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

И.М. Ажмухамедов

«22» июня 2023 г.

УТВЕРЖДАЮ

И.о. заведующего кафедрой
информационной безопасности

Р.Ю. Демина

«22» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Проектирование инженерно-технической системы защиты информации

наименование

Составитель(-и)	**Шукралиева Д.Э. доцент кафедры информационной безопасности;** **Корякова В.А., ассистент кафедры информационных технологий, начальник отдела информационной безопасности**
Направление подготовки / специальность	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ**
Квалификация (степень)	**бакалавр**
Форма обучения	**Очно-заочная**
Год приема	**2023**
Курс	**4**
Семестр	**7, 8**

Астрахань – 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели освоения дисциплины «Проектирование инженерно-технической системы защиты информации»: познакомить студентов с возможностями и ограничениями использования систем инженерно-технической защиты (СИТЗ) информации в общем комплексе средств обеспечения информационной безопасности путем освоения теоретических основ дисциплины и приобретения некоторых практических навыков, в т.ч. связанных с созданием эскизных проектов СИТЗ; оценками необходимых объемов ресурсов, требующихся для создания и эксплуатации СИТЗ.

1.2. Задачи освоения дисциплины (модуля):

- дать студентам-бакалаврам целостное представление о назначении СИТЗ;
- изучить основные этапы и направления развития СИТЗ;
- освоить основные подходы к созданию СИТЗ;
- изучить возможности использования информационных технологий и математических методов при решении задач проектирования и эксплуатации СИТЗ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Проектирование инженерно-технической системы защиты информации» относится к элективным дисциплинам (модулям) и осваивается в седьмом и восьмом семестрах.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами*:*

- Информатика.
- Физика.
- Физические основы защиты информации.
- Техническая защита информации.

Знания: основных понятий информатики, принципов и методов организационной защиты информации; технических каналов утечки информации, возможностей технических разведок, способов и средств защиты информации от утечки по техническим каналам, методов и средств контроля эффективности технической защиты информации.

Умения: анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации.

Навыки: поиска информации в глобальной информационной сети Интернет; применения методов технической защиты информации; методов расчета и инструментального контроля показателей технической защиты информации.

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

Знания, полученные в результате изучения дисциплины «Проектирование инженерно-технической системы защиты информации», используются студентами при прохождении преддипломной практики и написании бакалаврской работы.

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): Способен выполнять работы по установке, настройке и обслуживанию

программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем (ПК – 1); Способен выполнять работы по установке, настройке и техническом у обслуживанию защищенных технических средств обработки информации (ПК – 2).

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-1 - Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем	ИПК-1.1. нормативные правовые акты в области защиты информации, организационные меры по защите информации, программно-аппаратные средства обеспечения защиты информации автоматизированных систем, методы контроля эффективности защиты информации от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	ИПК 1.2. определять источники и причины возникновения инцидентов, устранять нарушения правил разграничения доступа, применять программные средства обеспечения безопасности данных, осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, использовать криптографические методы и средства защиты информации в автоматизированных системах	ПК-1.3. методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа
ПК-2 - Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации	ИПК 2.1. технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности информации	ИПК 2.2. проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией	ИПК 2.3. методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 2,3 зачетных единиц (216 часа).

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости Форма промежуточной аттестации
			Л	ПЗ	ЛР	КР	СР	
1.	*Тема 1. Введение в дисциплину. Основные виды информационных ресурсов, которые нуждаются в защите.*	7	***3***		***3***		***12***	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
2.	*Тема 2. Условия работы организаций различных типов с позиций необходимости использования мер инженерно-технической защиты информации*		***3***		***3***		***13***	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
3.	*Тема 3. Общие принципы проектирования и реализации систем инженерно-технической защиты информации*		***3***		***3***		***13***	Устный опрос, анализ «проблемных ситуаций»
4.	*Тема 4. Архитектура инженерно-технической системы защиты информации*		***3***		***3***		***12***	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
5.	*Тема 5. Разработка технического проекта инженерно-технической системы защиты информации.*		***4***		***4***		***8***	Устный опрос
	ИТОГО ЗА 7 СЕМЕСТР		**16**		**16**		**58**	**ЗАЧЕТ**
6.	*Тема 6. Разработка рабочей документации инженерно-технической системы защиты информации.*	8	***3***		***3***		***12***	Устный опрос, доклад-презентация
7.	*Тема 7. Проектирование помещений для работы с ИР с учетом требований нормативных документов по защите информации*		***3***		***3***		***13***	Устный опрос, доклад-презентация
8.	*Тема 8. Подготовка и оформление технической документации на поставку технических и программных средств для инженерно-технической системы защиты информации.*		***3***		***3***		***13***	Устный опрос, анализ «проблемных ситуаций»
9.	*Тема 9. Критерии оптимальности и ограничения, которые должны учитываться при выборе таких средств*		***4***		***4***		***10***	Устный опрос, анализ «проблемных ситуаций»
10.	*Тема 10. Разработка порядка и этапов внедрения инженерно-технической системы защиты информации*		***4***		***4***		***8***	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
	ИТОГО ЗА 8 СЕМЕСТР		**17**		**17**		**56**	**ЭКЗАМЕН**
	ИТОГО ЗА ВЕСЬ ПЕРИОД		**33**		**33**		**114**	

