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	УТВЕРЖДАЮ И.о. заведующего кафедрой информационной безопасности
Р.Ю. Демина	Р.Ю. Демина
«22» июня 2023 г.	«22» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информационных процессов в компьютерных системах

Составитель(-и)	**Шукралиева Д.Э., доцент кафедры информационной безопасности; Корякова В.А., ассистент кафедры информационных технологий, начальник отдела информационной безопасности**
Направление подготовки	**10.03.01.Информационная безопасность**
Направленность (профиль) ОПОП	**«Организация и технологии защиты информации»**
Квалификация (степень)	**бакалавр**
Форма обучения	**Очная**
Год приема	**2023**
Курс	**3**
Семестр	**6**

Астрахань, 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) «Защита информационных процессов в компьютерных системах» – научить студентов основным принципам и методам, применяемым при защите компьютерных систем.

1.2. Задачи освоения дисциплины (модуля): «Защита информационных процессов в компьютерных системах»:

- ознакомить студентов с основными понятиями, используемыми при защите информации в компьютерных системах;
- дать представление об основных проблемах защиты информации в компьютерных системах;
- обучить студентов методам защиты информации в компьютерных системах для построения защищенных информационных технологий.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Защита информационных процессов в компьютерных системах» относится к элективным дисциплинам и осваивается в 6 семестре.

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

1. Информатика.
2. Техническая защита информации.
3. Аппаратные средства вычислительной техники.

Знания: основных понятий информатики, принципов построения информационных систем, принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

Умения: использовать программные и аппаратные средства персонального компьютера, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности объекта.

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.), выявления и уничтожения компьютерных вирусов; владения методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации.

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

Дисциплина «Защита информационных процессов в компьютерных системах» поможет студентам при 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:

профессиональных (ПК): ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации; ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации	ИПК 2.1. Знать: 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. Уметь: 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. Владеть: методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем	ИПК-3.1. Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации основные меры по защите информации в автоматизированных системах, нормативные правовые акты в области защиты информации	ИПК-3.2. Уметь: администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры настройки программного обеспечения системы защиты информации	ИПК-3.3. Владеть: методикой анализа структурных и функциональных схем защищенной автоматизированной системы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 3 зачетные единицы (108 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. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.*	6	***3***		***5***		***4***	*Лабораторная работа 1, устный опрос*
2.	*Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».сигналов*		***3***		***5***		***4***	Лабораторная работа 2, устный опрос
3.	*Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.*		***3***		***5***		***4***	Лабораторная работа 3, контрольная работа 1, устный опрос
4.	*Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.*		***2***		***6***		***4***	Промежуточное тестирование. Лабораторная работа 4, устный опрос
5.	*Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.*		***2***		***6***		***4***	Лабораторная работа 5, устный опрос
6.	*Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев*		***1***		***6***		***5***	Лабораторная работа 6, контрольная работа 2, устный опрос
7.	*Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.*		***1***		***6***		***5***	Лабораторная работа 7, защита реферата, устный опрос
8.	*Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем*		***1***		***6***		***5***	Лабораторная работа 8. Защита реферата, устный опрос

9.	*Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем*		***1***		***6***		***5***	Контрольная работа 3, устный опрос
	ИТОГО		**17**		**51**		**40**	**ЭКЗАМЕН**

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*		*Общее количество компетенций*
		ПК 2	ПК 3	
Тема 1. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	12	+	+	2
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».сигналов	12	+	+	2
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	12	+	+	2
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	12	+	+	2
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	12	+	+	2
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев	12	+	+	2
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	12	+	+	2
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем	12	+	+	2
Тема 9. Разработка политик безопасности	12	+	+	2

для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем				
Итого	**108**			

Краткое содержание дисциплины

Тема 1

Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.

Тема 2

Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».

Тема 3

Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.

Тема 4

Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.

Тема 5

Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.

Тема 6

Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев

Тема 7

Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.

Тема 8

Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.

Тема 9

Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.

