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
«06» июня 2024 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ
_____ Т.Г. Гурская
протокол заседания кафедры № 9
от «06» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программно-аппаратные средства защиты информации

Составитель(-и)	**Демина Р.Ю., к.т.н., доц., доцент**
Направление подготовки	**09.03.02 Информационные системы и технологии**
Направленность (профиль) ОПОП	**«Безопасность информационных систем»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очно-заочная**
Год приема	**2021**
Курс	**4**
Семестр	**8**

Астрахань, 2024г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) «Программно-аппаратные средства защиты информации» является формирование у студентов знаний по основам защиты информации с помощью программных и программно-аппаратных средств защиты, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач программно-аппаратной защиты информации с учетом требований системного подхода.

1.2. Задачи освоения дисциплины (модуля):

– дать знания по:

– концепции программно-аппаратной защиты информации;

– теоретическим основам программно-аппаратной защиты информации;

– физическим основам программно-аппаратной защиты информации;

– техническим и программным средствам программно-аппаратной защиты

– организационным основам программно-аппаратной защиты информации;

– методическому обеспечению программно-аппаратной защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Программно-аппаратные средства защиты информации» относится к части, формируемой участниками образовательных отношений направления подготовки бакалавров 09.03.02 Информационные системы и технологии. «Безопасность информационных систем» приема 2022 года, и осваивается в 8 семестре 4 курса, обучение длится один семестр.

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

- Техническая защита информации.
- Методы и средства криптографической защиты информации.
- Основы программирования.

В результате освоения этих дисциплин, студент должен:

знать:

– современные средства разработки и анализа программного обеспечения на языках высокого уровня;

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

- принципы организации информационных систем в соответствии с требованиями по защите информации;

уметь:

− анализировать и оценивать угрозы информационной безопасности объекта;

− применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

− составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

− пользоваться нормативными документами по защите информации;

владеть:

− методами технической защиты информации;

− методами расчета и инструментального контроля показателей технической защиты информации;

− навыками выявления и уничтожения компьютерных вирусов;

− методами и средствами выявления угроз безопасности автоматизированным системам.

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

– Основы управления информационной безопасностью.

– Проектирование и эксплуатация защищённых информационных систем.

Также дисциплина «Программно-аппаратные средства защиты информации» поможет студентам при реализации задач производственной практики и написанию 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):

профессиональных (ПК): ПК-1. Способен проводить научные исследования при разработке, внедрении и сопровождении информационных технологий и систем на всех этапах жизненного цикла;

ПК-3. Способность выполнять работы по созданию (модификации) и сопровождению информационных систем и обеспечению их информационной безопасности.

В результате освоения дисциплины обучающийся должен:

Знать:

- виды, источники и носители защищаемой информации,
- основные угрозы безопасности информации,
- аппаратные средства вычислительной техники,
- основные принципы и методы программно-аппаратной защиты информации.

Уметь:

- описывать (моделировать) объекты защиты и угрозы безопасности информации,
- применять наиболее эффективные методы и средства программно-аппаратной защиты информации,
- строить политику безопасности для работы в рамках заданной модели нарушителя на выделенной ПЭВМ,
- контролировать эффективность мер защиты.

Владеть

- профессиональной терминологией,
- методами и средствами выявления угроз безопасности автоматизированным системам,
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов,
- навыками безопасного использования технических средств в профессиональной деятельности.

Таблица 1 – Декомпозиция результатов обучения

Код	Планируемые результаты обучения по дисциплине (модулю)

и наименование компетенции	Знать (1)	Уметь (2)	Владеть (3)
ПК-1. Способен проводить научные исследования при разработке, внедрении и сопровождении информационных технологий и систем на всех этапах жизненного цикла	ИПК-1.1. Знать методы проведения научных исследований на всех этапах жизненного цикла программных средств	ИПК-1.2. Уметь рационально планировать и выполнять научные исследования на всех этапах жизненного цикла программных средств	ИПК-1.3. Владеть навыками планирования и проведения научных исследований на всех этапах жизненного цикла программных средств
ПК-3. Способность выполнять работы по созданию (модификации) и сопровождению информационных систем и обеспечению их информационной безопасности	ИПК-3.1. Знать виды работ по созданию (модификации) и сопровождению информационных систем	ИПК-3.2. Уметь выполнять работы по созданию, сопровождению, модификации и обеспечению информационной безопасности информационных систем.	ИПК-3.3. Владеть навыками выполнения работ по созданию, сопровождению, модификации и обеспечению информационной безопасности информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет 4 зачетные единицы в 8-м семестре (144 часов). 36 часов выделено на контактную работу обучающихся с преподавателем Лекции – 18 часов, лабораторные занятия – 18 часов, курсовая работа – 18 часов, самостоятельная работа – 90 часов.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
			Л	ПЗ	ЛР	КР	СР	
1	**Раздел 1. Основы программно-аппаратных средств информационной безопасности**	7						
2	Тема 1.1 Проблемы обеспечения безопасности информационных систем.		1		1		6	входное тестирование
3	Тема 1.2 Основные понятия информационной безопасности.		1		1		7	Лабораторно-практическая работа 1, контрольная работа 1
4	**Раздел 2. Меры непосредственной защиты вычислительных средств**							
5	Тема 2.1 Общие положения по обеспечению защиты программ и данных		1		1		6	Лабораторно-практическая работа 2
6	Тема 2.2 Принципы защиты программ и данных		1		1		7	контрольная работа 2
7	**Раздел 3. Защита программ от изменений и контроль целостности**							
8	Тема 3.1 Системы защиты от несанкционированного копирования программ		1		1		6	Лабораторно-практическая работа 3
9	Тема 3.2 Особенности построения и программирования внешних запоминающих устройств		1		1		7	контрольная работа 3
10	**Раздел 4. Контроль доступа**							
11	Тема 4.1 Защита от разрушающих программных средств		2		2		6	Лабораторно-практическая работа 4