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Темы, разделы дисциплины	Кол-во часов	Компетенции		
		ПК 1	ПК 2	общее количество компетенций
Введение в дисциплину. Основные виды информационных ресурсов, которые нуждаются в защите.	18	+	+	2
Условия работы организаций различных типов с позиций необходимости использования мер инженерно-технической защиты информации	19	+	+	2
Общие принципы проектирования и реализации систем инженерно-технической защиты информации	19	+	+	2
Архитектура инженерно-технической системы защиты информации	18	+	+	2
Разработка технического проекта инженерно-технической системы защиты информации.	16	+	+	2
Разработка рабочей документации инженерно-технической системы защиты информации.	18	+	+	2
Проектирование помещений для работы с ИР с учетом требований нормативных документов по защите информации	19	+	+	2
Подготовка и оформление технической документации на поставку технических и программных средств для инженерно-технической системы защиты информации.	19	+	+	2
Критерии оптимальности и ограничения, которые должны учитываться при выборе таких средств	18	+	+	2
Разработка порядка и этапов внедрения инженерно-технической системы защиты информации	16	+	+	2
ИТОГО	108			

Краткое содержание дисциплины

Тема 1

Введение в дисциплину. Основные виды информационных ресурсов, которые нуждаются в защите. Демаскирующие признаки. Категорирование объектов защиты.

Тема 2

Условия работы организаций различных типов с позиций необходимости использования мер инженерно-технической защиты информации. Основные положения системного подхода к инженерно-технической защите информации

Тема 3

Цели и задачи инженерно-технической системы защиты. Общие принципы проектирования и реализации систем инженерно-технической защиты информации. Этапы процесса обеспечения информационной безопасности

Тема 4

Архитектура инженерно-технической системы защиты информации. Классификация методов инженерно-технической защиты информации. Классификация зон безопасности.

Тема 5

Разработка технического проекта инженерно-технической системы защиты информации.

Тема 6
Разработка рабочей документации инженерно-технической системы защиты информации.

Тема 7
Проектирование помещений для работы с ИР с учетом требований нормативных документов по защите информации. Интегрированные комплексные системы безопасности

Тема 8
Подготовка и оформление технической документации на поставку технических и программных средств для инженерно-технической системы защиты информации

Тема 9
Критерии оптимальности и ограничения, которые должны учитываться при выборе таких средств. Эффективность системы защиты.

Тема 10
Жизненный цикл систем безопасности. Разработка порядка и этапов внедрения инженерно-технической системы защиты информации.

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 и лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8. Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8, Интернет-источниками.

Таблица 4 – Содержание самостоятельной работы обучающихся
для очно-заочной формы обучения

Номер радела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	Подготовка к устному опросу Подготовка доклада-презентации	12	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
2	Подготовка к устному опросу Подготовка доклада-презентации	13	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
3	Подготовка к устному опросу Подготовка доклада-презентации	13	Устный опрос, анализ «проблемных ситуаций»
4	Подготовка к устному опросу Подготовка доклада-презентации	12	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»
5	Подготовка к устному опросу Подготовка доклада-презентации	8	Устный опрос
6	Подготовка к устному опросу Подготовка доклада-презентации	12	Устный опрос, доклад-презентация
7	Подготовка к устному опросу Подготовка доклада-презентации	13	Устный опрос, доклад-презентация
8	Подготовка к устному опросу Подготовка доклада-презентации	13	Устный опрос, анализ «проблемных ситуаций»
9	Подготовка к устному опросу Подготовка доклада-презентации	10	Устный опрос, анализ «проблемных ситуаций»

10	Подготовка к устному опросу Подготовка доклада-презентации	8	Устный опрос, доклад-презентация, анализ «проблемных ситуаций»

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

Доклад-презентация

Доклад должен оформляться в электронном виде в форме презентации Power Point и печатном виде на листах формата А4 и содержать задание, краткие необходимые теоретические сведения, полученные по каждому пункту задания результаты и выводы.

Защита реферата 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.

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

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Введение в дисциплину. Основные виды информационных ресурсов, которые нуждаются в защите.	*Обзорная лекция*	*Не предусмотрено*	*Фронтальный опрос*
Условия работы организаций различных типов с позиций необходимости использования мер инженерно-технической защиты информации	*Лекция-диалог*	*Не предусмотрено*	*Тематические дискуссии, анализ конкретных ситуаций*
Общие принципы проектирования и реализации систем инженерно-технической защиты информации	*Лекция*	*Не предусмотрено*	*Выполнение практических заданий, тематические дискуссии*
Архитектура инженерно-технической системы защиты информации	*Лекция*	*Не предусмотрено*	*Фронтальный опрос*
Разработка технического проекта инженерно-технической системы защиты информации.	*Лекция*	*Не предусмотрено*	*Фронтальный опрос*
Разработка рабочей документации инженерно-технической системы защиты информации.	*Обзорная лекция*	*Не предусмотрено*	*Фронтальный опрос*
Проектирование помещений для работы с ИР с учетом требований	*Лекция-диалог*	*Не предусмотрено*	*Фронтальный опрос, выполнение*