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 практическим занятиям необходимо воспользоваться учебно-методической литературой из п.8. Практические занятия необходимо проводить с использованием презентаций, созданных в Microsoft PowerPoint.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-

методической литературой из п.8, а также пользоваться ресурсами сети Интернет.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

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

Таблица 4 – Содержание самостоятельной работы обучающихся

для очной формы обучения

Номер раздела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
1.	Подготовка к лабораторной работе 1,	4	Внеаудиторная, изучение учебных пособий
2.	Подготовка к лабораторной работе 2	4	Внеаудиторная, изучение учебных пособий
3.	Подготовка к лабораторной работе 3, подготовка к контрольной работе 1	4	Внеаудиторная, изучение учебных пособий
4.	Подготовка к промежуточному тестированию. Подготовка к лабораторной работе 4	4	Внеаудиторная, изучение учебных пособий
5.	Подготовка к лабораторной работе 5	4	Внеаудиторная, изучение учебных пособий
6.	Подготовка к лабораторной работе 6, подготовка к контрольной работе 2	5	Внеаудиторная, изучение учебных пособий
7.	Подготовка к лабораторной работе 7, Подготовка реферата	5	Внеаудиторная, изучение учебных пособий
8.	Подготовка к лабораторной работе 8. Подготовка реферата	5	Внеаудиторная, изучение учебных пособий
9.	Подготовка к контрольной работе 3	5	Внеаудиторная, изучение учебных пособий

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

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 *Times New Roman 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:

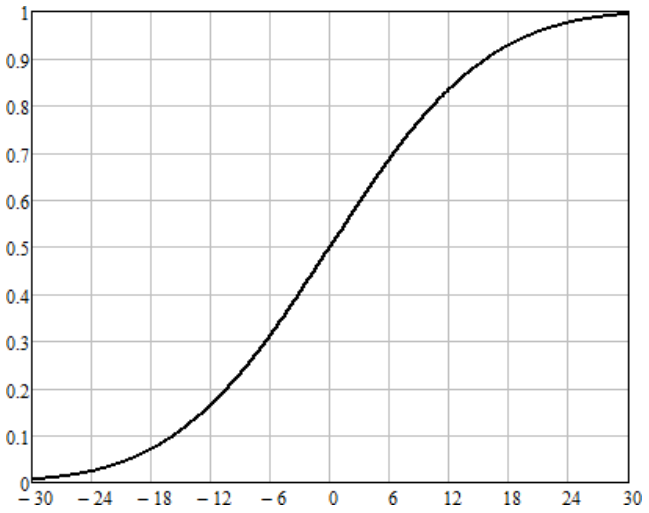

Рисунок 2.12 – Кривая коэффициента восприятия речи

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-Кавказкого региона : 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

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

В соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров в рамках изучения дисциплины предусмотрено использование в учебном процессе следующих активных и интерактивных форм проведения занятий:

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Тема 1. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».сигналов	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 7. Технология построения защищенных компьютерных	Лекция - презентация	Не предусмотрено	выполнение лабораторной

систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.			работы
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы

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%.

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)
Работа с электронными ресурсами	1-9	• Web-сервер Федеральной службы по техническому и экспортному контролю (ФСТЭК России) (правоприемник Государственной технической комиссии при Президенте Российской Федерации) http://www.fstec.ru/ • Два портала по информационной безопасности: http://infosecurity.report.ru/ http://www.void.ru/ • Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности http://www.jetinfo.ru
Использование возможностей электронной почты преподавателя	1-9	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1-9	Использование мультимедийной презентации

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов 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 (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров]

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

6.3.1. Программное обеспечение

В соответствии с ОПОП дисциплина должна быть поддержана соответствующими лицензионными программными продуктами.

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
MS Visual Studio	Среда разработки программ для ЭВМ

6.3.2. Современные профессиональные базы данных и информационные справочные системы

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

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. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.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) «Защита информационных процессов в компьютерных системах» 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	Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	ПК 2, ПК 3	Лабораторная работа 1
2	Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	ПК 2, ПК 3	Лабораторная работа 2
3	Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	ПК 2, ПК 3	Лабораторная работа 3, контрольная работа 1
4	Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	ПК 2, ПК 3	Промежуточное тестирование. Лабораторная работа 4
5	Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	ПК 2, ПК 3	Лабораторная работа 5
6	Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев	ПК 2, ПК 3	Лабораторная работа 6, контрольная работа 2
7	Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	ПК 2, ПК 3	Лабораторная работа 7, защита реферата
8	Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	ПК 2, ПК 3	Лабораторная работа 8. Защита реферата
9	Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	ПК 2, ПК 3	Контрольная работа 3. Вопросы к экзамену

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

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания

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
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 и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема «Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.»