№ п/п	Наименование радела (темы)	Семестр	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
			Л	ПЗ	ЛР	КР	СР	
	(РПС)							
12	Тема 4.2 Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий.		2		2		7	контрольная работа 4
13	**Раздел 5. Программно-аппаратные средства защиты в интерактивной среде**							
14	Тема 5.1 Классификация типовых программно-аппаратных средств защиты информации, обрабатываемой в ПЭВМ		1		1		6	Лабораторно-практическая работа 5
15	Тема 5.2 Программно-аппаратные средства безопасности ИС.		2		2		6	Лабораторная работа 5, контрольная работа 5
16	Тема 5.3 Система защиты информации ViPNet.		2		2		7	контрольная работа 5
17	**Раздел 6. Прикладные вопросы использования программно-аппаратных средств**							
18	Тема 6.1 Сертификация программно-аппаратных средств на соответствие требованиям информационной безопасности.		1		1		6	Лабораторно-практическая работа 6
19	Тема 6.2 Оценка эффективности программно-аппаратных средств.		1		1		6	контрольная работа 6
20	Тема 6.3 Экономические вопросы выбора состава программно-аппаратных средств.		1		1		7	Итоговое тестирование,

№ п/п	Наименование радела (темы)	Семестр	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
			Л	ПЗ	ЛР	КР	СР	
	Итого		18		18	18	90	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*	*Код компетенции*		*Σ общее количество компетенций*
		ПК 1	*ПК 3*	
Тема 1.1 Проблемы обеспечения безопасности информационных систем.	8	+	+	*2*
Тема 1.2 Основные понятия информационной безопасности.	9	+	+	*2*
Тема 2.1 Общие положения по обеспечению защиты программ и данных	8	+	+	*2*
Тема 2.2 Принципы защиты программ и данных	9	+	+	*2*
Тема 3.1 Системы защиты от несанкционированного копирования программ	8	+	+	*2*
Тема 3.2 Особенности построения и программирования внешних запоминающих устройств	9	+	+	*2*
Тема 4.1 Защита от разрушающих программных средств (РПС)	10	+	+	*2*

Тема 4.2 Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий.	11	+	+	*3*
Тема 5.1 Классификация типовых программно-аппаратных средств защиты информации, обрабатываемой в ПЭВМ	8	+	+	*3*
Тема 5.2 Программно-аппаратные средства безопасности ИС.	10	+	+	*3*
Тема 5.3 Система защиты информации ViPNet.	11	+	+	*2*
Тема 6.1 Сертификация программно-аппаратных средств на соответствие требованиям информационной безопасности.	8	+	+	*2*
Тема 6.2 Оценка эффективности программно-аппаратных средств.	8	+	+	*2*
Тема 6.3 Экономические вопросы выбора состава программно-аппаратных средств.	9	+	+	*2*
Курсовая работа	*18*	+	+	*2*
Итого	*144*			

Содержание разделов дисциплины «Программно-аппаратные средства защиты информации»

Раздел 1. Основы программно-аппаратных средств информационной безопасности

Тема 1.1 Проблемы обеспечения безопасности информационных систем.

Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств. Функциональные требования по защите вычислительных систем. Доктрина информационной безопасности РФ. Утверждена Президентом РФ 09.09.2000. № Пр-1895 // Российская газета. № 187. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. Закон РФ «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 4673.

Тема 1.2 Основные понятия информационной безопасности.

Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения безопасности. Зоны безопасности. Зоны безопасности вычислительной среды. Объекты и элементы защиты. Уровни обеспечения безопасности. Концепция диспетчера и иерархия режимов обеспечения безопасности программными и аппаратными средствами. Сочетание различных методов обеспечения безопасности. Взаимодействие программно-аппаратных средств с общесистемными средствами. Закон РФ «О безопасности» // ВСНД и ВС РФ. 1992. № 15. Ст. 769. Закон РФ «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ. Закон РФ «Об электронной цифровой подписи» от 6 апреля 2011 г. № 63-ФЗ.

Раздел 2. Меры непосредственной защиты вычислительных средств.

Тема 2.1 Общие положения по обеспечению защиты программ и данных

Классификация непосредственных угроз вычислительным устройствам. Защита от стихийных бедствий. Противопожарная защита, защита от затоплений, внезапных изменений электропитания. Защита от непосредственных злоумышленных воздействий: механических и других контактных воздействий, от помех и наводок, меры сигнализации. ГОСТ Р ИСО 7498-2-99. ИТ. ВОС. Базовая эталонная модель. Часть 2. Архитектура защиты информации. ГОСТ Р ИСО/МЭК 9594-8-98. ИТ. ВОС. Справочник. Часть 8. Основы аутентификации. ГОСТ Р ИСО/МЭК 9594-9-95. ИТ. ВОС. Справочник. Часть 9. Дублирование. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем». ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

Тема 2.2 Принципы защиты программ и данных

Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. Методы идентификации и аутентификации пользователей. Идентификация по системе паролей, по стандартному ключу и специальным характеристикам пользователей. Использование методов дублирования и резервирования элементов и устройств для повышения уровня информационной безопасности. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам. Доступ к данным со стороны процесса; способы фиксации факта доступа; надежность систем ограничения доступа. ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы». ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

Раздел 3. Защита программ от изменений и контроль целостности.

