20
1. Аудиторная работа	1,5	4	0	6
2. Практические работы	2	7	0	14
Рубежный контроль				15
1. Тестовые задания	0,6	25	0	15
Всего			0	35
Модуль 4				
Текущий контроль			0	20
1. Аудиторная работа	1,5	4	0	6
2. Практические работы	2	7	0	14
Рубежный контроль				15
1. Тестовые задания	0,6	25	0	15
Всего			0	35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
3. Посещение лекционных занятий				-6
4. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30