1. Практическое занятие

Вопросы для обсуждения:

Информационные технологии и информационные системы.

Примеры информационных технологий и информационных систем. Типы компьютерных систем, как элементов информационных технологий. Основные принципы успешного функционирования информационной (компьютерной) системы. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений. Основные принципы и методы защиты информационных процессов в компьютерных системах.

Проектирование и разработка защищенных информационных технологий

Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении. CASE-технологии создания информационных систем. Стандарт ITIL.

2. **Лабораторная работа 1.** Сравнительный анализ различных стандартов в области защиты информационных технологий с точки зрения эффективности достижения цели построения защищенных информационных систем.

Тема «Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».»

1. **Практическое занятие**

Вопросы для обсуждения:

Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга». Американский стандарт по защите информации «Оранжевая книга». Понятие гарантии защиты. Критерии оценки защищенности баз данных. Содержание классов защищенности. Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.

2. **Лабораторная работа 2.** Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев

Тема «Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC»

1. **Практическое занятие**

Вопросы для обсуждения:

Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC. Европейский стандарт по защите информации ITSEC. Понятие гарантии защиты в соответствии с европейским стандартом. Критерии оценки защищенности. Содержание классов защищенности. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения защищенных информационных систем.

2. **Лабораторная работа 3.** Анализ рисков для информационной системы предприятия (организации) и построение модели угроз безопасности

3. **Контрольная работа 1**

Вопросы к контрольной работе 1:

1. Примеры информационных технологий и информационных систем.
2. Типы компьютерных систем, как элементов информационных технологий.
3. Основные принципы успешного функционирования информационной (компьютерной) системы.
4. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
5. Основные принципы и методы защиты информационных процессов в компьютерных системах.
6. Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий.
7. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
8. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
9. CASE-технологии создания информационных систем.
10. Стандарт ITIL.
11. Американский стандарт по защите информации «Оранжевая книга».
12. Европейский стандарт по защите информации ITSEC.

Тема «Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.»

1. **Практическое занятие**

Вопросы для обсуждения

Подход к безопасности компьютерных систем в CC и базовые концепции

Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности. Содержание политики безопасности.

2. **Промежуточное тестирование**

Пробные тесты:

Тест 1. Выбрать правильные варианты ответов:

По каким критериям оценивается степень доверия по стандарту «Критерии оценки надежности компьютерных систем»

- Политика безопасности
- Уровень гарантированности
- Уровень безопасности
- Уровень секретности
- Концепция безопасности

Тест 2. Выбрать правильные варианты ответов:

Монитор обращений (по стандарту «Критерии оценки надежности компьютерных систем») должен обладать следующими качествами:

- Изолированность
- Полнота
- Верифицируемость
- Надежность
- Безопасность
- Подлинность

Тест 3. Выбрать правильные варианты ответов:

Согласно «Оранжевой книге», метки безопасности состоят из следующих частей –

- уровня секретности
- списка категорий
- уровня безопасности
- списка критериев
- уровня гарантированности
- принудительного управления доступом

Тест 3. Выбрать правильные варианты ответов:

Какие аспекты затрагивает гарантированность в стандарте «Гармонизированные критерии европейских стран»

- эффективность
- корректность средств безопасности
- мощность
- надежность
- быстродействие
- производительность

Тест 4. Выбрать правильные варианты ответов:

По стандарту «Гармонизированные критерии европейских стран» определяются следующие градации мощности

- базовая
- средняя
- высокая
- низкая

- основная
- дополнительная

Тест 5. Выбрать правильный вариант ответа:
В каком году в Германии вышло «Руководство по защите информационных технологий для базового уровня», дальнейшем которое было оформлено в виде германского стандарта BSI.