Тема 3.1 Системы защиты от несанкционированного копирования программ.

Основные объекты защиты аппаратных средств. Проблема выбора оптимального соотношения между затратами и уровнем защиты. Защита реальной и виртуальной памяти аппаратными средствами: использование регистров границ, ключей и замков, битов управления доступом к памяти, таблиц соответствие адресов. Контроль состояния выпол-

нение программ. Защита файлов от изменения. Защита программ от несанкционированного копирования; пароли и ключи, организация хранения ключей; защита программ от излучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям; Закон РФ «О частной детективной и охранной деятельности» // ВСНД и ВС РФ. 1992. № 17. Ст. 888. Закон РФ «О правовой охране программ для ЭВМ и баз данных» // ВСНД РФ и ВС РФ. 1992. № 42. Ст. 2325. Закон РФ «О внешней разведке» // СЗ РФ. 1996. № 3. Ст. 143.

Тема 3.2 Особенности построения и программирования внешних запоминающих устройств

Применение микропроцессоров для контроля и защиты между различными компонентами вычислительной аппаратуры. Аппаратная реализация функций операционной системы. Средства защиты устройств ввода-вывода. Методы и средства хранения ключевой информации. Закон РФ «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33. Ст. 3349. Закон РФ «О международном информационном обмене» // СЗ РФ. 1996. № 28. Ст. 3347. Закон РФ «О лицензировании отдельных видов деятельности» // СЗ РФ. 1998. № 39. Ст. 4857.

Раздел 4. Контроль доступа.

Тема 4.1 Защита от разрушающих программных средств (РПС).

Классификация компьютерных вирусов и «троянских» программ. Антивирусные программы, их функции и возможности. Средства нарушения безопасности компьютерных сетей. Принципы функционирования РПС. Модель взаимодействия объектов в вычислительной системе с точки зрения безопасности. Защита от разрушающих программных воздействий (РПВ); компьютерные вирусы как особый класс РПВ; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды. Закон РФ от 23.09.92 N 3526-1 *"О правовой охране топологий интегральных микросхем"*. Закон РФ от 10 июня 1993 г. N 5151-1 *"О сертификации продукции и услуг"* (в ред. Федерального закона от 27.12.95 N 211-ФЗ) Закон РФ от 10 июня 1993 г. N 5154-1 *"О стандартизации"* (в ред. Федерального закона от 27.12.95 N 211-ФЗ)

Тема 4.2 Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий.

Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства ограничения доступа. Реализация надзора: ведение протокола, управление доступом, контроль обращения к системе. Технология изоляции пользователя от компьютера и построение изолированной программной среды. Встраивание средств защиты в программное обеспечение. Изоляция области нарушения защиты. Защита от разрушающих программных воздействий. Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий. Методы и средства ограничения доступа к компонентам ЭВМ. Закон РФ от 09.07.93 N 5351-1 *"Об авторском праве и смежных правах"*. Постановление Правительства РФ от 05.12.91 г, № 35 «Перечень сведений, которые не могут составлять коммерческую тайну» // Собрание постановление Правительства РФ. 1992. № 1-2. Ст. 7. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // СЗ РФ. 1995. № 37. Ст. 3619.

Раздел 5. Программно - аппаратные средства защиты в интерактивной среде.

Тема 5.1 Классификация типовых программно-аппаратных средств защиты информации, обрабатываемой в ПЭВМ

Особенности программно - аппаратного обеспечения безопасности в интерактивной среде. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта. Защита информационной среды от нежелательных инфор-

мационных материалов, средства фильтрации сетевой информации. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти // СЗ РФ. 1995. № 17. Ст. 1455. Уголовный Кодекс РФ // СЗ РФ. 1996. № 25. Ст. 2954. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127

Тема 5.2 Программно-аппаратные средства безопасности ИС.

Средства и методы уменьшения риска сделок и переговоров в интерактивной среде. Защита интерактивной среды. Управление вычислительным процессом в интерактивной среде, сценарии поведения. Программно - аппаратные средства защиты интерактивных функций серверов. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ, 1997, № 10, ст. 1127. Указ Президента Российской Федерации от 24 января 1998 г. № 64 «О перечне сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г.) // СЗ РФ. 1995. № 49. ст. 4775; 1998, № 5, ст. 561. Указ Президента Российской Федерации от 12.05.2009 №537 «О стратегии национальной безопасности Российской Федерации до 2020 года».

Тема 5.3 Система защиты информации ViPNet.

Технология системы защиты информации ViPNet. ViPNet [Администратор]. Криптографические системы и их использование в ViPNet. PKI в структуре системы защиты информации. Межсетевое взаимодействие. Компоненты VPN. ViPNet [Клиент]. Логика обработки IP-трафика. Деловая почта. ViPNet [Координатор].

Электронная цифровая подпись (ЭП).

Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных; защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Указ Президента Российской Федерации от 12.05.2004 № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (в редакции от 03.03. 2006). Положение о сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Председателя Гостехкомиссии России от 05.01.1996 № 3. Зарегистрировано Госстандартом России в Государственном реестре 20.03.1995. (Свидетельство №РОСС RU.ООО1.О1БИОО). ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

Раздел 6. Прикладные вопросы использования программно - аппаратных средств.

Тема 6.1 Сертификация программно-аппаратных средств на соответствие требованиям информационной безопасности. Две основные линии развития ОС: открытые и закрытые - Windows и Unix.

