МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
О.Н. Выборнова
«05» мая 2025 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой
информационной безопасности
В.А. Черкасова
«05» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ(МОДУЛЯ)
Введение в инженерную деятельность

Составитель(-и)	**Гурская Т.Г., к.т.н., доцент кафедры информационной безопасности**
Согласовано с работодателям	**Барсуков В.А., начальник отдела информационной безопасности Управления корпоративной защиты ООО «Газпром добыча Астрахань»**
Направление подготовки	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**«Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная/ очно-заочная**
Год приема (курс)	**2025**
Курс	**1 (по всем формам обучения)**
Семестры	**1 (по всем формам обучения)**

Астрахань, 2025

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ(МОДУЛЯ)

1.1. Цели освоения дисциплины (модуля): формирование первых, основополагающих знаний, умений, навыков и компетенций у студентов в области выбранного профиля подготовки

1.2. Задачи освоения дисциплины (модуля):

- научить студентов осуществлять сбор научно-технической информации,

- научить студентов обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

Учебная дисциплина (модуль) «Введение в инженерную деятельность» относится к части, формируемая участниками образовательных отношений и осваивается в 1 семестре.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями): знания базовых понятий информатики и вычислительной техники и навыки работы на персональном компьютере на начальном уровне, приобретенные при изучении школьного курса «ИНФОРМАТИКА И ИКТ».

Знания: основных понятий информатики, структуры систем документационного обеспечения.

Умения: использовать программные и аппаратные средства персонального компьютера, пользоваться нормативными документами по защите информации.

Навыки и (или) опыт деятельности: навыки поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): методика и техника составления различных управленческих и документов учреждений, организаций и предприятий.

2.3.Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

Организационное и правовое обеспечение информационной безопасности.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) профессиональных (ПК): ПК 5 – Способен администрировать средства защиты информации в компьютерных системах и сетях.

Таблица 1. Декомпозиция результатов обучения

Код компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
ПК 5	ПК 5 – Способен администрировать средства защиты информации в	– источники угроз информационной безопасности в компьютерных	– анализировать угрозы безопасности информации в	– методикой оценки оптимальности выбора программно-аппаратных средств защиты информации

	компьютерных системах и сетях.	сетях и меры по их предотвращению	компьютерных системах и сетях	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 4 зачетные единицы (144 часа).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной формы обучения приведена в таблице 2.1.

Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
Объем дисциплины в зачетных единицах	4	4
Объем дисциплины в академических часах	144	144
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):	73	19
- занятия лекционного типа, в том числе:	36	0
- практическая подготовка (если предусмотрена)		0
- занятия семинарского типа (семинары, практические, лабораторные), в том числе:	36	18
- практическая подготовка (если предусмотрена)	2	2
- консультация (предэкзаменационная)		
- промежуточная аттестация по дисциплине	0,25	0,25
Самостоятельная работа обучающихся (час.)	70,75	124,75
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	экзамен – 1 семестр	экзамен – 1 семестр

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы представлены в таблице 2.2.

Таблица 2.2. Структура и содержание дисциплины (модуля)

для очной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 1. Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного	4				4			6	14	Опрос по теме.

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
стандарта по направлению										
Тема 2. Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.).Организация защиты информации в Российской Империи в XVIII - XIX вв.	4				4			8	16	Опрос по теме. Отчет по практическому заданию 1. Отчет по практическому заданию 2.
Тема 3. Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования.	4				4			8	16	Опрос по теме. Отчет по практическому заданию 3. Контрольная работа 1. Тест 1.
Тема 4. История развития систем защиты информации в зарубежных странах.	4				4			8	16	Опрос по теме. Отчет по практическому заданию 4.
Тема 5. Организация системы защиты информации в США и в странах Евросоюза.	4				4			8	16	Опрос по теме. Отчет по практическому заданию 5. Отчет по практическому заданию 6
Тема 6. Организация системы защиты информации в Японии и в Китае.	4				4			8	16	Опрос по теме. Отчет по практическому заданию 7.

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 7. Стандарты информационной безопасности.	4				4			8	16	Опрос по теме. Отчет по практическому заданию 8. Защита реферата.
Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.	4				4	2		8	16	Опрос по теме. Контрольная работа 2.
Тема 9. Международное сотрудничество в области обеспечения информационной безопасности	4				4			8,75	16	Опрос по теме. Тест 2.
Консультации									***1***	
Контроль промежуточной аттестации									**0,25**	**экзамен**
ИТОГО за семестр:	***36***				***36***	***2***		***70, 75***	***144***	

для очно-заочной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации *[по семестрам]*
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП	КР / КП			
Тема 1. Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного стандарта по направлению					2			12	14	Опрос по теме.

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации *[по семестрам]*
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП	КР / КП			
Тема 2. Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.).Организация защиты информации в Российской Империи в XVIII - XIX вв.					2			14	16	Опрос по теме. Отчет по практическому заданию 1. Отчет по практическому заданию 2.
Тема 3. Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования.					2			14	16	Опрос по теме. Отчет по практическому заданию 3. Контрольная работа 1. Тест 1.
Тема 4. История развития систем защиты информации в зарубежных странах.					2			14	16	Опрос по теме. Отчет по практическому заданию 4.
Тема 5. Организация системы защиты информации в США и в странах Евросоюза.					2			14	16	Опрос по теме. Отчет по практическому заданию 5. Отчет по практическому заданию 6
Тема 6. Организация системы защиты информации в Японии и в Китае.					2			14	16	Опрос по теме. Отчет по практическому заданию 7.
Тема 7. Стандарты информационной безопасности.					2			14	16	Опрос по теме. Отчет по практическ

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации *[по семестрам]*
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП	КР / КП			
										ому заданию 8. Защита реферата.
Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.					2	2		14	16	Опрос по теме. Контрольная работа 2.
Тема 9. Международное сотрудничество в области обеспечения информационной безопасности					2			14,75	16	Опрос по теме. Тест 2.
Консультации									***1***	
Контроль промежуточной аттестации									**0,25**	**экзамен**
ИТОГО за семестр:					***18***	***2***		***124, 75***	***144***	

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; КПА – контроль промежуточной аттестации; КС – консультации; СР – самостоятельная работа

[При заполнении таблиц 2.2. необходимо учесть следующее:

- заполняются таблицы только по реализуемым формам обучения;
- общий объем часов на каждую тему (раздел) для разных форм обучения должен быть одинаковым;
- практическая подготовка по видам учебных занятий распределяется разработчиком РПД по темам самостоятельно в пределах часов, выделенных в учебном плане на данную дисциплину;
- самостоятельная работа по каждой теме вычисляется как разность между общим объемом часов, выделенных на тему, и количеством часов, выделенных на сумму всех видов контактной работы;
- при подсчете консультаций необходимо учесть, что в случае наличия экзамена по дисциплине проводится одночасовая консультация; разбивать часы на консультации по разделам не нужно;
- при написании курсовой работы на контактную работу с преподавателем отводится 2 часа, объем самостоятельной работы студента на курсовую работу определяется разработчиком; разбивать часы на подготовку курсовой работы по разделам и (или) темам не нужно;
- контроль промежуточной аттестации вносится в соответствующую графу и столбец, разбивать часы на КПА по разделам не нужно.

Далее в данном пункте программы размещается матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых в них компетенций]

Таблица 3. Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции	Общее количество компетенций
		ПК5	
Тема 1. Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного стандарта по направлению	14	+	1
Тема 2. Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.).Организация защиты информации в Российской Империи в XVIII - XIX вв.	16	+	1
Тема 3. Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования.	16	+	1
Тема 4. История развития систем защиты информации в зарубежных странах.	16	+	1
Тема 5. Организация системы защиты информации в США и в странах Евросоюза.	16	+	1
Тема 6. Организация системы защиты информации в Японии и в Китае.	16	+	1
Тема 7. Стандарты информационной безопасности.	16	+	1
Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.	16	+	1
Тема 9. Международное сотрудничество в области обеспечения информационной безопасности	16	+	1
ИТОГО	144		

Краткое содержание каждой темы дисциплины (модуля)

Тема 1. Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного стандарта по направлению

Сущность направления подготовки «Информационная безопасность», характеристика ее составляющих. Место и значение направления подготовки в системе специальностей по направлению подготовки «Информационная безопасность».

Назначение и структура Федерального государственного образовательного стандарта по направлению подготовки.

Тема 2. Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.). Организация защиты информации в Российской Империи в XVIII - XIX вв.

Образование Российского государства. Формирование органов государственного управления. Возникновение необходимости защиты информации в области военной, внешне- и внутриполитической деятельности государства. Складывание элементов защиты информации.

Функции Боярской думы в области внешней и внутренней политики и обеспечения безопасности государства. Система обеспечения безопасности и «опричнина». Основные функции в области обеспечения внешней и внутренней безопасности государства и защиты информации Разрядного, Оружейного, Казенного, Посольского приказов.

Методы защиты информации от иностранных государств. Ограничения на въезд в Россию. Царский «тайный совет». Учреждение Приказа тайных дел. Его функции.

Вопросы защиты информации в Судебниках 1497 и 1550 гг.

Значение для становления системы защиты государственной тайны Соборного Уложения 1649 г. Ответственность за шпионаж и государственную измену. Ответственность за хищение и подделку документов и печатей.