- 1998
- 2000
- 2002
- 2010

3. **Лабораторная работа 4.** Порядок сертификации средств защиты информации для разработчика СЗИ.

Тема «Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.»

1. **Практическое занятие**

Вопросы для обсуждения:

Классы защищенности в системе общих критериев. Понятие аудита политики безопасности. Требования к подсистемам аудита. Подсистемы подтверждения подлинности отправки и получения сообщения. Подсистемы разграничения доступа. Подсистемы идентификации и аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы. Подсистемы защиты связи. Требования к подсистемам, предъявляемые в каждом классе защищенности.

Гарантии безопасности компьютерных систем в системе общих критериев

Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

2. **Лабораторная работа 5.** Порядок сертификации защищенных информационных систем.

Тема «Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев»

1. **Практическое занятие**

Вопросы для обсуждения:

Каналы утечки и их анализ в системе общих критериев

Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.

Безопасное функционирование в системе общих критериев

Управление конфигурацией. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

2. **Лабораторная работа 6.** Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем для руководителя предприятия (организации) – соискателя лицензии

3. **Контрольная работа 2**

Вопросы к контрольной работе 2:

1. Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности.
2. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности.
3. Содержание политики безопасности.
4. Классы защищенности в системе общих критериев.
5. Понятие аудита политики безопасности. Требования к подсистемам аудита.
6. Подсистемы подтверждения подлинности отправки и получения сообщения.
7. Подсистемы разграничения доступа.
8. Подсистемы идентификации и аутентификации.

9. Подсистемы защиты функций защиты.
10. Подсистемы защиты ресурсов системы.
11. Подсистемы защиты связи.
12. Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
13. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.
14. Управление конфигурацией. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

Тема «Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз»

1. **Практическое занятие**

Вопросы для обсуждения:

Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в открытых сетях. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных. Анализ рисков. Модель противника, возможности противника. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

Модель угроз.

2. **Лабораторная работа 7.** Разработка профиля защиты и построение политик безопасности для компьютерной системы предприятия (организации)

3. **Защита реферата**

Тематика рефератов:

1. Основные угрозы информации, обрабатываемой в компьютерных системах.
2. Особенности построения систем защиты информации в зависимости от источника угроз.
3. Использование средств разграничения доступа для повышения защищённости компьютерных систем.
4. Использование мониторов безопасности повышения защищённости компьютерной системы.
5. Особенности реализации политик безопасности в компьютерных системах.
6. Изменение конфигурации оборудования для повышения защищённости компьютерных систем.
7. Использования шифрования для повышения защищённости компьютерных систем.
8. Межсетевые экраны. Назначение, основные виды, особенности использования.
9. Виртуальные частные сети. Назначение, основные виды, особенности использования.

Тема «Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем»

1. **Практическое занятие**

Вопросы для обсуждения:

Анализ критичных технологий

Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.

Государственная политика в области безопасности компьютерных систем

Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа

2. **Лабораторная работа 8.** Проведение аттестационных испытаний компьютерных

систем в защищенном исполнении и выдача «Аттестата соответствия»

3. Защита реферата

Тематика рефератов:

1. Системы обнаружения атак. Назначение, основные виды, особенности использования.
2. Криптографические методы защиты информации.
3. Механизмы повышения защищённости, реализуемые в центральном процессоре.
4. Механизмы повышения защищённости, реализуемые во внешних устройствах.
5. Механизмы защиты файловых систем.
6. Скрытые каналы по памяти и по данным. Борьба со скрытыми каналами.
7. Перспективы обеспечения защиты информационных процессов в компьютерных системах.
8. Защита информационных ресурсов от несанкционированного доступа.
9. Защита информационных процессов в распределенных компьютерных системах.

Тема «Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем»

1. Практическое занятие

Вопросы для обсуждения:

Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.