Общие положения. Система сертификации. Порядок сертификации. ГОСТ 45.127-99. Система обеспечения информационной безопасности Взаимоувязанной сети связи РФ. Термины и определения. ГОСТ Р 34.10-94. ИТ. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма. ГОСТ Р 34.10-01. ИТ. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.

Тема 6.2 Оценка эффективности программно-аппаратных средств.

Показатели эффективности программно-аппаратных средств. Модели и методы оценки эффективности. Достоверность оценки экономической эффективности предприятий за счет автоматизации управленческих и производственных процессов. ГОСТ Р 34.11-94. ИТ. Криптографическая защита информации. Функция хэширования. ГОСТ Р 50739-95. СВТ. Защита от НСД к информации. ГОСТ Р 51188-98. Испытания ПС на наличие компьютерных вирусов.

Тема 6.3 Экономические вопросы выбора состава программно-аппаратных средств.

Классификация информации по её ценности, анализ угроз, оценка риска и затрат на обеспечение информационной безопасности. ГОСТ Р 51275-99 ЗИ. Объект информатизации. Факторы, воздействующие на информацию. ГОСТ Р 51624-00. ЗИ. АС в защищенном исполнении. Общие требования. ГОСТ Р ИСО/МЭК 15408-2001. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. (часть 1, часть 2, часть 3)

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 (семинарским) занятиям необходимо воспользоваться учебно-методической литературой из п.8. Лекции (семинары) необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

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)

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

Отчет по лабораторной работе

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

Результаты исследования отдельных категорий аудита должны включать описание, как проводились исследования, примеры различных событий данной категории, интерпретацию информации, выдаваемой для отдельных событий, анализ связи отдельных событий, полученные результаты и сделанные результаты и выводы.

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

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.

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.

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 понятие и виды вредоносных программ.
3. Определяются факторы, влияющие на организацию защиты информации на данном предприятии.
4. Формулируются основные задачи и мероприятия программно-аппаратной защиты информации.
5. Определяются проблемные вопросы, связанные с организацией защиты информации на предприятии по соответствующей теме занятия.
6. 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 от вирусов на предприятии (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
7. Студентами каждой группы обсуждаются вопросы с целью выработки общих позиций.
8. Руководителями каждой группы излагаются позиции по совершенствованию рекомендуемых мероприятий защиты информации
9. Подводятся итоги занятия с объявлением окончательных оценок участников занятия.

На учебном файловом сервере АГУ (fsever) размещены задания для лабораторной и самостоятельной работы студентов, тесты, а также лекционный материал.

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

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Раздел 1.	**Основы программно-аппаратных средств информационной безопасности**		
Тема 1.1.	Подготовка к тестированию	6	входное тестирование
Тема 1.2	Подготовка к лабораторной работе №1. Подготовка к контрольной работе №1	7	Лабораторно-практическая работа 1, контрольная работа 1
Раздел 2.	**Меры непосредственной защиты вычислительных средств**		
Тема 2.1	Подготовка к лабораторной работе №2.	6	Лабораторно-практическая работа 2
Тема 2.2	Подготовка к контрольной работе №2	7	контрольная работа 2
Раздел 3.	**Защита программ от изменений и контроль целостности**		
Тема 3.1	Подготовка к лабораторной работе №3.	6	Лабораторно-практическая работа 3
Тема 3.2	Подготовка к контрольной работе №3.	7	контрольная работа 3
Раздел 4.	**Контроль доступа**		
Тема 4.1	Подготовка к лабораторной работе №4.	6	Лабораторно-практическая работа 4
Тема 4.2	Подготовка к контрольной работе №4.	7	контрольная работа 4
Раздел 5.	**Программно-аппаратные средства защиты в интерактивной среде**		
Тема 5.1	Подготовка к лабораторной работе №5.	6	Лабораторно-практическая работа 5
Тема 5.2	Подготовка к лабораторной работе №5. Подготовка к контрольной	6	Лабораторная

	работе №5.		работа 5, контрольная работа 5
Тема 5.3	Подготовка к контрольной работе №5.	7	контрольная работа 5
Раздел 6.	**Прикладные вопросы использования программно-аппаратных средств**		
Тема 6.1	Подготовка к контрольной работе №6.	6	Лабораторно-практическая работа 6
Тема 6.2	Подготовка к контрольной работе №6.	6	контрольная работа 6
Тема 6.3	Подготовка к тестированию	7	Итоговое тестирование

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

Курсовой проект

Курсовой проект должен оформляться в электронном и печатном виде на листах формата А4 и содержать задание, краткие необходимые теоретические сведения, полученные по каждому пункту задания результаты и выводы.

Правила оформления текста пояснительной записки курсового проекта

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, тема курсового проекта, 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.

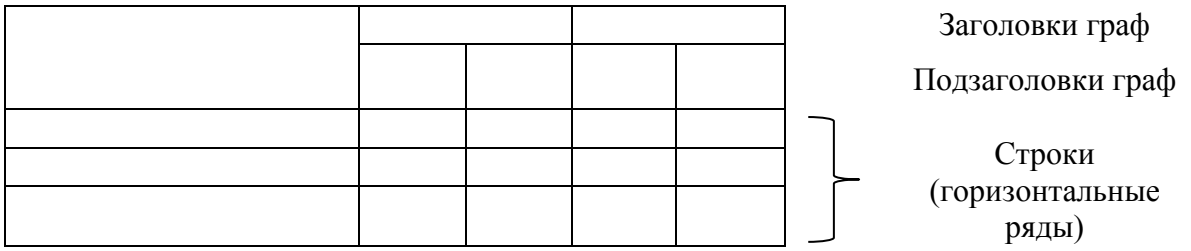
Ссылка в тексте на формулу: «…в формуле (3.1)».