Развитие торгово-промышленной деятельности. Создание и развитие акционерных компаний. Формирование законодательной основы акционерного предпринимательства.

Организация кредитных отношений. Формирование системы казенных банков. Создание частных банкирских домов. Формирование биржевой деятельности.

Органы защиты информации. Функции в области защиты информации Преображенского приказа и Верховного тайного совета. Основные задачи и деятельность Первого и Пятого департаментов Сената. Деятельность Военной Коллегии, Коллегии иностранных дел в области защиты информации. Основные функции Тайной розыскных дел канцелярии, Тайной экспедиции.

Регламентирование вопросов защиты информации в государственных учреждениях. Генеральный регламент 1720 г.

Основные направления и методы защиты информации. Совершенствование шифрованной переписки. Ответственность за разглашение защищаемых сведений.

Функции в области защиты информации Государственного Совета, Комитета министров, Сената. Основные задачи и деятельность Первого и Третьего отделений Собственной его императорского величества канцелярии. Основные функции в области защиты информации Постоянного секретного комитета.

Совершенствование законодательной основы деятельности министерств. «Общее учреждение министерств» от 25 июня 1811 г. Вопросы защиты информации в деятельности Министерства внутренних дел, Министерства полиции, Министерства юстиции, Военного министерства, Министерства финансов, Министерства иностранных дел. Организация и деятельность «черных кабинетов». Органы цензуры.

Правовые основы защиты информации. «Уложение о наказаниях уголовных и исправительных» (1845).

Формирование законодательства Российской империи в области патентного и авторского права. Ответственность за разглашение защищаемых сведений.

Реформа военной промышленности.

Функции Главного управления по делам печати. Деятельность Третьего, Пятого и Шестого делопроизводств Департамента полиции.

Особый отдел Департамента полиции и региональная сеть охранных отделений. Функции в области защиты военно-промышленной тайны Военного и Морского министерств. Функции в области защиты коммерческой тайны Министерства финансов.

Организация защиты информации в учреждениях Российской империи за рубежом. Реформа цензуры (1865). «Временные правила о печати». Дополнения к «Временным правилам о печати» (1873). Положение о привилегиях на изобретения от 20 мая 1896г.

Тема 3. Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования.

Функции в области защиты информации Государственной думы, Государственного Совета, Комитета министров (Совета министров), Министерства внутренних дел, Департамента полиции, Военного министерства, Министерства иностранных дел. Функции Совета государственной обороны. Деятельность «Особого совещания» в области координации важнейших вопросов внутренней политики и государственной безопасности.

Функции в области защиты государственной тайны Главного управления Генерального штаба. Первый отдел Генерального штаба. Деятельность в области защиты информации Министерства внутренних дел, Департамента полиции, Военного министерства, Министерства иностранных дел, Управления дворцового коменданта Министерства императорского двора. Функции по защите информации Петербургского телеграфного агентства. Функции в области защиты коммерческой тайны и предупреждения недобросовестной конкуренции Министерства торговли и промышленности.

Основные направления и методы защиты информации. Защита профессиональной тайны. Защита коммерческой тайны. Состав защищаемой информации. Объекты защиты.

Основные направления и методы защиты информации. Правовые основы защиты информации. Положение об авторском праве от 20 марта 1911 г. Ответственность за разглашение защищаемых сведений.

Функции особого совещания для обсуждения и объединения мероприятий по обороне (1915).

Органы защиты военной тайны. Создание Особого отдела ВЧК и его местных органов. Основные задачи органов военной контрразведки.

Создание и задачи Специального отдела ВЧК – ГПУ – ОГПУ. Ликвидация Специального отдела и создание 7 отдела ГУГБ НКВД СССР, его задачи и функции. Органы защиты государственных секретов в наркоматах, ведомствах и на предприятиях.

Совершенствование методов защиты государственных секретов.

Ответственность за разглашение государственной тайны.

Активизация разведывательной деятельности фашистской Германии. Реорганизация разведывательных служб. Направления и методы добывания информации о военно-экономическом потенциале СССР.

Перечни сведений, составляющих государственную тайну.

Появление новых видов носителей секретной информации, средств и способов ее обработки, хранения и передачи в связи с внедрением АСОД. Расширение угроз защищаемой информации и каналов несанкционированного доступа к ней. Объекты защиты.

Совершенствование методов добывания секретной информации иностранными спецслужбами, появление новых технических средств несанкционированного получения информации. Государственная политика в области защиты информации. Постановления ЦК КПСС и СМ СССР по сохранению государственной тайны и укреплению режима секретности.

Основные положения нормативных документов по обеспечению сохранения государственной тайны. Создание и задачи Центральной межведомственной комиссии по электросвязи.

Постановления ЦК КПСС и СМ СССР 1970, 1976, 1980 гг. по укреплению режима секретности. Нормативные документы по усилению противодействия иностранным техническим разведкам, улучшению охраны объектов, предотвращению утечки информации через публикации и др.

Создание, задачи и функции Государственной технической комиссии. Подразделения режимно-секретных органов предприятий.

Базовые законы в области защиты информации: «О безопасности», «Об информации, информационных технологиях и защите информации».

Отражение вопроса защиты информации в административном, хозяйственном, уголовном и гражданском законодательстве.

Реорганизации органов защиты информации в 90-е гг.

Тема 4. История развития систем защиты информации в зарубежных странах.

Становление систем, формирование основных понятий, выработка принципов, методов, основных подходов и направлений защиты информации.

Особенности опыта организации защиты информации на Древнем Востоке. Истоки разделения и классификации видов тайн. Основные направления защиты государственной тайны. Опыт создания служб безопасности, организация проверок, методика работы с персоналом, классификация личных характеристик, необходимых для сотрудника, владеющего сведениями, которые составляют тайну.

Становление основных направлений, принципов и методов защиты информации в средневековой Европе.

Основные направления совершенствования защиты информации в Новое время. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Опыт криптографической защиты информации в странах Западной Европы. Методы защиты коммерческих сведений. Банковская тайна и особенности ее защиты.

Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в XVIII - начале XX вв.

Формирование правовых и организационных основных основ защиты информации.

Разведка и контрразведка как необходимые элементы политического обеспечения безопасности государств и как факторы взаимного развития и совершенствования.

Промышленный шпионаж: его значение для формирования систем защиты информации. Особенности государственной политики по отношению к промышленному шпионажу в национальных и межгосударственных рамках.

Формирование авторского и патентного права.

Защита информации, содержащейся в торговых книгах, в XIX - начале XX в. (на примере Германии, Франции, Италии, Голландии, Австрии, Венгрии). Особенности формирования современных систем защиты информации в ведущих зарубежных странах в XX в.

Влияние исторического опыта защиты информации на последующее формирование и развитие современных основ защиты информации в зарубежных странах.

Тема 5. Организация системы защиты информации в США и в странах Евросоюза.

Особенности государственного устройства США. Состояние проблемы информационной безопасности в странах Евросоюза (Великобритании, Северной Ирландии, Германии, Франции, Швеции.

Государственная политика в области защиты информации

Организация защиты информации по национальной безопасности (государственных секретов).

Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности. Структура разведывательного сообщества и его роль в осуществлении политики защиты информации по национальной безопасности.

Особенности организации защиты информации в национальной промышленности.

Защита секретной информации, используемой в международных программах.

Защита информации в ходе деловых визитов и встреч.

Классификация защищаемой информации. Состав грифов ограничения доступа к документам. Право первоначальной классификации информации. Состав информации, не подлежащей классификации по степени секретности. Порядок изменения степени секретности.

Организация доступа к грифованной информации. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Обязанности руководителей ведомств, разрешающих доступ служащих к секретным документам. Обязанности служащих, имеющих право на доступ к грифованной информации. Особенности организации работы с секретной научно-технической информацией.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к информации по национальной безопасности.

Правовые основы защиты информации по национальной безопасности.

Организация защиты коммерческой тайны.

Функции по защите коммерческой тайны частных охранно-сыскных агентств и служб промышленной и коммерческой безопасности. Государственный контроль за их деятельностью. Координация деятельности частных агентств безопасности и правоохранительных органов. Создание системы координации национальной безопасности предпринимательской деятельности. Ассоциации охранно-сыскных агентств и служб безопасности, особенности их деятельности и функции в области защиты информации.

Организация и основные направления деятельности служб безопасности фирм.

Классификация информации, составляющей коммерческую тайну.

Доступ к информации, принадлежащей частным лицам.

Разработка программы защиты информации. Обязательный перечень защитных мер. Организация профилактических мероприятий.

Регламентация процедур обеспечения защиты коммерческой тайны.

Защита документального обеспечения деятельности фирм.

Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к информации, составляющей коммерческую тайну фирмы.

Тема 6. Организация системы защиты информации в Японии и в Китае.

Особенности государственного устройства в Японии. Государственная политика в области защиты информации в Японии. Особенности процесса формирования системы защиты информации в Китае.

Организация системы специальных служб и их основные функции в области защиты информации.