нормативных документов по защите информации			*практических заданий, тематические дискуссии*
Подготовка и оформление технической документации на поставку технических и программных средств для инженерно-технической системы защиты информации.	*Лекция*	*Не предусмотрено*	*Тематические дискуссии, анализ конкретных ситуаций*
Критерии оптимальности и ограничения, которые должны учитываться при выборе таких средств	*Лекция-диалог*	*Не предусмотрено*	*Фронтальный опрос*
Разработка порядка и этапов внедрения инженерно-технической системы защиты информации	*Лекция*	*Не предусмотрено*	*Фронтальный опрос*

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%.

Название образовательной технологии	Краткое описание применяемой технологии
Лекция-визуализация	Использование мультимедийных роликов
Деловая игра	Выберите конкретную организацию – реальную или вымышленную, для которой необходимо спроектировать систему инженерно-технической защиты информации. Дайте краткую характеристику условий и особенностей деятельности организации.
Разбор ситуаций	Выберите конкретную организацию, опишите условия ее деятельности. Выберите комплекс мер инженерно-технической защиты информации, которые Вы собираетесь внедрять в этой организации, включая программно-технические средства защиты информации. Укажите календарную продолжительность процессов внедрения.

6.2. Информационные технологии

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. Перечень программного обеспечения и информационных справочных систем

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 10 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 MARK SQL 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) «Проектирование инженерно-технической системы защиты информации» 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

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1.	Введение в дисциплину. Основные виды информационных ресурсов, которые нуждаются в защите.	***ПК 1, ПК 2***	Вопросы для устного опроса, темы докладов, «проблемные ситуации»
2.	Условия работы организаций различных типов с позиций необходимости использования мер инженерно-технической защиты информации	***ПК 1, ПК 2***	Вопросы для устного опроса, темы докладов, «проблемные ситуации»
3.	Общие принципы проектирования и реализации систем инженерно-технической защиты информации	***ПК 1, ПК 2***	Вопросы для устного опроса, «проблемные ситуации»
4.	Архитектура инженерно-технической системы защиты информации	***ПК 1, ПК 2***	Вопросы для устного опроса, темы докладов, «проблемные ситуации»
5.	Разработка технического проекта инженерно-технической системы защиты информации	***ПК 1, ПК 2***	Вопросы для устного опроса
6.	Разработка рабочей документации инженерно-технической системы защиты информации.	***ПК 1, ПК 2***	Вопросы для устного опроса, темы докладов
7.	Проектирование помещений для работы с ИР с учетом требований нормативных документов по защите информации	***ПК 1, ПК 2***	Вопросы для устного опроса, темы докладов
8.	Подготовка и оформление технической документации на поставку технических и программных средств для инженерно-технической системы защиты информации.	***ПК 1, ПК 2***	Вопросы для устного опроса, «проблемные ситуации»
9.	Критерии оптимальности и ограничения, которые должны учитываться при выборе таких средств	***ПК 1, ПК 2***	Вопросы для устного опроса, «проблемные ситуации»
10.	Разработка порядка и этапов внедрения инженерно-технической системы защиты информации	***ПК 1, ПК 2***	Вопросы для устного опроса, темы докладов, «проблемные ситуации»

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

Для оценки результатов обучения применяются следующие критерии:

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 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	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
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 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

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

7 СЕМЕСТР

Тема «Введение в дисциплину. Основные виды информационных ресурсов, которые нуждаются в защите»

1. **Доклад-презентация**

Темы докладов:

- Основные исторические этапы развития систем инженерно-технической защиты информации
- Изменение характеристик средств накопления (хранения) информации в электронной форме по мере развития информационных технологий – для различных типов таких средств хранения.
- Надежностные характеристики средств хранения информации – подходы к оценкам и величины оценок.

2. **Анализ «проблемных ситуаций»**

Ситуация 1. Предположим, что Вы уже окончили университет и Вам необходимо разработать комплексный проект обеспечения системы безопасности в организации (Вы можете разрабатывать такой проект и будучи сотрудником проектной организации, а не обязательно той, для которой предназначен проект).

Оцените информация (знания) и умения (компетенции) из каких учебных курсов Вам потребуются для подготовки технического проекта.

В каком объеме потребуются такие знания (градации: в большом объеме; в среднем; в небольшом; в незначительном; не потребуются).

Укажите также направления разработки, по которым с Вашей точки зрения у Вас в настоящий момент недостаточно знаний (компетенций) для разработки такого проекта.

Тема «Условия работы организаций различных типов с позиций необходимости использования мер инженерно-технической защиты информации»

1. **Доклад-презентация**

Темы докладов:

- Изменение содержания мер инженерно-технической защиты информации по мере развития информационных технологий
- Нормативные документы, которые регламентируют необходимость и содержание мер инженерно-технической защиты информации для организаций различных типов.
- Типичные архитектуры систем инженерно-технической защиты информации, которые используются в практике проектирования (для организаций определенного типа).