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 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».

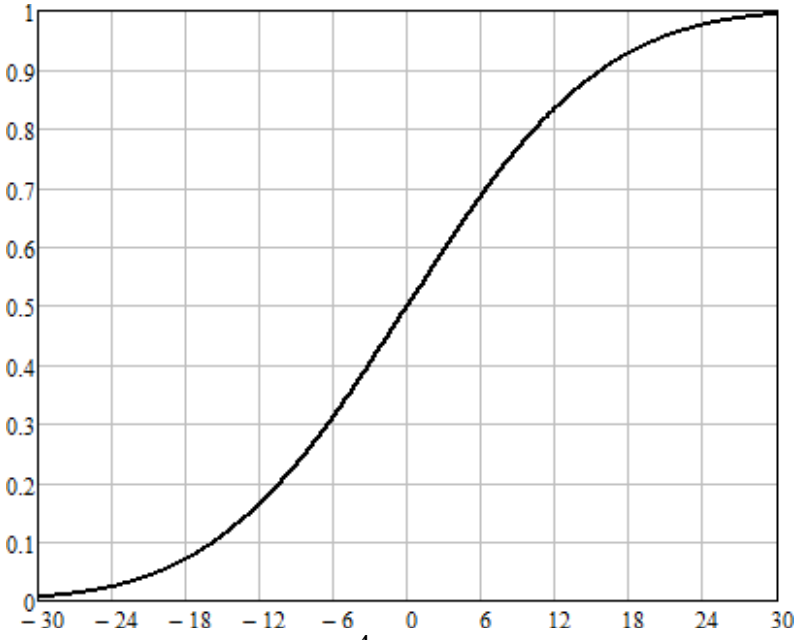
Продолжение Таблицы 2.1

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:



4.

5. Рисунок 2.12 – Кривая коэффициента восприятия речи

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

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

7. Рисунок В.1 – Название рисунка

8.

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

Защита курсового проекта 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.

Критерии оценки курсового проекта:

– оценка «отлично» выставляется обучающемуся, если студент представил курсовой проект в соответствии с методическими указаниями, информация в курсовом проекте сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы в области информационной безопасности, умеет применять программно-аппаратные средства защиты информации;

– оценка «хорошо» выставляется обучающемуся, если студент представил курсовой проект в соответствии с методическими указаниями, информация в курсовом проекте сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы в учтены основные нормативно-правовые документы в области информационной безопасности, умеет применять программно-аппаратные средства защиты информации, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил курсовой проект в соответствии с методическими указаниями, информация в курсовом проекте сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на учтены основные нормативно-правовые документы в области информационной безопасности, умеет применять некоторые программно-аппаратные средства защиты информации;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил курсовой проект или выполнил его неверно, без использования методических указаний, обоснования неверные, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы учтены основные нормативно-правовые документы в области информационной безопасности, не умеет применять программно-аппаратные средства защиты информации.

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
Тема 1.1 Проблемы обеспечения безопасности информационных систем.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 1.2 Основные понятия информационной безопасности.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 2.1 Общие положения по обеспечению защиты программ и данных	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 2.2 Принципы защиты программ и данных	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 3.1 Системы защиты от несанкционированного копирования программ	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 3.2 Особенности построения и программирования внешних запоминающих устройств	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 4.1 Защита от разрушающих программных средств (РПС)	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 4.2 Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 5.1 Классификация типовых программно-аппаратных средств защиты информации, обрабатываемой в ПЭВМ	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 5.2 Программно-аппаратные средства безопасности ИС.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 5.3 Система защиты информации ViPNet.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 6.1 Сертификация программно-аппаратных средств на соответствие требованиям информационной безопасности.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 6.2 Оценка эффективности программно-аппаратных	Лекция - презентация	Не предусмотрено	выполнение лабораторной ра-

средств.			боты
Тема 6.3 Экономические вопросы выбора состава программно-аппаратных средств.	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. В соответствии с требованиями ФГОС ВПО по направлению подготовки бакалавров в рамках изучения дисциплины «Программно-аппаратные средства защиты информации» предусмотрено использование в учебном процессе следующих активных и интерактивных форм проведения занятий:

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

6.2. Информационные технологии

– 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
MathCad 14	Система компьютерной алгебры из класса систем автоматизированного проектирования, ориентированная на подготовку интерактивных документов с вычислениями и визуальным сопровождением, отличается лёгкостью использования

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
Платформа IPC-25*NFR АПКШ «Континент» 3.7	Детектор атак
«Континент» АПКШ 3.7. ЦУС-платформа IPC-25 (4 порта)	Сервер доступа.
ASA 5512-X with SW.6GE Data 1GE Mgmt.AC.DES	Межсетевой экран Cisco.
Учебно-методический комплекс ViPNet "Программно-аппаратная защита информации"	• Учебное пособие - Система защиты информации ViPNet (курс лекций) • Учебное пособие - Система защиты информации ViPNet (практикум) • Учебное пособие - Программно-аппаратные комплексы ViPNet (практикум) • Учебное пособие - Технология построения виртуальных защищенных сетей ViPNet Windows&Linux (практикум) • CD-диск (содержащий программное обеспечение и лицензии предназначенный для проведения лабораторных работ, дополнительные материалы) • Программно-аппаратный комплекс ViPNet Coordinator HW1000. • Программно-аппаратный комплекс ViPNet Coordinator HW100C.
TrustAccess	Для защиты 1 сервера