Состав, структура и основные направления деятельности специальных служб безопасности. Частные сыскные бюро, частные фирмы охраны и безопасности и их функции в сфере защиты информации. Ассоциации служб охраны и безопасности. Общественные организации, оказывающие помощь органам полиции в сфере защиты

экономической информации (территориальные советы по предупреждению преступности, общества содействия полиции, пункты связи по предупреждению преступности). Службы безопасности отдельных организаций. Подразделения внутреннего самоконтроля отдельных организаций и их функции в сфере защиты информации. Основные функции служб безопасности. Методы и основные направления совершенствования работы служб безопасности.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации.

Организация защиты информации. Принцип корпоративной защиты и обеспечения безопасности объекта. Защита информации в процессе взаимодействия фирм с иностранными партнерами.

Классификация защищаемой информации.

Правовые основы защиты информации.

Представление об информационном противоборстве в Китае. «Великая стена» информационной безопасности Китая.

Тема 7. Стандарты информационной безопасности.

Предпосылки создания стандартов информационной безопасности

Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт B7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT.

Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.

Состав защищаемой информации в России и за рубежом.

Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ.

Регулирование состава защищаемой информации законом «О государственной тайне».Перечень сведений, составляющих государственную тайну. Указ Президента Российской Федерации от 30.11.95 № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне». Сведения, которые не могут быть отнесены к государственной тайне.Правовое регулирование состава информации, относимой к государственной тайне.Постановление Правительства Российской Федерации от 04.09.95 № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

Закон РФ «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ.Правовое регулирование состава информации, относимой к коммерческой тайне. Постановление Правительства Российской Федерации от 05.12.91 «О перечне сведений, которые не могут составлять коммерческую тайну».

Нормативное регулирование зашиты информации, составляющей служебную, профессиональную и личную тайну.Указ Президента Российской Федерации от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера».

Полномочия органов законодательной власти, Президента РФ, правительства, органов исполнительной и судебной власти в области защиты информация.

Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны.

Указ Президента Российской Федерации от 19.02.99 № 212 «Положение о Государственной технической комиссии при Президенте Российской Федерации».

Полномочия Государственной технической комиссии и Федерального агентства правительственной связи и информации в области защиты информации.Указ Президента Российской Федерации от 24.12.91 № 313 «О создании Федерального агентства правительственной связи и информации при Президенте Российской Федерации».

Полномочия органов Федеральной службы безопасности, Министерства обороны, Министерства внутренних дел, Министерства иностранных дел, Службы внешней разведки в области защиты информации.Указ Президента Российской Федерации об утверждении Положения о Федеральной службе безопасности Российской Федерации от 23.06.95 № 633. Закон РФ «О безопасности». Закон РФ «О внешней разведке». Закон Российской Федерации от 22.02.95 «Об органах Федеральной службы безопасности в Российской Федерации».

Полномочия предприятий в области защиты информации.

Особенности концепции национальной безопасности России.

Тема 9. Международное сотрудничество в области обеспечения информационной безопасности

Научно-техническое сотрудничество с зарубежными партнерами.

Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов. Система контроля.

Порядок предоставления защищаемой информации другим странам.

Международный опыт защиты информации в процессе банковской деятельности.

Международный опыт стандартизации в области защиты информации.

Международная защита интеллектуальной собственности.

Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Договор об образовании Европейского экономического общества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю):

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой (основной) из п.8.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой (дополнительной) из п.8.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-ресурсами.

Таблица 4. Содержание самостоятельной работы обучающихся

для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	*Кол-во часов*	*Формы работы*
Сущность направления подготовки «Информационная безопасность», характеристика ее составляющих. Объекты профессиональной деятельности бакалавра.	6	Внеаудиторная, изучение учебных пособий
Изучить материалы Судебников 1497 и 1550 гг., Соборного Уложения 1649 г. и определить меры ответственности за	8	Внеаудиторная, изучение

шпионаж, государственную измену, нарушение внутренней безопасности государства, хищение и подделку документов и печатей.		учебных пособий
Регламентирование вопросов защиты информации в государственных учреждениях, содержащихся в «Генеральном регламенте» 1720 г., «Общем учреждении министерств» 1811 г., «Уложения о наказаниях уголовных и исправительных» 1845 г., «Положения о военном министерстве» 1869 г. Определить состав, структуру, основные направления деятельности центральных учреждений Российской империи, выполняющих функции в области защиты информации и порядок установления ответственности за преступления в области защиты	8	Внеаудиторная, изучение учебных пособий
Определить состав, структуру, основные направления деятельности центральных учреждений Российской Федерации, выполняющих функции в области защиты информации	8	Внеаудиторная, изучение учебных пособий
Сравнительный анализ зарубежных аналогов российских технических средств	8	Внеаудиторная, изучение учебных пособий
Сравнительный анализ нормативного обеспечения криптографической защиты в России и зарубежных странах	8	Внеаудиторная, изучение учебных пособий
Сравнительный анализ обеспечения и реализации в России и зарубежных странах современных криптографических алгоритмов	8	Внеаудиторная, изучение учебных пособий
Сравнительный анализ российских и зарубежных служб обеспечения информационной безопасности	8	Внеаудиторная, изучение учебных пособий
Анализ средств ведения информационно-психологической войны. Анализ международных стандартов в области информационной безопасности	8,75	Внеаудиторная, изучение учебных пособий

для очно-заочной формы обучения

Вопросы, выносимые на самостоятельное изучение	*Кол-во часов*	*Формы работы*
Сущность направления подготовки «Информационная безопасность», характеристика ее составляющих. Объекты профессиональной деятельности бакалавра.	12	Внеаудиторная, изучение учебных пособий
Изучить материалы Судебников 1497 и 1550 гг., Соборного Уложения 1649 г. и определить меры ответственности за шпионаж, государственную измену, нарушение внутренней безопасности государства, хищение и подделку документов и печатей.	14	Внеаудиторная, изучение учебных пособий

Регламентирование вопросов защиты информации в государственных учреждениях, содержащихся в «Генеральном регламенте» 1720 г., «Общем учреждении министерств» 1811 г., «Уложения о наказаниях уголовных и исправительных» 1845 г., «Положения о военном министерстве» 1869 г. Определить состав, структуру, основные направления деятельности центральных учреждений Российской империи, выполняющих функции в области защиты информации и порядок установления ответственности за преступления в области защиты	14	Внеаудиторная, изучение учебных пособий
Определить состав, структуру, основные направления деятельности центральных учреждений Российской Федерации, выполняющих функции в области защиты информации	14	Внеаудиторная, изучение учебных пособий
Сравнительный анализ зарубежных аналогов российских технических средств	14	Внеаудиторная, изучение учебных пособий
Сравнительный анализ нормативного обеспечения криптографической защиты в России и зарубежных странах	14	Внеаудиторная, изучение учебных пособий
Сравнительный анализ обеспечения и реализации в России и зарубежных странах современных криптографических алгоритмов	14	Внеаудиторная, изучение учебных пособий
Сравнительный анализ российских и зарубежных служб обеспечения информационной безопасности	14	Внеаудиторная, изучение учебных пособий
Анализ средств ведения информационно-психологической войны. Анализ международных стандартов в области информационной безопасности	14,75	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно – подготовка реферата.

Правила оформления текста пояснительной записки реферата

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы реферата, Ф.И.О. студента, номер группы, Ф.И.О. преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

Текстовая часть

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *TimesNewRoman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

Дополнительный *интервал перед* заголовком подраздела – *6 пт, после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

Пример оформления заголовков текста:

1 Разработка аппаратных средств

1.1
1.2
1.3

Нумерация пунктов первого раздела отчета

2 Технические характеристики

2.1
2.2
2.3

Нумерация пунктов второго раздела отчета

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

Перечисления

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом***.**

Примеры написания:
- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
- приложения;
- перечень терминов;
- перечень сокращений;
- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;
б)…;
1)…;
2)…;
в).

Примеры написания:
1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:
а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
б) приложения;
в) перечень терминов;
г) перечень сокращений;
д) перечень литературы.

Сокращения слов

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

Формулы

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными

строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0\left(1 + \frac{\Delta H}{100}\right)^t, \qquad ((3.1)$$

где H_0 – число жителей на время проведения переписи населения, тыс. чел.;

ΔH – средний годовой прирост населения в данной местности, % (принимается 2…3%);

t – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс. чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

Ссылка в тексте на формулу: «…в формуле (3.1)».

Таблицы

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы

Заголовки граф

Подзаголовки граф

Строки (горизонтальные ряды)

Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается.

Графу «Номер по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

Протяженность участка проектируемой трассы, км	Тип кабеля
0,084	ДПС-04-24А06-7,0
0,167	ДПС-04-24А06-7,0
0,301	ДПС-04-24А06-7,0
0,779	ДПС-04-24А06-7,0
Общая длина кабеля: 1,331 км	ДПС-04-24А06-7,0

Примечание – Толщину линий таблицы задайте 1 пт.