2. **Анализ «проблемных ситуаций»**

Ситуация 2. Для выбранной Вами организации (реальной или вымышленной) кратко опишите условия ее деятельности.

Оцените состав внешних угроз для деятельности организации и от кого (чего) они могут исходить.

Результаты желательно представить в виде таблицы: по строкам – виды угроз; по столбцам – от кого (чего) они могут исходить. В клетках таблицы – оценки вероятности реализации угроз (качественные).

Обратите внимание, что угрозы могут быть связаны не только с деятельностью «злоумышленников» или конкурентов, но и с общим ухудшением экономической ситуации в стране или регионе; возможностью перерывов в электропитании и пр.

Тема «Общие принципы проектирования и реализации систем инженерно-технической защиты информации»

1. **Анализ «проблемных ситуаций»**

Ситуация 3. Выберите конкретную организацию, кратко опишите условия ее деятельности.

Оцените ее потребности в разработке инженерно-технической системы, предназначенной для обеспечения информационной безопасности (или в модификации существующей системы – если она есть).

Укажите основные принципы, руководствуясь которыми необходимо будет разрабатывать рассматриваемую инженерно-техническую систему защиты информации.

Обоснуйте те принципы, которыми необходимо будет руководствоваться при реализации (внедрении) разработанной системы.

Обоснуйте, в каких случаях может быть необходимо приостановить или вообще прекратить процесс внедрения этой системы.

Ситуация 4. Выберите конкретную организацию, кратко опишите условия ее деятельности.

Охарактеризуйте используемую в ней систему обеспечения информационной безопасности.

Представьте архитектуру этой системы в наглядной (графической) форме.

Укажите на схеме объекты, связанные с хранением резервных копий информации (которые могут быть использованы для целей ее восстановления при необходимости).

Укажите «слабые места» существующей архитектуры и их причины.

Предложите изменения в архитектуре системы инженерно-технической защиты информации, в том числе, возможно, и в отношении количества «рубежей защиты».

Оцените, в каких пропорциях целесообразно распределять средства между различными «рубежами защиты».

Тема «Архитектура инженерно-технической системы защиты информации»

1. **Доклад-презентация**

Темы докладов:

- Типы окон, которые могут использоваться в помещениях, предназначенных для работы с информационными ресурсами.
- Основные типы (виды) мебели которая может использоваться в помещениях, предназначенных для работы с информационными ресурсами
- Типы напольных покрытий, которые могут использоваться в помещениях, предназначенных для работы с информационными ресурсами
- Типы стен, которые могут использоваться в помещениях, предназначенных для работы с информационными ресурсами
- Осветительные устройства, которые могут использоваться в помещениях, предназначенных для работы с информационными ресурсами
- Устройства для обогрева и кондиционирования воздуха, которые могут использоваться в помещениях, предназначенных для работы с информационными ресурсами.
- Датчики систем охранной и пожарной сигнализации, которые могут использоваться в помещениях, предназначенных для работы с информационными ресурсами.
- Электронные пропуска для входа в здания и отдельные помещения – с магнитной полоской и чипованные (анализ предлагаемой номенклатуры устройств, их преимуществ и недостатков)

Тема «Разработка технического проекта инженерно-технической системы защиты информации»

1. **Анализ «проблемных ситуаций»**

Ситуация 5. Возьмите проект инженерно-технической защиты информации, который разработал другой студент (или группа студентов).

Проведите аудит этого проекта в отношении инженерно-технического уровня и эффективности предлагаемых решений, практической реализуемости предлагаемых решений, сроков реализации решений и пр.

Свое мнение представьте по каждому из направлений (их номенклатуру Вы выбираете самостоятельно).

В конце документа дайте итоговую оценку разработанного проекта (по совокупности оцениваемых направлений).

Перечень вопросов к зачету

1. Общая характеристика роли инженерно-технической защиты информационных ресурсов в обеспечении деятельности организаций различных типов.

2. Номенклатура и толкование основных терминов по теме данного курса. Переводы основных терминов на английский язык

3. Характеристика частоты и объемов использования различных видов информационных ресурсов, применяемых в практике деятельности организаций.

4. Состав и степень опасности угроз информационной безопасности в отношении различных видов информационных ресурсов.

5. Номенклатура носителей информации, используемых для ее хранения, обработки и распространения. Особенности угроз для различных типов носителей.

6. Особенности угроз информационной безопасности, связанные со страной и регионом размещения организаций; населенным пунктом и местоположением зданий; помещений, занимаемых в нем организациями.

7. Номенклатура инженерно-технических решений, которые могут использоваться для обеспечения информационной безопасности.

8. Основные цели и ограничения, учитываемые при проектировании новых систем инженерно-технической защиты информации, модернизации уже существующих систем.

9. Математические постановки задач оптимального выбора решений по проектированию систем инженерно-технической защиты информации в четких и нечетких условиях.