TrustAccess	Для защиты 1 рабочей станции.
«Соболь» (версия 3.0), PCI (NFR-образец)	Комплекс программно-аппаратный.
«Соболь» (версия 3.0), PCI-E (NFR-образец)	Комплекс программно-аппаратный.
SecretNet 7	Средство защиты информации. Клиент (автономный)
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда

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. 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) «Программно-аппаратные средства 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	Тема 1.1 Проблемы обеспечения безопасности информационных систем.	*ПК 1, ПК 3*	Входной тест. Вопросы к экзамену

2	Тема 1.2 Основные понятия информационной безопасности.	*ПК 1, ПК 3*	Лабораторно-практическая работа 1, контрольная работа 1. Вопросы к экзамену
3	Тема 2.1 Общие положения по обеспечению защиты программ и данных	*ПК 1, ПК 3*	Лабораторно-практическая работа 2. Вопросы к экзамену
4	Тема 2.2 Принципы защиты программ и данных	*ПК 1, ПК 3*	контрольная работа 2. Вопросы к экзамену
5	Тема 3.1 Системы защиты от несанкционированного копирования программ	*ПК 1, ПК 3*	Лабораторно-практическая работа 3. Вопросы к экзамену
6	Тема 3.2 Особенности построения и программирования внешних запоминающих устройств	*ПК 1, ПК 3*	контрольная работа 3. Вопросы к экзамену
7	Тема 4.1 Защита от разрушающих программных средств (РПС)	*ПК 1, ПК 3*	Лабораторно-практическая работа 4. Вопросы к экзамену
8	Тема 4.2 Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий.	*ПК 1, ПК 3*	контрольная работа 4. Вопросы к экзамену
9	Тема 5.1 Классификация типовых программно-аппаратных средств защиты информации, обрабатываемой в ПЭВМ	*ПК 1, ПК 3*	Лабораторно-практическая работа 5. Вопросы к экзамену
10	Тема 5.2 Программно-аппаратные средства безопасности ИС.	*ПК 1, ПК 3*	Лабораторная работа 5, контрольная работа 5. Вопросы к экзамену
11	Тема 5.3 Система защиты информации ViPNet.	*ПК 1, ПК 3*	контрольная работа 5. Вопросы к экзамену
12	Тема 6.1 Сертификация программно-аппаратных средств на соответствие требованиям информационной безопасности.	*ПК 1, ПК 3*	Лабораторно-практическая работа 6. Вопросы к экзамену
13	Тема 6.2 Оценка эффективности программно-аппаратных средств.	*ПК 1, ПК 3*	контрольная работа 6. Вопросы к экзамену
14	Тема 6.3 Экономические вопросы	*ПК 1, ПК 3*	Итоговый тест.

	выбора состава программно-аппаратных средств.		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
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)

Тема 1.1 Проблемы обеспечения безопасности информационных систем.

Вопросы к входному тестированию.

Вопрос 1

Сеть на уровне компании, в которой используются программные средства, основанные на стеке протоколов TCP/IP – это

- Интранет
- Экстранет
- Интернет

Вопрос 2

Под _____ взаимодействием понимается взаимодействие двух локальных сетей, при котором они функционируют как самостоятельные единицы объединенной сети.

Вопрос 3

Потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам информационной системы:

Угроза
Опасность
Риск

Вопрос 4

Вставьте пропущенные слова. _____ _____ – это программа , которая позволяет злоумышленнику обходить нормальный контроль безопасности входа и дает ему доступ к компьютеру – жертве.

Вопрос 5

По используемым уязвимостям атаки можно разбить на классы:
Семантические атаки
Атаки грубой силы
Атаки с постоянной скоростью
Синтаксические атаки
Атаки, исходящие из одного из одного источника

Вопрос 6

Действия по проверке подлинности субъекта доступа в информационной системе
Аутентификация
Идентификация
Аудиторская проверка
Аутентичность

Вопрос 7

Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта

Доступность
Достоверность
Целостность
Верифицируемость

Тема 1.2 Основные понятия информационной безопасности.

Лабораторно-практическая работа 1. Средства защиты от несанкционированного доступа. Установка и настройка ПАК "Соболь".

Цель работы: знакомство со средствами защиты от несанкционированного доступа.
Задача №1: Изучить теоретический материал по работе с программно-аппаратным средством защиты компьютера от несанкционированного доступа: Электронный замок "Соболь" (ПАК "Соболь").
Задача №2: Провести установку и первичную настройку ПАК "Соболь".

Вопросы к контрольной работе № 1
Основы программно-аппаратных средств информационной безопасности

1. Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств.
2. Функциональные требования по защите вычислительных систем.
3. Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД.
4. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения безопасности.
5. Зоны безопасности. Зоны безопасности вычислительной среды.
6. Объекты и элементы защиты.
7. Уровни обеспечения безопасности.
8. Концепция диспетчера и иерархия режимов обеспечения безопасности программными и аппаратными средствами.
9. Сочетание различных методов обеспечения безопасности.
10. Взаимодействие программно-аппаратных средств с общесистемными средствами.

Тема 2.1 Общие положения по обеспечению защиты программ и данных

Лабораторно-практическая работа 2. Управление доступом и защита ресурсов в системе Secret Net 7.

Цель работы: изучение принципов защиты ресурсов с помощью управления доступом и приобретение навыков администрирования системы защиты информации Secret Net 7.
Задача №1: Изучить теоретический материал по работе с системой защиты компьютера от несанкционированного доступа: Secret Net 7.
Задача №2: Управление доступом и защита ресурсов в системе Secret Net 7.