Порядок аттестации защищенных компьютерных систем

Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

2. Контрольная работа 3

Вопросы к контрольной работе 3:

1. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах.
2. Специфика возникновения угроз в открытых сетях.
3. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных.
4. Анализ рисков. Модель противника, возможности противника.
5. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
6. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.
7. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.
8. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
9. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа
10. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.
11. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.
12. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации.
13. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
14. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Примерный план проведения лабораторно-практического занятия

1. Студенты распределяются по группам. Студентами выбирается одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.
2. Определяются принципы защиты информации в компьютерных системах организации.
3. Формулируются основные задачи и мероприятия защите информации в компьютерных системах организации.
4. Определяются проблемные вопросы, связанные с организацией защиты информации на предприятии по соответствующей теме занятия.
5. Каждой группе студентов выдаются задания (ситуации) и каждая из групп должна в роли руководителя, начальника службы безопасности, специалиста по защите информации и т.д. решать управленческие задачи, связанные с организацией защиты информации на предприятии (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
6. Студентами каждой группы обсуждаются вопросы с целью выработки общих позиций.
7. Руководителями каждой группы излагаются позиции по совершенствованию рекомендуемых мероприятий защиты информации
8. Подводятся итоги занятия с объявлением окончательных оценок участников занятия.

Для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (далее вместе – обучающиеся с ограниченными возможностями здоровья) предусмотрена система обучения с использованием дистанционных образовательных технологий.

Перечень вопросов к экзамену

1. Примеры информационных технологий и информационных систем.
2. Типы компьютерных систем, как элементов информационных технологий.
3. Основные принципы успешного функционирования информационной (компьютерной) системы.
4. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
5. Основные принципы и методы защиты информационных процессов в компьютерных системах.
6. Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий.
7. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
8. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
9. CASE-технологии создания информационных систем.
10. Стандарт ITIL.
11. Американский стандарт по защите информации «Оранжевая книга».
12. Европейский стандарт по защите информации ITSEC.
13. Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности.
14. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности.
15. Содержание политики безопасности.
16. Классы защищенности в системе общих критериев.
17. Понятие аудита политики безопасности. Требования к подсистемам аудита.
18. Подсистемы подтверждения подлинности отправки и получения сообщения.
19. Подсистемы разграничения доступа.
20. Подсистемы идентификации и аутентификации.
21. Подсистемы защиты функций защиты.
22. Подсистемы защиты ресурсов системы.

23. Подсистемы защиты связи.

24. Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

25. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.

26. Управление конфигурацией. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

27. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах.

28. Специфика возникновения угроз в открытых сетях.

29. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных.

30. Анализ рисков. Модель противника, возможности противника.

31. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.

32. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

33. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.

34. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.

35. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа

36. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.

37. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.

38. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации.

39. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.

40. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации				
1.	Задание закрытого типа	В каком году был принят Международный стандарт ISO 17799? 1. 1998 2. 2000 3. 2002 4. 2010	2	2
2.		В каком году в Германии вышло "Руководство по защите	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		информационных технологий для базового уровня", дальнейшем которое было оформлено в виде германского стандарта BSI. 1. 1998 2. 2000 3. 2002 4. 2010		
3.		Какие аспекты затрагивает гарантированность в стандарте "Гармонизированные критерии европейских стран" 1. эффективность 2. корректность средств безопасности 3. мощность 4. надежность 5. быстродействие 6. производительность	1, 2	2
4.		По каким критериям оценивается степень доверия по стандарту «Критерии оценки надежности компьютерных систем» 1. Политика безопасности 2. Уровень гарантированности 3. Уровень безопасности 4. Уровень секретности 5. Концепция безопасности	1, 2	2
5.		По стандарту "Гармонизированные критерии европейских стран" определяются следующие градации мощности 1. базовая 2. средняя 3. высокая 4. низкая 5. основная 6. дополнительная	1, 2, 3	2
6.	Задание открытого типа	Какие шаги рекомендуется проделать для определения последствий нарушения безопасности?	Для определения последствий нарушения безопасности рекомендуется проделать следующие шаги: зафиксировать инцидент с помощью записи сетевою трафика, снятия копий файлов журналов, активных учетных записей и сетевых подключений; ограничить дальнейшие	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			нарушения путем отключения учетных записей, отсоединения сетевого оборудования от локальной сети и от Интернета; провести резервное копирование скомпрометированных систем для проведения детального анализа повреждений и метода атаки; попытаться найти другие подтверждения компрометации (часто при компрометации системы оказываются затронутыми другие системы и учетные записи); хранить и просматривать файлы журналов устройств безопасности и сетевого мониторинга, так как они часто являются ключом к определению метода атаки.	
7.		Типы АИС по структуре	По структуре АИС подразделяются на три типа: 1) на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (АРМ); 2) комплексы АРМ, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные системы); 3) комплексы АРМ и (или) локальных систем, объединенных в единую информационную систему средствами связи с	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			использованием технологии удаленного доступа (распределенные информационные системы).	
8.		Класс, которые присваивается типовой информационной системе по результатам анализа исходных данных	По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов: • класс 1 (К1) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных; • класс 2 (К2) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к средним негативным последствиям для субъектов персональных данных; • класс 3 (К3) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных; • класс 4 (К4) – системы, для которых нарушение заданной характеристики безопасности	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.	
9.		Основные направления деятельности в области аудита безопасности информации	Основными направлениями деятельности в области аудита безопасности информации являются: 1. Аттестация объектов информатизации по требованиям безопасности информации. 2. Контроль защищенности информации ограниченного доступа. 3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН). 4. Проектирование объектов в защищенном исполнении	2
10.		Масштабы проведения аудита	Масштабы проведения аудита: 1. Аудит безопасности всей фирмы в комплексе. 2. Аудит безопасности отдельных зданий и помещений (выделенные помещения). 3. Аудит оборудования и технических средств конкретных типов и видов. 4. Аудит отдельных видов и направлений деятельности:	2
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем				
1.	Задание закрытого типа	Действия против средств электронных коммуникаций, радиосвязи, радаров,	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		компьютерных сетей – 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна		
2.		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 информационная война 4. Кибервойна	4	2
3.		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
4.		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 6. экономические средства	1, 2, 3	2
5.		В «Оранжевой книге» рассматривается несколько видов гарантированности 1. операционная 2. технологическая 3. информационная 4. техническая 5. безопасная 6. подлинная	1, 2	2
6.	Задание открытого типа	Аспекты ИБ в соответствии со стандартом BS 7799	Аспектами ИБ в соответствии со стандартом BS 7799	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			являются: • Политика безопасности. • Организация защиты. • Классификация и управление информационными ресурсами. • Управление персоналом. • Физическая безопасность. • Администрирование компьютерных систем и сетей. • Управление доступом к системам. • Разработка и сопровождение систем. • Планирование бесперебойной работы организации. • Проверка системы на соответствие требованиям ИБ.	
7.		Какие тома должны входить в комплект документации надежной системы согласно "Оранжевой книге"?	Согласно "Оранжевой книге", в комплект документации надежной системы должны входить следующие тома: • Руководство пользователя по средствам безопасности. • Руководство администратора по средствам безопасности. • Тестовая документация. • Описание архитектуры.	2
8.		Элементы, которые должна обязательно включать в себя политика безопасности согласно «Оранжевой книге»	Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы: • произвольное управление доступом; • безопасность повторного использования объектов;	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			• метки безопасности; • принудительное управление доступом.	
9.		Согласно «Оранжевой книге» дать определение политики безопасности	Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.	2
10.		Согласно «Оранжевой книге» дать определение уровня гарантированности	Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности.	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			Это пассивный аспект защиты.	

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)

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению зачета

Отчет по лабораторной работе

Отчет по лабораторной 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 лабораторной работе должны быть указаны:

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

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.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине отводится 100 баллов (90 баллов на текущие формы контроля и до 10 баллов отводится на бонусы), которые накапливаются студентом в течение всего семестра изучения дисциплины.

Каждая лабораторная работа (всего 8) оценивается максимально в 5 баллов, контрольная работа (всего 3) оценивается максимально в 5 баллов, тестирование – 3 баллов, реферат – максимально 4 балла, за активность на каждом практическом занятии (14 занятий) максимально 2 балла.