10. Принципы выбора архитектуры системы инженерно-технической защиты информации. Важнейшие критерии и ограничения, которые необходимо учитывать при проектировании архитектуры, выборе аппаратно-технических и иных средств в рамках проектируемой архитектуры.

8 СЕМЕСТР

Тема «Разработка рабочей документации инженерно-технической системы защиты информации.»

1. **Доклад-презентация**

Темы докладов:

- Проектные организации в г.Астрахани, которые осуществляют (или могут осуществлять) проектирование инженерно-технических систем защиты информации.
- Проектные организации федерального уровня, работающие в сфере инженерно-технической защиты информации.
- Состав организаций в г.Астрахани, которые могут изготавливать на заказ стеклопакеты и жалюзи – для использования в помещениях, предназначенных для работы с информационными ресурсами (эта тема важна в случае модернизации зданий – с заменой деревянных рам на стеклопакеты, в т.ч. для целей энергосбережения).
- Состав организаций в г.Астрахани, которые могут изготавливать и монтировать тамбурные входы в здания и/или отдельные помещения.
- Номенклатура организаций в России, предлагающих системы контроля доступа в здания с использованием «вертушек» - аналогично используемым на входе в главный корпус Астраханского государственного университета.

Тема «Проектирование помещений для работы с ИР с учетом требований нормативных документов по защите информации»

1. **Доклад-презентация**

Темы докладов:

- Номенклатура программных средств, которые могут использоваться для автоматизированного проектирования систем инженерно-технической защиты информации.
- Номенклатура программных средств, которые могут использоваться для информационного моделирования (информационного проектирования) систем инженерно-технической защиты информации.
- Технические средства, которые могут использоваться для представления проектов систем инженерно-технической защиты информации на бумажных и иных носителях (последний вариант – в рекламно-информационных целях).
- Соответствие форматов файлов с документацией для проектов систем инженерной защиты информации тем программным средствам, в которых эта документация была создана (включая системы автоматизированного проектирования).

Тема «Подготовка и оформление технической документации на поставку технических и программных средств для инженерно-технической системы защиты информации.»

1. **Анализ «проблемных ситуаций»**

Ситуация 6. Выберите конкретную организацию, дайте краткую характеристику условий ее деятельности, включая занимаемое здание (помещения) – в т.ч. его износ.

Оцените необходимость (периодичность) проведения косметических ремонтов, капитального ремонта, реконструкции помещений с установкой перегородок, обустройством фальш-потолка (для обеспечения удобства прокладки кабелей); строительства пристроя к зданию – для увеличения производственных площадей; надстройки здания на 1-2 этажа (если позволяет фундамент); замены в здании внутренних инженерных сетей; замены систем отопления и кондиционирования воздуха; переезда организации в другое здание (или использования дополнительного здания).

В случае недостаточности средств для одновременной реализации всех предложенных мер обоснуйте этапность их реализации.

Ситуация 7. Возьмите результаты выполнения лабораторно-практических заданий по данной теме, которые выполнил другой студент (или группа студентов).

Проведите аудит этих материалов в отношении обоснованности предлагаемых инженерно-технических решений, стоимости их реализации.

Подготовьте отзыв об аудируемой работе – конкретно по отдельным направлениям и в целом по проекту.

Предложите улучшения, которые с Вашей точки зрения сделают предлагаемый проект лучше с позиций обеспечения информационной безопасности (улучшения могут касаться не только выбора оборудования, но и архитектуры системы защиты).

Эти предложения должны быть оформлены в письменной (электронной) форме.

Также желательно провести (дополнительно) анализ внерегиональных организаций, которые смогли бы выполнить необходимые заказные работы, в т.ч. по изготовлению изделий. Это могут быть, в частности, организации в Волгоградской, Саратовской областях, республике Дагестан.

Тема «Критерии оптимальности и ограничения, которые должны учитываться при выборе таких средств»

1. **Анализ «проблемных ситуаций»**

Ситуация 8. Каждый студент (группа студентов) подготавливает технический проект для одной и той же организации, работающей в изменяющихся во времени условиях. Результаты проектирования помимо самого проекта представляются в виде краткой презентации.

Затем проекты публично защищаются. Преподаватель и другие студенты (авторы других проектов) могут при этом задавать вопросы по докладу, а также содержанию разработанного проекта, его техническому оформлению.

Проект-победитель выявляется, таким образом, на конкурсной (конкурентной) основе.

Для подведения итогов у каждого студента (группы студентов) запрашиваются оценки других проектов (не своего) по нескольким ключевым показателям.

Объективности выставления студентами таких оценок проектов также могут оцениваться преподавателями (умение объективно оценивать инженерно-техническую деятельность других лиц является важным направлением компетентности специалистов).

Ситуация 9. Предположим, что среди закупленного оборудования, предназначенного для обеспечения работы системы инженерно-технической защиты информации оказалось 30% бракованных изделий.

Каким образом Вы сможете подтвердить, что это именно заводской (производственный) брак, а не повреждения, связанные с выполнением монтажных или пуско-наладочных работ.