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

Дата	Наименование	Стоимость

Рисунки

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

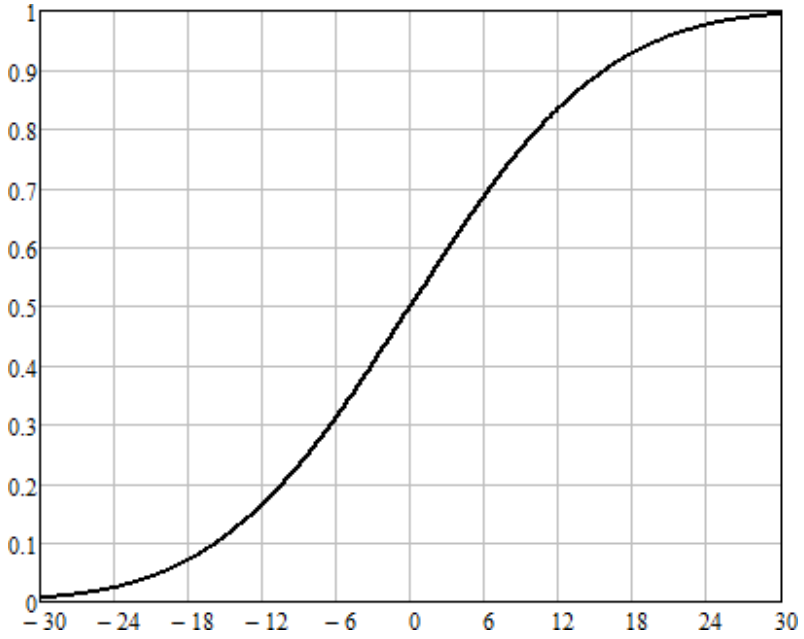

Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».

Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :

Рисунок В.1 – Название рисунка

Список использованных источников

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья :аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкогорегиона :дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

Оформление приложений

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О.

В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении, слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

ПРИЛОЖЕНИЕ А
Диаграмма классов

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

Критерии оценки реферата:

– оценка «отлично» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил реферат или выполнил ее неверно, без использования методических указаний, обоснования неверные, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

Таблица 5. Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Тема 1. Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного стандарта по направлению.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 2. Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.). Организация защиты информации в Российской Империи в XVIII - XIX вв.	Лекция-презентация	Не предусмотрено	выполнение лабораторной работы
Тема 3. Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования.	Лекция-презентация	Не предусмотрено	выполнение лабораторной работы
Тема 4. История развития систем защиты информации в зарубежных странах.	Лекция-презентация	Не предусмотрено	выполнение лабораторной работы
Тема 5. Организация системы защиты информации в США и в странах Евросоюза.	Лекция-презентация	Не предусмотрено	выполнение лабораторной работы
Тема 6. Организация системы защиты информации в Японии и в Китае.	Лекция-презентация	Не предусмотрено	выполнение лабораторной работы
Тема 7. Стандарты информационной безопасности.	Лекция-презентация	Не предусмотрено	выполнение лабораторной работы
Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Тема 9. Международное сотрудничество в области обеспечения информационной безопасности.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы

6.2. Информационные технологии

Название информационной технологии	Темы, разделы дисциплины	Краткое описание применяемой технологии
Использование возможностей Интернета в учебном процессе	1 - 9	Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения)
Использование возможностей электронной почты преподавателя	1 - 9	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1 - 9	Использование мультимедийной презентации

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

-использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));

- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;
- использование возможностей электронной почты преподавателя;
- использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных(традиционных)лекций и семинаров с использованием презентаций и т.д.);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);
- использование виртуальной обучающей среды (или системы управления обучением LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор

Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARKSQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Введение в инженерную деятельность» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6.Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Тема 1. Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного стандарта по направлению	ПК 5	Вопросы для обсуждения.
Тема 2. Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.). Организация защиты информации в Российской Империи в XVIII - XIX вв.	ПК 5	Вопросы для обсуждения. Практическое задание 1. Практическое задание 2.
Тема 3. Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования.	ПК 5	Вопросы для обсуждения. Практическое задание 3. Контрольная работа 1. Тест 1

Тема 4. История развития систем защиты информации в зарубежных странах.	ПК 5	Вопросы для обсуждения. Практическое задание 4.
Тема 5. Организация системы защиты информации в США и в странах Евросоюза.	ПК 5	Вопросы для обсуждения. Практическое задание 5. Практическое задание 6
Тема 6. Организация системы защиты информации в Японии и в Китае.	ПК 5	Вопросы для обсуждения. Практическое задание 7.
Тема 7. Стандарты информационной безопасности.	ПК 5	Вопросы для обсуждения. Практическое задание 8. Реферат
Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.	ПК 5	Вопросы для обсуждения. Контрольная работа 2.
Тема 9. Международное сотрудничество в области обеспечения информационной безопасности	ПК 5	Вопросы для обсуждения. Тест 2.

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

Таблица 7. Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8. Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы

Шкала оценивания	Критерии оценивания
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задания

7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1. «Сущность и значение направления подготовки. Назначение и структура Государственного образовательного стандарта по направлению»

1. Вопросы для обсуждения

1) Сущность направления подготовки «Информационная безопасность», характеристика ее составляющих.
2) Место и значение направления подготовки в системе специальностей по направлению подготовки «Информационная безопасность».
3) Назначение и структура Федерального государственного образовательного стандарта по направлению подготовки.
4) Объекты профессиональной деятельности бакалавра.
5) Виды профессиональной деятельности.
6) Состав задач в области экспериментально-исследовательской, проектной, организационно-управленческой и эксплуатационной деятельности по защите информации, к решению которых должен быть подготовлен бакалавр.

Тема 2.Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.) Организация защиты информации в Российской Империи в XVIII - XIX вв.

Предпосылки формирования системы защиты информации в России (вторая половина XV - XVII вв.)

1. Вопросы для обсуждения

1) Основные особенности формирования политики безопасности государства в Древней Руси (связь с географическим положением государства, особенностями быта и расселения славян, системой градостроительства и другими факторами).
2) Значение первых дипломатических договоров Древней Руси с Византией для формирования нормативной базы защиты информации и развития предпринимательской деятельности.
3) Функции Боярской думы в области внешней и внутренней политики и обеспечения государства. Опричнина и система обеспечения безопасности.
4) Основные функции в области обеспечения внешней и внутренней безопасности государства и защиты информации Разрядного, Оружейного, Казенного, Посольского приказов.

5) Методы защиты информации от иностранных государств. Ограничения на въезд в Россию. Дезинформация. Ограничения на контакты и продвижения послов.
6) Подготовка и хранение «тайных» бумаг. Организация шифрованной переписки. Дипломатические шифры.
7) Царский «тайный совет». Учреждение Приказа тайных дел. Его функции.
8) Вопросы защиты информации в Судебниках 1497 и 1550 гг.

2. Практическое задание1

1) Изучить материалы Судебников 1497 и 1550 гг., Соборного Уложения 1649 г.
2) Определить меры ответственности за шпионаж, государственную измену, нарушение внутренней безопасности государства, хищение и подделку документов и печатей.
3) Выбрать статьи, касающиеся вопросов защиты информации и заполнить таблицу 1:

Таблица 1.

Вопросы защиты информации в документах XV - XVII вв.

№ п/п	Название документа	Номер, название статьи	Краткое описание

Организация защиты информации в Российской Империи в XVIII - XIX вв.

1. Вопросы для обсуждения

1) Развитие торгово-промышленной деятельности в XVIII – XIX вв. Формирование законодательной основы акционерного предпринимательства.
2) Организация кредитных отношений в XVIII - XIX вв. Формирование системы казенных банков. Формирование биржевой деятельности.
3) Органы защиты информации. Функции в области защиты информации Преображенского приказа и Верховного тайного совета. Основные функции Тайной розыскных дел канцелярии, Тайной экспедиции.
4) Деятельность Военной Коллегии, Коллегии иностранных дел в области защиты информации.
5) Основные направления и методы защиты информации. Совершенствование шифрованной переписки. Ответственность за разглашение защищаемых сведений.
6) Защита информации в области печати, организация цензуры.
7) Основные органы верховной власти в Российской империи XIX в. и состав выполняемых ими функций в области защиты информации. Функции в области защиты информации Государственного Совета, Комитета министров, Сената.
8) Основные задачи и деятельность Первого и Третьего отделений Собственной его императорского величества канцелярии.
9) Организация защиты коммерческой тайны Министерства финансов. Защита тайны торговых (купеческих) книг. Цензурные уставы.
10) Формирование законодательства в области авторского и патентного права.
11) Функции особого отдела полиции в области защиты военно-промышленной тайны. Вопросы защиты информации в деятельности Министерства внутренних дел. Функции Главного управления по делам печати.
12) Деятельность Третьего, Пятого и Шестого делопроизводств Департамента полиции. Особый отдел Департамента полиции и региональная сеть охранных отделений.

2. Практическое задание2

1) Изучить регламентирование вопросов защиты информации в государственных учреждениях, содержащихся в «Генеральном регламенте» 1720 г., «Общем учреждении министерств» 1811 г., «Уложения о наказаниях уголовных и исправительных» 1845 г., «Положения о военном министерстве» 1869 г.
2) Заполнить таблицу 2:

Таблица 2.

Вопросы защиты информации в документах XVIII - XIX вв.

№ п/п	Название документа	Номер, название статьи	Краткое описание

3) Определить состав, структуру, основные направления деятельности центральных учреждений Российской империи, выполняющих функции в области защиты информации и порядок установления ответственности за преступления в области защиты и заполнить таблицу 3:

Таблица 3.