Тема 2.2 Принципы защиты программ и данных

Вопросы к контрольной работе № 2
Меры непосредственной защиты вычислительных средств

1. Классификация непосредственных угроз вычислительным устройствам.
2. Защита от стихийных бедствий.
3. Противопожарная защита, защита от затоплений, внезапных изменений электропитания.
4. Защита от непосредственных злоумышленных воздействий: механических и других контактных воздействий, от помех и наводок, меры сигнализации.
5. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
6. Методы идентификации и аутентификации пользователей.
7. Идентификация по системе паролей, по стандартному ключу и специальным

характеристикам пользователей.

8. Использование методов дублирования и резервирования элементов и устройств для повышения уровня информационной безопасности.

9. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.

10. Доступ к данным со стороны процесса; способы фиксации факта доступа; надежность систем ограничения доступа.

Тема 3.1 Системы защиты от несанкционированного копирования программ

Лабораторно-практическая работа 3. Система контроля целостности (Secret Net 7).

Цель работы: изучение принципов работы и получение практических навыков по работе с системой контроля целостности.

Задача №1: Изучить теоретический материал по работе с системой контроля целостности: Secret Net 7.

Задача №2: получить практические навыки по работе с системой контроля целостности (Secret Net 7).

Тема 3.2 Особенности построения и программирования внешних запоминающих устройств

Вопросы к контрольной работе № 3
Защита программ от изменений и контроль целостности

1. Основные объекты защиты аппаратных средств.
2. Проблема выбора оптимального соотношения между затратами и уровнем защиты.
3. Защита реальной и виртуальной памяти аппаратными средствами: использование регистров границ, ключей и замков, битов управления доступом к памяти, таблиц соответствие адресов.
4. Контроль состояния выполнение программ.
5. Защита файлов от изменения.
6. Защита программ от несанкционированного копирования; пароли и ключи, организация хранения ключей; защита программ от излучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям;
7. Применение микропроцессоров для контроля и защиты между различными компонентами вычислительной аппаратуры.
8. Аппаратная реализация функций операционной системы.
9. Средства защиты устройств ввода-вывода.
10. Методы и средства хранения ключевой информации.

Тема 4.1 Защита от разрушающих программных средств (РПС)

Лабораторно-практическая работа 4. Знакомство с аппаратными межсетевыми экранами. Cisco ASA. Обзор и первоначальная настройка.

Цель работы: изучение принципов работы и получение практических навыков по работе с аппаратным межсетевым экраном Cisco ASA.

Задача №1: Изучить теоретический материал по работе с Cisco ASA.

Задача №2: Произвести настройку сетевых интерфейсов и правил фильтрации.

Тема 4.2 Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий.

Вопросы к контрольной работе № 4
Контроль доступа

1. Классификация компьютерных вирусов и «троянских» программ. Антивирусные программы, их функции и возможности.
2. Средства нарушения безопасности компьютерных сетей.
3. Принципы функционирования РПС.
4. Модель взаимодействия объектов в вычислительной системе с точки зрения безопасности.
5. Защита от разрушающих программных воздействий (РПВ); компьютерные вирусы как особый класс РПВ; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.
6. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
7. Методы и средства ограничения доступа.
8. Реализация надзора: ведение протокола, управление доступом, контроль обращения к системе.
9. Технология изоляции пользователя от компьютера и построение изолированной программной среды.
10. Встраивание средств защиты в программное обеспечение. Изоляция области нарушения защиты.
11. Защита от разрушающих программных воздействий.
12. Технология резервного копирования программного обеспечения: частота и полнота копирования, хранение и тестирование резервных копий. Методы и средства ограничения доступа к компонентам ЭВМ.

Тема 5.1 Классификация типовых программно-аппаратных средств защиты информации, обрабатываемой в ПЭВМ

Лабораторно-практическая работа 5. *(тема 5.1 и 5.2)* **Сетевые системы обнаружения вторжений (IDS).**

Цель работы: изучение принципов работы и получение практических навыков по работе со свободной сетевой системой предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом - Snort.
Задача №1: Изучить теоретический материал по работе со Snort.
Задача №2: Произвести установку и первичную настройку системы Snort.

Тема 5.2 Программно-аппаратные средства безопасности ИС.

Вопросы к контрольной работе № 5 *(первый блок)*
Программно - аппаратные средства защиты в интерактивной среде

1. Особенности программно - аппаратного обеспечения безопасности в интерактивной среде.
2. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта.
3. Защита информационной среды от нежелательных информационных материалов, средства фильтрации сетевой информации.
4. Средства и методы уменьшения риска сделок и переговоров в интерактивной

среде. Защита интерактивной среды.

5. Управление вычислительным процессом в интерактивной среде, сценарии поведения.

6. Программно - аппаратные средства защиты интерактивных функций серверов.

Тема 5.3 Система защиты информации ViPNet.

Вопросы к контрольной работе № 5 (второй блок)

Программно - аппаратные средства защиты в интерактивной среде

1. Технология системы защиты информации ViPNet. ViPNet [Администратор].
2. Криптографические системы и их использование в ViPNet.
3. PKI в структуре системы защиты информации. Межсетевое взаимодействие.
4. Компоненты VPN. ViPNet [Клиент].
5. Логика обработки IP-трафика. Деловая почта. ViPNet [Координатор].
6. Электронная цифровая подпись (ЭП).
7. Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных; защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты.