На каких основаниях Вы сможете требовать обмена бракованной продукции на работоспособную и в какие сроки.

Кто будет оплачивать дополнительные стоимости бракованной продукции и заменяющих ее изделий.

Сможете ли Вы через суд добиваться возмещения потерь, обусловленных поставкой некачественной продукции исходя из «упущенной выгоды».

Собираетесь ли Вы эксплуатировать оставшиеся 70% продукции или предпочтете полностью вернуть всю партию изделий поставщику. Что может являться основанием для такого возврата.

Можете ли Вы назначить собственного представителя, который будет участвовать в приемке продукции у ее производителя на его производственной площадке.

Тема «Разработка порядка и этапов внедрения инженерно-технической системы защиты информации»

1. **Доклад-презентация**

Темы докладов:

- Примеры успешных внедрений крупных проектов, включающих использование систем инженерно-технической защиты информации (по России).
- Примеры из зарубежной практики по внедрению инженерно-технических систем защиты информации.

2. **Анализ «проблемных ситуаций»**

Ситуация 10. Выберите конкретную организацию, опишите условия ее деятельности. Дайте характеристику персонала – количество, половозрастная структура, семейное положение, уровни оплаты, занимаемые должности и пр.

Выберите комплекс мер инженерно-технической защиты информации, которые Вы собираетесь внедрять в этой организации, включая программно-технические средства защиты информации. Кратко опишите этот комплекс.

Укажите календарную продолжительность процессов внедрения.

Поясните, какие группы персонала могут оказать сопротивление внедрению предлагаемого Вами комплекса мер по инженерно-технической защите информации; по каким причинам они могут оказать такое сопротивление.

Предложите варианты мер для убеждения персонала в необходимости этих мер, а также административные решения, направленные на соблюдение этих мер.

Если сочтете целесообразным, то предложите варианты материального стимулирования персонала, связанные с внедрением этих мер – однако это необходимо обосновать и указать, что будет являться критериями премирования.

Перечень вопросов к экзамену

1. Методы обеспечения необходимого уровня надежности функционирования системы инженерно-технической защиты информации.
2. Техническое задание на разработку инженерно-технической системы защиты информации: содержание, порядок разработки, согласования и утверждения.
3. Основные этапы разработки технического проекта инженерно-технической системы защиты информации. Характеристика рисков для отдельных этапов и мер риск-менеджмента.
4. Использование средств информационного моделирования при разработке проектов инженерно-технической систем защиты информационных ресурсов.
5. Использование методологии «управления проектами» и соответствующих программных средств при разработке проектов инженерно-технической защиты информации в организациях.
6. Рабочая документация систем инженерно-технической защиты информации: основные требования к документации; содержание; правила составления и утверждения.

7. Использование нормативных документов и нормоконтроль рабочей документации для систем инженерно-технической защиты информации.

8. Учет требований информационной безопасности при проектировании помещений, предназначенных для работы с информационными ресурсами, представленными в различных формах.

9. Принципы комплексирования аппаратных и программных средств при разработке систем инженерно-технической защиты информации с учетом особенностей помещений (зданий), специфики направлений работы организаций.

10. Правила, порядок подготовки и оформления технической документации на поставку технических средств для инженерно-технической системы защиты информации. Использование тендерных процедур для оптимизации условий поставки.

11. Правила, порядок подготовки и оформления технической документации на поставку программных средств для инженерно-технической системы защиты информации. Использование тендерных процедур для оптимизации условий поставки.

12. Понятие о внедрении систем инженерно-технической защиты информации. Особенности внедрения таких систем в организациях различных типов.

13. Типичные этапы внедрения систем инженерно-технической защиты информации. Использование программных средств для планирования действий, связанных с внедрением таких систем (включая построение план-графиков внедрения и различных диаграмм, использования методологии «управления проектами» для мониторинга фактического выполнения запланированных действий и пр.).

14. Цели и методы проведения испытаний систем инженерно-технической защиты информации. Документирование выполняемых действий и выявившихся недочетов при внедрении систем инженерно-технической защиты информации.

15. Использования методов «управления качеством» при эксплуатации внедренных систем инженерно-технической защиты информации – включая проведение аудита, планирование и реализацию корректирующих действий.