10 баллов предусмотрено на бонусы: участие с докладами на научных конференциях – максимально 5 баллов, активность студента на занятии – максимально 3 балла, отсутствие

пропусков лекции (посетил все лекции) – максимально 1 балл, отсутствие пропусков практических занятий – максимально 1 балл.

Оценивание студентов на зачете 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 зачета.

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 зачете 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)

№ 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*	8/2	16	
3.	*Выполнение контрольной работы*	3/3	9	
4.	*Тест*	1/3	3	
5.	*Реферат*	1/3	3	
Всего			**40**	-
Блок бонусов				
6.	*Посещение занятий без пропусков*	1	3	
7.	*Своевременное выполнение всех заданий*	1	3	
8.	*Активность студента на занятии*	1	4	
Всего			**10**	-
Дополнительный блок				
9.	**Экзамен**		**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)	
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	

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. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).
2. Политики безопасности компании при работе в Интернет [Электронный ресурс] / С.А. Петренко, В.А. Курбатов - М. : ДМК Пресс, 2018. - http://www.studentlibrary.ru/book/ISBN9785937000576.html.
3. Введение в программную инженерию [Электронный ресурс]: учебное пособие / Соловьев Н.А. - Оренбург: ОГУ, 2017. - http://www.studentlibrary.ru/book/ISBN9785741016855.html

8.2. Дополнительная литература

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202572.html (ЭБС «Консультант студента»).
2. Интеллектуальные системы защиты информации : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785942756673.html (ЭБС «Консультант студента»).
3. Интеллектуальные интерактивные системы и технологии управления удаленным доступом (Методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intranet): Учебное пособие / Ботуз С.П. - 3-е изд., доп. - М. : СОЛОН-ПРЕСС, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785913591326.html (ЭБС «Консультант студента»).
4. Куприянова, А.И. Основы защиты информации : доп. УМО по образованию в области авиации, ракетостроения и космоса в качестве учеб.пособ. для студ., обуч. по спец. "Радиоэлектронные системы", "Средства радиоэлектронной борьбы" и "Информационные системы и технологии" / А. И. Куприянова, Сахаров, А.В., Шевцов, В.А. - - М. : Академия, 2008. - 256 с. (11 экз.)
5. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: Рек. УМО вузов по университетскому п/тех. образованию в качестве учеб. пособ.

для вузов... по специальности "Информатика и вычислительная техника" / П. Б. Хорев,. - М.: Акдемия, 2005. - 256 с. (69 экз.)

6. Садердинов, А.А. Информационная безопасность предприятия: Учеб. пособ. - 2-е изд. - М.: Дашков и К, 2005. - 336 с. (45 экз.)

7. Девянин, П.Н. Модели безопасности компьютерных систем : Доп. УМО объединением вузов по образованию в области информационной безопасности в качестве учеб. пособ. для вузов... по специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / П. Н. Девянин. - М. : Академия, 2005. - 144 с. (50 экз.)

4. 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. Галатенко, В.А. Основы информационной безопасности : Курс лекций. Учебное пособие. Рек. для вузов ... по специальностям в области информационных технологий / В. А. Галатенко ; Под ред. В.Б. Бетелина. - Изд. 3-е. - М. : ИНТУИТ. РУ "Интернет-университет Информационных Технологий", 2004 - 264 с. (45 экз.)

5. Технологии борьбы с компьютерными вирусами. Практическое пособие. - М.: СОЛОН-ПРЕСС, 2009. - 352 с.: ил. - URL: http://www.studentlibrary.ru/book/ISBN9785913590596.html (ЭБС «Консультант студента»).

6. Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. - М. : Компания АйТи; ДМК Пресс. 2004. - 288 с.: ил. - (Информацион ные технологии для инженеров). URL: http://www.studentlibrary.ru/book/ISBN5940742483.html (ЭБС «Консультант студента»).

7. Марьенков А.Н., Лим В.Г., Обеспечение информационной безопасности вычислительных сетей: Учебно-методическое пособие для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» (учебно-методическое пособие). Сорокин Роман Васильевич, Астрахань, 2018. 72с. (5 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).