Органы защиты информации и основные органы власти XVIII - XIX вв.

№ п/п	Название учреждения	Период	Структура	Направления деятельности в области защиты информации

Тема 3.Организация защиты информации в России в XX в. Современное состояние системы защиты информации в России и перспективы ее совершенствования

1. Вопросы для обсуждения

1) Этапы становления системы защиты государственной тайны и коммерческой тайн в Российской империи в начале XX в. Организация защиты информации в период Первой мировой войны.
2) Государственная политика в области военной тайны в годы Гражданской войны и в период нэпа.
3) Создание Особого отдела ВЧК и его местных органов. Создание и задачи Специального отдела ВЧК – ГПУ – ОГПУ.
4) Органы защиты военной тайны, основные задачи органов военной контрразведки в XX в. Усиление ответственности за разглашение государственной тайны и утрату защищаемых документов накануне и в период Великой Отечественной войны.
5) Усиление государственных мер в области защиты информации. Постановления ЦК КПСС и СМ СССР 1970, 1976, 1980 гг. по укреплению режима секретности.
6) Нормативные документы по усилению противодействия иностранным техническим разведкам, улучшению охраны объектов, предотвращению утечки информации через публикации и др.
7) Государственные органы защиты информации в конце XX в. Создание, задачи и функции Государственной технической комиссии, ФСТЭК.
8) Государственная политика в области защиты информации. Указ Президента РФ «О защите государственных секретов Российской Федерации». Базовые законы в области защиты информации: «О безопасности», «Об информации, информатизации и защите информации», «О государственной тайне».
9) Регулирование состава защищаемой информации законом «О государственной тайне». Перечень сведений, составляющих государственную тайну. Сведения, которые не могут быть отнесены к государственной тайне.
10) Полномочия органов законодательной власти, Президента РФ, правительства, органов исполнительной и судебной власти в области защиты информация.

11) Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны.
12) Полномочия органов Федеральной службы безопасности, Министерства обороны, Министерства внутренних дел, Министерства иностранных дел, Службы внешней разведки в области защиты информации.

2. Практическое задание3

1) Определить состав, структуру, основные направления деятельности центральных учреждений Российской Федерации, выполняющих функции в области защиты информации, и заполнить таблицу 4:

Таблица 4.

Органы защиты информации и основные органы власти в XX в.

№ п/п	Название учреждения	Период деятельности	Структура	Направления деятельности в области защиты информации

3. Контрольная работа 1

Вопросы к контрольной работе № 1 по темам 1 – 3.

1. Сущность направления подготовки «Информационная безопасность», характеристика ее составляющих. Место и значение направления подготовки в системе специальностей по направлению подготовки «Информационная безопасность».
2. Назначение и структура Федерального государственного образовательного стандарта по направлению подготовки.
3. Функции Боярской Думы в области внешней и внутренней политики и обеспечения государства. Опричнина и система обеспечения безопасности государства.
4. Основные функции в области обеспечения внешней и внутренней безопасности государства и защиты информации Разрядного, Оружейного, Казенного, Посольского приказов.
5. Вопросы защиты информации в Судебниках 1497 и 1550 гг**.**Вопросы защиты информации в Соборном Уложении 1649 года.
6. Регламентирование вопросов защиты информации в Генеральном регламенте 1720 г.
7. Развитие торгово-промышленной деятельности в XVIII в. Формирование законодательной основы акционерного предпринимательства.
8. Функции в области защиты информации Преображенского приказа и Верховного тайного совета. Основные задачи и деятельность Первого и Пятого департаментов Сената.
9. Деятельность Военной Коллегии, Коллегии иностранных дел в области защиты информации. Основные функции Тайной розыскных дел канцелярии, Тайной экспедиции.
10. Функции в области защиты информации Государственного Совета, Комитета министров, Сената. Основные задачи и деятельность Первого и Третьего отделений Собственной его императорского величества канцелярии.
11. «Общее учреждение министерств» от 25 июня 1811 г.
12. Вопросы защиты информации в деятельности Министерства внутренних дел, Министерства полиции, Министерства юстиции, Военного министерства, Министерства финансов, Министерства иностранных дел.
13. Правовые основы защиты информации. «Уложение о наказаниях уголовных и исправительных» (1845).
14. Вопросы защиты информации в деятельности Министерства внутренних дел. Деятельность Третьего, Пятого и Шестого делопроизводств Департамента полиции.Особый отдел Департамента полиции и региональная сеть охранных отделений.

15. Функции в области защиты военно-промышленной тайны Военного и Морского министерств. Деятельность Главного артиллерийского управления.

18. Функции в области защиты государственной тайны Главного управления Генерального штаба. Первый отдел Генерального штаба.

19. Основные особенности организации защиты информации в советский период. Усиление роли государства в области защиты информации. Создание специальных органов защиты информации.

20. Создание и задачи Специального отдела ВЧК – ГПУ – ОГПУ. Региональные государственные органы по защите информации. Подразделения защиты информации в наркоматах, ведомствах, на предприятиях. Создание 7 отдела ГУГБ НКВД СССР, его задачи и функции.

21. Основные направления и методы защиты государственных секретов в предвоенное время и в период действия военного положения (1940-е годы).

22. Усиление ответственности за разглашение государственной тайны и утрату документов, содержащих государственную тайну (1940-50-е годы).

23. Государственная политика в области защиты информации (1960-70-е годы). Постановления ЦК КПСС и СМ СССР по сохранению государственной тайны и укреплению режима секретности.

24. Постановления ЦК КПСС и СМ СССР 1970, 1976, 1980 гг. по укреплению режима секретности. Нормативные документы по усилению противодействия иностранным техническим разведкам, улучшению охраны объектов, предотвращению утечки информации через публикации и др.

25. Государственная политика в области защиты информации; обеспечение преемственности и новые аспекты. Указ Президента РФ «О защите государственных секретов Российской Федерации».

26. Базовые законы в области защиты информации: «О безопасности», «Об информации, информационных технологий и защите информации».

27. Правовое регулирование состава информации, относимой к коммерческой тайне. Сведения, которые не могут являться коммерческой тайной.Нормативное регулирование зашиты информации, составляющей служебную, профессиональную и личную тайну.

4. Тест 1

Вопросы теста 1 по темам 1 – 3
Банк тестовых заданий размещен на сайте центра цифрового обучения
http://moodle.asu.edu.ru

ТЗ № 1.

Выберите правильный вариант ответа. Как наказывались измена Родине и шпионаж по Постановлению ЦИК СССР от 2 октября 1937 г.

- лишение свободы до 25 лет.
- лишение свободы до 10 лет
- лишение свободы до 15 лет
- лишение свободы до 5 лет
- смертная казнь
- лишение свободы до 50 лет

ТЗ № 2.

Выберите правильный вариант ответа. Кто стал первым председателем Всероссийской Чрезвычайной Комиссии, созданной в декабре 1917 г.?

- Ф.Э.Дзержинский
- М.С.Урицкий
- М.С.Лацис
- А.Д.Цюрупа

ТЗ № 3
Выберите правильный вариант ответа. Наркомом внутренних дел в период массовых репрессий 1937 г. являлся:

- А.Я.Вышинский
- Н.И.Ежов
- Г. Н.Ягода
- Л.П. Берия

ТЗ № 4.
Выберите правильный вариант ответа. Как называется правовой документ, принятый Государственной Думой 25 января 1995 года?

- Указ об утверждении перечня сведений конфиденциального характера
- Федеральный закон об информации, информатизации и защите информации
- Доктрина информационной безопасности Российской Федерации
- Закон РФ о государственной тайне

ТЗ № 5.
Выберите правильный вариант ответа. Сколько установлено степеней секретности сведений по Закону РФ «О государственной тайне» от 21 июля 1993 г.?

- 1
- 2
- 3
- 4
- 5

Тема4. История развития систем защиты информации в зарубежных странах

1. Вопросы для обсуждения

1) Особенности опыта организации защиты информации на Древнем Востоке.
2) Становление основных направлений, принципов и методов защиты информации в средневековой Европе.
3) Основные направления совершенствования защиты информации в Новое время.
4) Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии).
5) Опыт криптографической защиты информации в странах Западной Европы.
6) Методы защиты коммерческих сведений. Банковская тайна и особенности ее защиты.
7) Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в XVIII - начале XX вв.
8) Формирование правовых и организационных основных основ защиты информации.
9) Разведка и контрразведка как необходимые элементы политического обеспечения безопасности.
10) Промышленный шпионаж: его значение для формирования систем защиты информации. Формирование авторского и патентного права.
11) Защита информации, содержащейся в торговых книгах, в XIX - начале XX в. (на примере Германии, Франции, Италии, Голландии, Австрии, Венгрии).

2. Практическое задание4

1) Рассмотреть российские технические средства, сертифицированные для защиты информации в государственных учреждениях РФ:
   a. Средства выявления каналов утечки информации.
   b. Средства активной защиты от утечки по техническим каналам.
   c. Средства аппаратной криптографии.
   d. Досмотровая техника, устройства радиоподавления.
2) Выявить наиболее полные зарубежные аналоги и заполнить таблицу 5.

Таблица 5.