16. Влияние развития информационных технологий на номенклатуру угроз информационной безопасности и решения, используемые в рамках систем инженерно-технической защиты информации.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-1 - Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем				
1.	Задание закрытого типа	Вероятностные методы включают такие параметры как 1. вероятности реализации угроз; 2. вероятности обнаружения угроз; ложных тревог; 3. вероятности пресечения несанкционированных действий 4. вероятности ликвидации угроз	1, 2, 3	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		5. вероятности подсчета экономической эфеективности		
2.		При автономной тактике охрана объекта может осуществляться 1. охранниками 2. службой безопасности объекта 3. сторонними охранными структурами 4. подразделениями вневедомственной охраны МВД РФ 5. тревожной сигнализацией	1, 2, 3	2
3.		Первичный преобразователь, реагирующий на воздействие на него (прямое или косвенное) объекта обнаружения и воспринимающий изменение состояния окружающей среды 1. Чувствительный элемент 2. Датчик 3. Выходное устройство 4. Измеритель	1	2
4.		Устройство, применяемое для обработки информации от считывателей идентификаторов, принятия решения, и управления исполнительными устройствами 1. Чувствительный элемент 2. Датчик 3. Контроллер доступа 4. Выходное устройство	3	2
5.		Оптико-электронное устройство, которое преобразует оптическое изображение наблюдаемого объекта в электрический видеосигнал определенного стандарта (набора требований к структуре и характеру составляющих видеосигнала, позволяющего стандартизировать процесс	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		приема/передачи видеоизображений 1. Видеокамера 2. Система охранная телевизионная 3. Видеостена 4. ПЗС-матрица		
6.	Задание открытого типа	Объекты группы AI (особо важные объекты высокой ценности или высокой опасности)	Объекты группы AI (особо важные объекты высокой ценности или высокой опасности): - объекты особо важные, повышенной опасности и жизнеобеспечения, включенные в Перечень объектов подлежащих государственной охране; - объекты, включенные органами власти субъектов РФ или местного самоуправления в перечни объектов особо важных, повышенной опасности и жизнеобеспечения; - объекты по производству, хранению и реализации наркотических веществ, сильнодействующих ядов и химикатов, токсичных и психотропных веществ и препаратов; - ювелирные магазины, базы, склады и другие объекты, использующие в своей деятельности	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			ювелирные изделия, драгоценные металлы и камни; - объекты и помещения для хранения оружия и боеприпасов, радиоизотопных веществ и препаратов, предметов старины, искусства и культуры; - объекты кредитно-финансовой системы; - кассы предприятий, организаций, учреждений, головные кассы крупных торговых предприятий; - сейфовые комнаты, предназначенные для хранения денежных средств, ювелирных изделий, драгоценных металлов и камней; - другие аналогичные объекты и имущественные комплексы.	
7.		Объекты группы AII (наиболее опасные помещения на объектах группы AI):	Объекты группы AII (наиболее опасные помещения на объектах группы AI): - хранилища и кладовые денежных и валютных средств, ценных бумаг; - хранилища ювелирных изделий, драгоценных металлов и камней; - хранилища секретной документации, изделий; - специальные хранилища	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов; - специальные фондохранилища музеев и библиотек.	
8.		Объекты группы БI (объекты розничной торговли и пр.)	Объекты группы БI (объекты розничной торговли и пр.): - объекты с хранением или размещением изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и другого имущества; - объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и другие аналогичные объекты)	2
9.		Объекты группы БII (объекты категории Б, содержащие алкогольную продукцию или наиболее компактные легкосбываемые товары – электронику, товары повседневного спроса)	Объекты группы БII (объекты категории Б, содержащие алкогольную продукцию или наиболее компактные легкосбываемые товары – электронику, товары повседневного спроса):	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			- объекты с хранением или размещением товаров, предметов повседневного спроса, продуктов питания, компьютерной техники, оргтехники, видео- и аудиотехники, кино- и фотоаппаратуры, натуральных и искусственных мехов, кожи, автомобилей и запасных частей к ним, алкогольной продукции с содержанием этилового спирта свыше 13% объема готовой продукции и другого аналогичного имущества.	
10.		Основные разделы концептуального проекта	Основными разделами концептуального проекта являются: 1. Анализ уязвимости объекта и существующей СБ. 2. Разработка принципов комплексной защиты объекта. 3. Разработка технико-экономического обоснования (ТЭО) создания СБ и комплекса ТСОБ.	2
ПК-2 - Способен выполнять работы по установке, настройке и техническом у обслуживанию защищенных технических средств обработки информации				
1.	Задание закрытого типа	Документ, который может использоваться службой безопасности заказчика в качестве руководства по организации системы	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		безопасности (СБ) и планированию работ по оборудованию объекта комплексом технических средств обеспечения безопасности (ТСОБ) или его подсистемами 1. ТЭО 2. СОТ 3. ПЗС 4. ПСПЛ		
2.		Совокупность средств и методов поддержания безопасного состояния объекта, предупреждения, обнаружения и ликвидации угроз жизни, здоровью и среде обитания, имуществу и информации 1. Система безопасности 2. Информационная безопасность 3. Защита информации 4. Система техническая сложная для защиты объекта	1	2
3.		Организационно-техническая система, включающая в себя совокупность технических средств или их комплексов, программное обеспечение, а также документированные процедуры штатных действий персонала, эксплуатационную документацию, материалы, инструменты, приборы, необходимые для использования в комплексной защите объекта 1. Система безопасности 2. Информационная безопасность 3. Защита информации 4. Система техническая сложная для защиты объекта	4	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
4.		К мерам организационного характера при построении и функционировании системы безопасности объектов относятся: 1. правила поведения сотрудников объектов, посетителей и сотрудников службы безопасности, как в штатных, так и во внештатных ситуациях; 2. разработка системы документооборота службы охраны 3. организация систем контроля и управления доступом 4. организация систем охранной и тревожной сигнализации	1, 2	2
5.		В каком документе Вы, как руководитель структурного подразделения, обоснуете свои предложения для руководства фирмы по расширению вашего отдела? 1) в письме 2) в решении 3) в докладной записке 4) в справке	3	2
6.	Задание открытого типа	На какие основные группы подразделяются объекты в зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз?	В зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз объекты подразделяются на три основные группы: – критически важные и потенциально опасные объекты; – социально значимые объекты;	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			– объекты сосредоточения материальных ценностей.	
7.		Какие задачи решаются при предпроектном обследовании, которое проводится с целью анализа уязвимости существующей на объекте системы безопасности (СБ)?	Предпроектное обследование проводится с целью анализа уязвимости существующей на объекте СБ. При этом решаются следующие задачи: - определение объекта охраны и его категории значимости; - составление списка и параметров угроз для объекта охраны; - создание модели нарушителя; - оценка вероятности реализации угроз; - оценка потенциального ущерба при реализации угроз; - оценка эффективности существующей СБ.	8
8.		Какие задачи решаются при разработке ТЭО?	При разработке ТЭО решаются следующие задачи: - разработка структуры СБ и различных вариантов построения комплекса ТСОБ с оценкой стоимости их реализации; - количественная оценка уязвимости СБ с различными вариантами структуры ТСОБ и выбор наиболее	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			эффективного варианта охраны.	
9.		Какие обязательные элементы включаются в рабочую документацию при проектировании системы безопасности (СБ)?	При проектировании системы безопасности (СБ) создается, согласуется и утверждается рабочая документация, включающая следующие обязательные элементы: - структурные и функциональные схемы СБ; - планы объектов с указанием мест размещения оборудования СБ; - схемы соединений; - кабельный журнал; - сметы расходов; - расчетно-пояснительная записка с описанием схем и расчетами для обоснования предлагаемых технических, организационных и тактических аспектов защиты объекта охраны; - описание последовательности оснащения объекта элементами СБ.	8
10.		При выборе технических средств обеспечения безопасности (ТСОБ) в наличии на каждую систему какой документации необходимо предварительно убедиться?	При выборе технических средств обеспечения безопасности (ТСОБ) необходимо предварительно убедиться в наличии на	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			каждую систему следующей документации: - сертификатов соответствия: ГОСТ Р и пожарной безопасности на систему и все блоки, входящие в ее состав; - сертификата ISO 9001 (для импортных систем); - полного комплекта эксплуатационно-технической и ремонтной документации на русском языке; - русифицированного ПО и отображения информации на блоках контроля и управления; - лицензий на проектирование и монтаж соответствующих систем; - наличие предлагаемого оборудования в перечне МВД РФ; - расчета эффективности использования базового комплекта аппаратуры для защиты заданного количества объектов.	