Сравнительный анализ зарубежных аналогов российских технических средств

	Название российских технических средств	Название зарубежных технических средств
Технические характеристики		
1.		
2.		
…		
Функциональные возможности		
1.		
2.		
…		
Цена		

Тема 5. Организация системы защиты информации в США и в странах Евросоюза

Организация системы защиты информации в США

1. Вопросы для обсуждения

1) Особенности государственного устройства. Государственная политика в области защиты информации. Организация защиты информации по национальной безопасности (государственных секретов).
2) Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности. Структура разведывательного сообщества и его роль в осуществлении политики защиты информации по национальной безопасности.
3) Особенности организации защиты информации в национальной промышленности.
4) Защита секретной информации, используемой в международных программах. Защита информации в ходе деловых визитов и встреч.
5) Классификация защищаемой информации. Состав грифов ограничения доступа к документам. Состав информации, не подлежащей классификации по степени секретности.
6) Организация доступа к грифованной информации. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Особенности организации работы с секретной научно-технической информацией.
7) Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к информации по национальной безопасности.
8) Правовые основы защиты информации по национальной безопасности.
9) Организация защиты коммерческой тайны. Функции по защите коммерческой тайны частных охранно-сыскных агентств и служб промышленной и коммерческой безопасности. Государственный контроль за их деятельностью.

10) Координация деятельности частных агентств безопасности и правоохранительных органов. Создание системы координации национальной безопасности предпринимательской деятельности. Ассоциации охранно-сыскных агентств и служб безопасности, особенности их деятельности и функции в области защиты информации. Организация и основные направления деятельности служб безопасности фирм.

11) Классификация информации, составляющей коммерческую тайну. Доступ к информации, принадлежащей частным лицам. Разработка программы защиты информации. Обязательный перечень защитных мер.

12) Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к информации, составляющей коммерческую тайну фирмы.

2. Практическое задание5

1) Рассмотреть нормативное обеспечение криптографической защиты в России и зарубежных странах и заполнить таблицу 6:

Таблица 6.

Сравнительный анализ нормативного обеспечения криптографической защиты в России и зарубежных странах

№ п/п	Название закона, стандарта в России	Краткое описание	Название закона, стандарта в зарубежных странах	Краткое описание

1. Сделать сравнительный анализ обеспечения и реализации в России и зарубежных странах следующих современных криптографических алгоритмов:
   - алгоритмы симметричного шифрования;
   - алгоритмы ассиметричного шифрования;
   - алгоритмы электронно-цифровой подписи и хэширования.
2. Получившимися данными заполнить таблицу 7:

Таблица 7.

Сравнительный анализ обеспечения и реализации в России и зарубежных странах современных криптографических алгоритмов

№ п/п	Название алгоритма	Страна	Краткое описание	Применение

Организация системы защиты информации в странах Евросоюза

1. Вопросы для обсуждения

1) Особенности государственного устройства. Государственная политика в области защиты информации.

2) Состав, структура и основные направления деятельности специальных служб безопасности. Особенности и принципы организации их деятельности.

3) Функции разведывательных и полицейских органов в области защиты информации. Парламентско-правительственный контроль за деятельностью специальных служб.

4) Агентства, предоставляющие частным фирмам, банкам, государственным учреждениям услуги по обеспечению безопасности зданий и лиц, подлежащих охране. Частные промышленные и коммерческие службы безопасности.

5) Подразделения внутренней охраны, создаваемые самими предприятиями, фирмами, финансово-кредитными организациями, государственные организации по борьбе с экономическим шпионажем, преступностью.

6) Добывание информации, контроль за деятельностью иностранных граждан на территории данных стран. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности.

7) Основные функции служб безопасности. Основные направления совершенствования работы служб безопасности.

8) Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации. Требования к персоналу в совместных фирмах.

9) Организация защиты информации. Особенности защиты информации в банковской сфере.

10) Правовые основы защиты информации. Государственная тайна и доступ к правительственной, парламентской и судебной информации.

11) Правовая защита служебной, налоговой тайны, тайны судебного разбирательства, тайны почтовых и телесообщений (телефонных, телеграфных и пр.).

12) Правовая защита коммерческой и производственной тайны. Организация доступа к информации, принадлежащей частным лицам.

2. Практическое задание6

1) Провести сравнительный анализ специальных служб обеспечения информационной безопасности иностранных государств (США, Великобритании, Франции, Германии, Китая, Израиля), аналогичных следующим российским службам:
   a. Федеральная служба безопасности (ФСБ).
   b. Федеральная служба по техническому и экспортному контролю (ФСТЭК).
   c. Служба внешней разведки (СВР).
   d. Главное разведывательное управление Генерального штаба ВС (ГРУ).
2) Получившимися данными заполнить таблицу 8:

Таблица 8.Сравнительный анализ российских и зарубежных служб обеспечения информационной безопасности

№ п/п	Название иностранного государства	Название спецслужбы	Структура спецслужбы	Направления деятельности	Название соответствующей спецслужбы России

Тема 6. Организация системы защиты информации в Японии и в Китае

Организация системы защиты информации в Японии

1. Вопросы для обсуждения

1) Особенности государственного устройства Японии. Государственная политика в области защиты информации.

2) Организация системы специальных служб и их основные функции в области защиты информации.

3) Состав, структура и основные направления деятельности специальных служб безопасности. Частные сыскные бюро, частные фирмы охраны и безопасности и их функции в сфере защиты информации.

4) Ассоциации служб охраны и безопасности. Общественные организации, оказывающие помощь органам полиции в сфере защиты экономической информации (территориальные советы по предупреждению преступности, общества содействия полиции, пункты связи по предупреждению преступности).

5) Службы безопасности отдельных организаций. Подразделения внутреннего самоконтроля отдельных организаций и их функции в сфере защиты информации.

6) Основные функции служб безопасности. Методы и основные направления совершенствования работы служб безопасности.

7) Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации.

8) Организация защиты информации. Принцип корпоративной защиты и обеспечения безопасности объекта.

9) Защита информации в процессе взаимодействия фирм с иностранными партнерами.

10) Классификация защищаемой информации.

11) Правовые основы защиты информации. .Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов.

12) Правовая защита коммерческой тайны, тайны корреспонденции. Коммерческая организация доступа к информации, принадлежащей частным предприятиям.

2. Практическое задание7

1) Изучить средства ведения информационно-психологической войны:
   - Информационное оружие, предназначенное для негативного воздействия на человека:
   - средства массовой информации;
   - психотронные генераторы;
   - психотропные препараты.
2) Информационное оружие, предназначенное для вывода из строя средств электронных коммуникаций противника:
   - средства радиоэлектронной борьбы (РЭБ);
   - средства специального программно-технического воздействия (СПТВ).
3) Заполнить таблицу 9:

Таблица 9.

Анализ средств ведения информационно-психологической войны:

№ п/п	Название информационного оружия	Механизм действия	Период применения	Практика применения

Организация системы защиты информации в Китае

1. Вопросы для обсуждения

1) Особенности государственного устройства Китая. Особенности процесса формирования системы защиты информации в Китае. Государственная политика в области защиты информации.

2) Организация системы специальных служб и их основные функции в области защиты информации.

3) Представление об информационном противоборстве в Китае

4) Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации.

5) «Великая стена» информационной безопасности Китая.

6) Правовые основы защиты информации. Ответственность за компьютерные преступления.
7) Организация защиты информации. Особенности защиты информации в банковской сфере.
8) Правовые основы защиты информации.
9) Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов.
10) Правовая защита коммерческой тайны, тайны корреспонденции. Коммерческая организация доступа к информации, принадлежащей частным предприятиям.

Тема 7. Стандарты информационной безопасности.

1. Вопросы для обсуждения

1) Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга).
2) Международный стандарт ISO 17799.
3) Международный стандарт ISO 15408 «Общие критерии».
4) Стандарт COBIT.
5) Гармонизированные критерии европейских стран.
6) Германский стандарт BSI.
7) Британский стандарт B7799.

2. Практическое задание8

1) Изучить основные международные стандарты, регламентирующие обеспечение защиты конфиденциальной информации:
2) Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга).
3) Международный стандарт ISO 17799.
4) Международный стандарт ISO 15408 «Общие критерии».
5) Стандарт COBIT.
6) Сравнить вышеназванные стандарты и заполнить таблицу 10:

Таблица 10.

Анализ международных стандартов в области информационной безопасности:

№ п/п	Название зарубежного стандарта	Назначение стандарта	Описание стандарта	Название российского стандарта	Назначение стандарта	Описание стандарта

3. Реферат

Тематика рефератов

1. Информационное законодательство в США (Конституционные положения о праве СМИ в США.
2. Информационное законодательство в Великобритании (Источники права о прессе в Великобритании. Место международных соглашений о правах человека в национальном праве в Великобритании. Клевета. Доступ к информации).
3. Информационное законодательство в Федеративной Республике Германии (Конституционные положения и источники права СМИ в ФРГ. Разделение полномочий в регулировании прессы между центральным и региональными правительствами. Государственная тайна и доступ к правительственной информации. Механизм

саморегулирования прессы).

4. Французское законодательство о средствах массовой информации. Конституция Франции и другие источники права СМИ (Разделение полномочий между центральным и региональными правительствами. Включение элементов международного права в национальное право Франции. Доступ к информации. Клевета).