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

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

Доклад-презентация

Защита 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.

Зачет

Зачет проводится в виде письменном ответа на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

Экзамен

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На экзамене осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю) (7 семестр)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	16/2	32	В соответствии с таблицей 2
2.	*Выполнение доклада-презентации*	3/11	33	
3.	*Выполнение ситуационных задач*	5/5	25	
Всего			**90**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*		3	
5.	*Своевременное выполнение всех заданий*		3	
6.	*Активность студента на занятии*		4	
Всего			**10**	-
ИТОГО			**100**	-

Таблица 10а – Технологическая карта рейтинговых баллов по дисциплине (модулю) (8 семестр)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	18/1	18	В соответствии с таблицей 2
2.	*Выполнение доклада-презентации*	3/4	12	
3.	*Выполнение ситуационных задач*	5/2	10	
Всего			**40**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*		3	
5.	*Своевременное выполнение всех заданий*		3	
6.	*Активность студента на занятии*		4	
Всего			**10**	-
Дополнительный блок				
7.	*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)	Не зачтено

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. Информационная безопасность и защита информации / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
2. Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785222269114.html (ЭБС «Консультант студента»).
3. Системы безопасности и устройства кодового доступа: просто о сложном / Кашкаров А.П. - М. : ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747697.html (ЭБС «Консультант студента»).
4. Защита персональных данных в организации / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин - М.: ФЛИНТА, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785976512733.html (ЭБС «Консультант студента»).
5. Информационная безопасность и защита информации / Шаньгин В.Ф. - М: ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. Под ред. А.П. Зайцева и А. А. Шелупанова. - 7-е изд., испр. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202336.html (ЭБС «Консультант студента»).
2. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - Вып. 4. - М. : Горячая линия - Телеком, 2012. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991201797.html (ЭБС «Консультант студента»).

3. Технология проектирования автоматизированных систем обработки информации и управления: Учебное пособие для вузов / Рудинский И.Д. - М. : Горячая линия - Телеком, 2011. - URL: http://www.studentlibrary.ru/book/ISBN9785991201483.html (ЭБС «Консультант студента»).

4. 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.)

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.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

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. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).