5. Законодательство о средствах массовой информации в Австрии (Источники права СМИ в Австрии. Конституционные положения и другие источники права СМИ Австрии. Место международных соглашений о правах человека в национальном праве Австрии. Клевета. Доступ к информации).

6. Основные лицензирующие органы в области защиты информации –Федеральная служба по техническому и экспортному контролю (ФСТЭК России) (правопреемник Гостехкомиссии).

7. Полномочия предприятий в области защиты информации.

8. Особенности концепции национальной безопасности России.

9. Особенности опыта организации защиты информации на Древнем Востоке.

10. Международный опыт защиты информации в процессе банковской деятельности.

11. Ответственность за разглашение государственной тайны.

12. Перечни сведений, составляющих государственную тайну.

13. Появление новых видов носителей секретной информации, средств и способов ее обработки, хранения и передачи в связи с внедрением АСОД. Расширение угроз защищаемой информации и каналов несанкционированного доступа к ней. Объекты защиты.

14. Полномочия органов законодательной власти, Президента РФ, правительства, органов исполнительной и судебной власти в области защиты информация.

15. Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны.

16. Полномочия Государственной технической комиссии и Федерального агентства правительственной связи и информации в области защиты информации.

17. Полномочия органов Федеральной службы безопасности, Министерства обороны, Министерства внутренних дел, Министерства иностранных дел, Службы внешней разведки в области защиты информации.

18. Защита профессиональной тайны.

19. Защита коммерческой тайны.

20. Состав защищаемой информации. Объекты защиты.

Тема 8. Состав защищаемой информации в России и за рубежом. Современная нормативная база по защите информации в России и за рубежом.

1. Вопросы для обсуждения

1) Состав защищаемой информации в России и за рубежом.

2) Сокращение объема сведений, составляющих государственную тайну. Регулирование состава защищаемой информации законом "О государственной тайне". Перечень сведений, составляющих государственную тайну. Сведения, которые не могут быть отнесены к государственной тайне.

3) Правовое регулирование состава информации, относимой к государственной тайне.

4) Правовое регулирование состава информации, относимой к коммерческой тайне. Сведения, которые не могут являться коммерческой тайной.

5) Нормативное регулирование зашиты информации, составляющей служебную, профессиональную и личную тайну.

6) Полномочия органов законодательной власти, Президента РФ, правительства, органов исполнительной и судебной власти в области защиты информация.

7) Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны.

8) Полномочия Государственной технической комиссии и Федерального агентства правительственной связи и информации в области защиты информации.

9) Полномочия органов Федеральной службы безопасности, Министерства обороны, Министерства внутренних дел, Министерства иностранных дел, Службы внешней разведки в области защиты информации.

10) Полномочия предприятий в области защиты информации.

11) Особенности концепции национальной безопасности России.

2. Контрольная работа 2

Вопросы к контрольной работе № 2 по темам 4 – 8.

1. Формирование подходов к защите информации в Древнем мире.
2. Становление систем, методов и принципов защиты информации в зарубежных странах в Новое время.
3. Методы противодействия промышленному шпионажу в Европе в XIX в.
4. Правовая регламентация процесса защиты информации в зарубежных странах в XIX - начале XX в.
5. Состав и структура органов, осуществляющих защиту информации по национальной безопасности в США.
6. Состав основных нормативных документов, используемых в процессе режимно-секретной деятельности США.
7. Особенности категорирования информации по национальной безопасности в США.
8. Законодательное регулирование процесса защиты информации Германии, Франции, Великобритании, Швеции.
9. Состав и основные направления деятельности органов защиты информации Германии, Франции, Великобритании, Швеции.
10. Организация защиты информации в банковской сфере. Германии, Франции, Великобритании, Швеции.
11. Состав и основные направления деятельности служб безопасности Германии, Франции, Великобритании, Швеции.
12. Становление и развитие системы защиты информации в Японии.
13. Законодательное регулирование процесса защиты информации в Японии.
14. Состав и основные направления деятельности органов защиты информации в Японии.
15. Особенности современной системы защиты информации Японии.
16. Законодательное регулирование процесса защиты информации в Китае.
17. Состав и основные направления деятельности органов защиты информации в Китае.
18. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга).
19. Гармонизированные критерии европейских стран.
20. Германский стандарт BSI. Виды угроз.
21. Британский стандарт B7799.
22. Международный стандарт ISO 17799.
23. Международный стандарт ISO 15408 «Общие критерии».
24. Стандарт COBIT.
25. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др.

26. Порядок предоставления защищаемой информации другим странам.
27. Международный опыт стандартизации в области защиты информации.
28. Международная защита интеллектуальной собственности.
29. Международные договоры и иные международно-правовые документы о защите информации.
30. Состав защищаемой информации в России и за рубежом.
31. Нормативное регулирование зашиты информации, составляющей служебную, профессиональную и личную тайну.
32. Полномочия органов законодательной власти, Президента РФ, правительства, органов исполнительной и судебной власти в области защиты информация.
33. Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны.
34. Полномочия Государственной технической комиссии и Федерального агентства правительственной связи и информации в области защиты информации.
35. Полномочия органов Федеральной службы безопасности, Министерства обороны, Министерства внутренних дел, Министерства иностранных дел, Службы внешней разведки в области защиты информации.

Тема 9. Международное сотрудничество в области обеспечения информационной безопасности

1. Вопросы для обсуждения

1) Научно-техническое сотрудничество с зарубежными партнерами.
2) Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов. Система контроля.
3) Порядок предоставления защищаемой информации другим странам.
4) Международный опыт защиты информации в процессе банковской деятельности.
5) Международный опыт стандартизации в области защиты информации.
6) Международная защита интеллектуальной собственности.
7) Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Договор об образовании Европейского экономического общества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений.

2. Тест 2

Вопросы теста 2 по темам 4 – 8
Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

ТЗ 1.
Выбрать правильные варианты ответов:
Концепция информационной войны в США предполагает деление на следующие уровни

- государственный уровень
- военный уровень
- экономический уровень
- муниципальный уровень
- национальный уровень

ТЗ 2.
Выбрать правильный вариант ответа:
Основная задача службы MI6 в Великобритании

- разведка
- контрразведка
- радиошпионаж
- топография

ТЗ 3.
Выбрать правильный вариант ответа:
Основная задача службы MI5 в Великобритании

- разведка
- контрразведка
- радиошпионаж
- борьба с терроризмом

ТЗ 4.
Выбрать правильные варианты ответов:
Основные задачи Федерального бюро защиты конституции в Германии

- сбор информации об экстремистских группировках и партиях, их деятельности, планах и намерениях, противоречащих основному закону страны
- нейтрализация разведывательной и подрывной деятельности секретных зарубежных служб на территории Германии;
- борьба с промышленным шпионажем
- выдача разрешений на внедрение информационных систем в важные государственные объекты
- разработка критериев, методов и испытательных средств для оценки степени защищенности национальных коммуникационных систем

ТЗ 5.
Выбрать правильные варианты ответов:
Какие службы действуют под эгидой Министерства обороны Франции

- Генеральная дирекция внешней безопасности (DGSE)
- Управление военной разведки (DRM)
- Управление военной контрразведки (DPSD)
- Контразведка (DST)
- Военная разведка (MUST)
- Радиоуправление национальной обороны (FRA)

Перечень вопросов к экзамену

1) Сущность и значение направления подготовки. Назначение и структура Федерального государственного образовательного стандарта по направлению
2) Особенности формирования системы защиты информации в России до XVI в.
3) Вопросы защиты информации в Судебниках 1497, 1550 гг. и Соборном Уложении 1649 г.
4) Организация защиты информации в России в XVII в.
5) Организация защиты информации в России в XVIII в.
6) Вопросы защиты информации в Генеральном регламенте 1720 г.
7) Система защиты информации в Российской империи в XIX в.
8) Нормативная база защиты информации в Российской империи в XIX в.
9) Органы защиты информации в Российской империи в XX в.
10) Система защиты информации в Российской империи в XX в.

11) Нормативная база защиты информации в России в XX в.
12) Организация защиты информации в банковских учреждениях в Российской империи во второй половине XIX - XX в.
13) Организация защиты информации в акционерных организациях в Российской империи во второй половине XIX - XX в.
14) Организация защиты коммерческой тайны в Российской империи в XX в.
15) Организационные меры по защите информации в годы Гражданской воины.
16) Становление системы защиты информации в 20-х гг.
17) Организация защиты информации накануне и в период ВеликойОтечественной войны.
18) Формирование нормативной базы и организации, основ системы защиты информации 40 - 80-х гг.
19) Современная нормативная база и организационные основы защиты государственных секретов и коммерческой тайны.
20) Основные задачи и функции Межведомственной комиссии по защите государственной тайны.
21) Основные задачи и функции Федеральной службы безопасности РФ.
22) Перечислите особенности, общие черты и различия законодательств стран Западной Европы и США в области защиты информации в XIX-начале XX в.
23) Осуществление становления и развития системы защиты информации в Японии.
24) Назовите основные нормативные документы, регламентирующие порядок организации защиты информации в США в 1970 - 1980-е гг.
25) Назовите состав и основные направления деятельности органов, осуществляющих защиту информации по национальной безопасности в США.
26) Назовите состав, основные направления деятельности и особенности функционирования органов защиты информации в Германии.
27) Назовите основные правовые документы, регламентирующие вопросы защиты государственной и коммерческой тайны в Германии.
28) Какие организации и подразделения учреждений осуществляют защиту коммерческой тайны в Великобритании?
29) Назовите основные категории служб безопасности в Великобритании.
30) Назовите основные правовые документы, регламентирующие порядок защиты информации в Великобритании.
31) Как организована система специальных служб Франции и какова их роль в обеспечении защиты информации?
32) Как осуществляется правовая защита государственной и коммерческой тайны во Франции?
33) Назовите состав органов защиты информации и их основные функции в Китае.
34) Какими документами осуществляется правовое регулирование процесса защиты информации в Японии?
35) Как осуществляется классификация защищаемой информации в Японии?
36) Перечислите особенности защиты информации в процессе проведения международных конференций, обмена специалистами, посещения охраняемых объектов представителями зарубежных фирм.
37) Как осуществляется международное сотрудничество в области защиты информации в процессе банковской деятельности?
38) Назовите основные правовые документы о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства.
39) Место и роль стандартов в развитии сферы информационной безопасности.

40) Стандартизация и сертификация как единый процесс управления качеством средств, систем и технологий в сфере защиты информации и информационной безопасности бизнеса.
41) Стандарты информационной безопасности как основа для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий.
42) Предпосылки создания стандартов информационной безопасности.
43) Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга).
44) Гармонизированные критерии европейских стран.
45) Германский стандарт BSI. Виды угроз.
46) Британский стандарт B7799.
47) Международный стандарт ISO 17799.
48) Международный стандарт ISO 15408 «Общие критерии».
49) Стандарт COBIT.
50) Защита информации и информационная безопасность в условиях информационного противоборства.

Таблица 9. Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
ПК 5 – Способен администрировать средства защиты информации в компьютерных системах и сетях.				
1.	Задание закрытого типа	Прочитайте текст, выберите один правильный вариант ответа. Действия против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей – 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна	1	2
2.		Прочитайте текст, выберите один правильный вариант ответа. Диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным 1. Электронная война 2. Психологическая война 3. Экономическая	4	2

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
		информационная война 4. Кибервойна		
3.		Прочитайте текст, выберите один правильный вариант ответа Защита информации, предусматривающая возмещение убытков от её уничтожения или модификации путем получения страховых выплат, - это 1. страховая защита 2. моральная защита 3. этическая защита	1	2
4.		Прочитайте текст, выберите все правильные варианты ответов Монитор обращений (по стандарту «Критерии оценки надежности компьютерных систем») должен обладать следующими качествами: 1. Изолированность 2. Полнота 3. Верифицируемость 4. Надежность 5. Безопасность 6. Подлинность	1, 2, 3	2
5.	Комбини-рованный	Прочитайте текст, выберите все правильные варианты ответов и запишите аргументы, обосновывающие выбор ответов Назовите средства радиоэлектронной борьбы 1. аппаратные средства 2. средства подавления связи 3. оперативные технические средства 4. средства борьбы с системами управления противника 5. программные средства экономические средства	1, 2, 3	5
6.	Задание открытого типа	Прочитайте текст и запишите развернутый ответ Дать определение «Информационное и	воздействие, которое осуществляется с применением информационного оружия, т. е. таких	8

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
		информационно-психологическое воздействие»	средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия. Информационно-психологическое воздействие представляет собой целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние (положительное или отрицательное) на функционирование и развитие информационно-психологической среды общества, психику и поведение населения, руководство страны, военнослужащих.	
7.		Прочитайте текст и запишите развернутый ответ Дать определение «Информационная война»	это открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере. Информационную войну также можно определить как	8

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
			комплекс мероприятий и операций, проводимых вооруженными силами государств и другими (как правительственными, так и частными) организациями, направленных на обеспечение информационного превосходства над противником и нанесения ему материального, идеологического или иного ущерба. В информационной войне информация является одновременно оружием, ресурсом и целью.	
8.		Прочитайте текст и запишите развернутый ответ Основными формами информационной войны являются	Командно-управленческая война – война, нацеленная на каналы связи между командованием и исполнителями. Перерезая «шею» (каналы связи), нападающий изолирует «голову» от «туловища». Разведывательная война – сбор важной в военном отношении информации (как нападение) и защита собственной. Электронная война – действия против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей. Ее важный раздел – криптография (шифровка-	8

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
			расшифровка электронной информации). Сюда же входит и кибервойна (компьютерный терроризм), которая подразумевает диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным. Оружием в этой войне являются компьютерные вирусы и др. программное обеспечение. Психологическая война – пропаганда, «промывание мозгов», информационная обработка населения. Эта форма войны имеет три составляющие — подрыв гражданского духа, деморализация вооруженных сил, дезориентация командования. Экономическая информационная война – нанесение ущерба экономической (производственной, финансовой, коммерческой и т.д.) сфере противника, создание предпосылок для кризисных ситуаций.	

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
9.		Прочитайте текст и запишите развернутый ответ Что понимается под информационным оружием	В широком смысле под информационным оружием понимаются способы целенаправленного информационного воздействия на противника, рефлексивного управления им с целью изменения его замысла на проведение стратегических или тактических действий в нужном направлении. В более узком смысле под информационным оружием понимается комплекс способов, методов, технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника и вмешательства в работу его информационных систем для выведения их из строя, нарушения процесса нормального функционирования, получения или модификации содержащихся в них данных, а также целенаправленного продвижения выгодной информации (или дезинформации). При этом сама информация, попадание которой к противнику может нанести ему заметный материальный или иной ущерб, также	8

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
			нередко совершенно справедливо и обоснованно рассматривается в качестве одного из видов информационного оружия.	
10.		Прочитайте текст и запишите развернутый ответ Назовите средства борьбы на основе разведывательных технологий (СРТ)	Сенсорные системы дистанционного действия космического базирования (например, на основе лазерного излучения с различной длиной волны), а также датчики, фиксирующие сейсмические и акустические воздействия; Приближенные к боевой зоне системы (например, беспилотные летательные аппараты, оснащенные аппаратурой спектрального обнаружения, спецрадарами электронной разведки, береговые и наземные радарные системы); Датчики, расположенные непосредственно на поле боя (биохимические, гравиметрические, акустические и оптические); Сенсорные системы, установленные непосредственно на различных видах вооружения (инфракрасные, фиксирующие	8

№ п/п	Тип задания	Формулировка задания	Правильный Ответ	Время выполнения (в минутах)
			световые аномалии и пр.).	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля).

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Методические рекомендации по выполнению практических и контрольных работ, проведению экзамена

Критерии оценки обсуждения вопросов по теме:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки.

Отчет по практической работе

Отчет по практической работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной практической работе должны быть указаны:

- тема практической работы,
- пакет документов в соответствии с темой практической работы,
- использованная литература.

Критерии оценки по практическим работам:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;

- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;

- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.

- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.

- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;

- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-24 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала.

11-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

10 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме. 0 баллов – нет ответа.

Таблица 10.Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	9/1	9	По расписанию
2.	*Выполнение лабораторной работы*	8/1	8	
3.	*Выполнение контрольной работы*	2/5	10	
4.	*Тест*	2/4	8	
5.	*Реферат*	1/5	5	
Всего			**40**	-
Блок бонусов				
6.	*Посещение занятий без пропусков*	1	3	

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
7.	*Своевременное выполнение всех заданий*	1	3	
8.	*Активность студента на занятии*	1	4	
Дополнительный блок				
9.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11. Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	незачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. М.: Флинта, 2016. 224с. URL: http://www.studentlibrary.ru/book/ISBN9785976512740.html (ЭБС «Консультант студента»).

2. Аверченков В.И., Ерохин В.В., Голембиовская О.М. История развития системы государственной безопасности России: учебное пособие. ФЛИНТА, 2011 г., 192 сURL: http://www.studentlibrary.ru/book/ISBN9785976512597.html (ЭБС «Консультант студента»).

3. Т.Г. Гурская, История и современная система защиты информации в россии и зарубежных странах. Издательский дом «Астраханский университет», 2012.URL: https://biblio.asu.edu.ru/Reader/Book/2014060215315427039600007308 ЭБС Электронный Читальный зал – БиблиоТех).

8.2. Дополнительная литература

1. Мельников, В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ; стер. -М. : Академия, 2009. - 336 с. (19 экз.)
2. Мельников, В.П. Информационная безопасность: учеб. пособие под ред. С.А. Клейменова. - М. : Академия, 2005. - 336 с. (45 экз.)
3. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия; уч. пособие. -2 изд. – М.: Издат.-торговая корпорация «Дашков и К», 2005, – 336 ч. (45 экз.)
4. Хорев П.Б. Методы и средства защиты информации в компьютерных системах :уч.пособие. – М.: Издат центр «Академия», 2005, – 256 с. (69 экз.)
5. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html (ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований.www.studentlibrary.ru.
2. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет и установлено программное обеспечение.

10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть

представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).