Тема 6.1 Сертификация программно-аппаратных средств на соответствие требованиям информационной безопасности.

Лабораторно-практическая работа 6. Средства анализа защищенности информационных систем.

Цель работы: изучение принципов работы и получение практических навыков по работе с системой контроля защищённости и соответствия стандартам - Maxpatrol.
Задача №1: Изучить теоретический материал по работе с системой Maxpatrol.
Задача №2: Произвести установку и сканирование информационного ресурса с помощью системы Maxpatrol.

Тема 6.2 Оценка эффективности программно-аппаратных средств.

Вопросы к контрольной работе № 6

Прикладные вопросы использования программно - аппаратных средств.

1. Общие положения сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
2. Система сертификации.
3. Порядок сертификации.
4. Показатели эффективности программно-аппаратных средств.
5. Модели и методы оценки эффективности.
6. Достоверность оценки экономической эффективности предприятий за счет автоматизации управленческих и производственных процессов.
7. Классификация информации по её ценности, анализ угроз, оценка риска и затрат на обеспечение информационной безопасности.

Тема 6.3 Экономические вопросы выбора состава программно-аппаратных средств.

Вопросы к итоговому тестированию.

Вопрос 1.

Какая из перечисленных ниже аббревиатур означает динамическую трансляцию IP-адресов, которая ставит в соответствие множеству адресов локальной сети единственный IP-адрес, используя различные номера портов?

А) UDP;

Б) RFC;

В) PAT;

Г) IPX.

Вопрос 2.

Технология NAT позволяет (необходимо выбрать несколько правильных вариантов):

А) Обрабатывать информацию внутри пакетов.

Б) Спрятать топологию доверенной сети.

В) При обнаружении подозрительных на атаку признаков, адаптивно изменять конфигурацию МЭ.

Г) Использовать внутри организации пул IP-адресов меньшего размера.

Д) Все ответы верные.

Вопрос 3.

Туннелирование – это:

А) посылка и анализ IP-пакетов для определения возможности определенного пакета пройти на хост назначения через устройство фильтрации пакетов.

Б) кодирование данных приложения для передачи по сети.

В) технология передачи протокола через общую сеть с использование другого протокола.

Г) технология представления данных в сетях с неоднородными устройствами и программным обеспечением.

Вопрос 4.

Межсетевой экран прикладного уровня характеризуется следующими признаками (необходимо выбрать несколько правильных вариантов):

А) Возможность оперировать данными внутри пакета.

Б) Использование службы Proxy.

В) Быстрота работы по сравнению с другими МЭ.

Г) Практически не имеет аудита

Д) Все ответы верные.

Вопрос 5.

Криптография с открытыми ключами характеризуется (возможны несколько вариантов ответов):

А) Относительно высокой производительностью алгоритмов.

Б) Только одной стороне известен ключ шифрования, который нужно держать в секрете.

В) Необходимостью использования сложного механизма распределения ключей.

Г) Не нужно предварительно передавать секретный ключ по надёжному каналу.

Д) Технологическими трудностями обеспечения неотказуемости.

Вопрос 6.

Криптография с симметричными ключами характеризуется (возможны несколько вариантов ответов):

А) Относительно высокой производительностью алгоритмов.

Б) Только одной стороне известен ключ шифрования, который нужно держать в секрете.

В) Необходимостью использования сложного механизма распределения ключей.

Г) Не нужно предварительно передавать секретный ключ по надёжному каналу.

Д) Технологическими трудностями обеспечения неотказуемости.

Вопрос 7.

Какие из указанных ниже типов подписей (согласно ФЗ-63 «Об электронной подписи») формируются и проверяются с помощью криптографического средства электронной подписи и ключа электронной подписи? (возможны несколько вариантов ответов)

А) Простая электронная подпись.

Б) Неквалифицированная электронная подпись.

В) Квалифицированная электронная подпись.

Г) Все указанные варианты верны.

Вопрос 8.

Что из указанного ниже входит в состав сертификата открытых ключей? (возможны несколько вариантов ответов)

А) Информация об издателе сертификата.

Б) Информация о владельце сертификата.

В) Период действия ключа.

Г) Информация об отзыве ключа.

Д) Все перечисленные варианты входят в состав сертификата открытых ключей.

Вопрос 9.

В криптографии с симметричными ключами для шифрования используется:

А) Открытый ключ.

Б) Секретный ключ.

В) Данный класс криптографии не используется для шифрования из-за технологических трудностей.

Вопрос 10.

Для чего используется штамп времени?

А) Показывает время выдачи сертификата ключа электронной подписи.

Б) Отображает время отзыва сертификата ключа электронной подписи.

В) Удостоверяет время создание документа для последующего разрешения конфликтов.

Г) Показывает срок действия сертификата ключа электронной подписи.

Примерная тематика курсовых проектов

1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.

2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.

3. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.

4. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.

5. Инструментальные средства анализа рисков информационной безопасности.

Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей.

6. Использование ЭП для обеспечения защиты информации при использовании системы электронного документооборота.

7. Интеграция защищенных операционных систем в защищенную сеть.

8. Биометрическая аутентификация пользователя.

9. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

10. VPN-решения для построения защищенных сетей.

11. Безопасность баз данных.

12. Технический контроль эффективности мер защиты информации.

13. Идентификация и установление личности.

14. Аудит в операционных системах.

15. Реализация подсистем безопасности.

Перечень вопросов к экзамену

1. Идентификация субъекта, протоколы идентификации, идентифицирующая информация.

2. Основные подходы к защите данных от НСД.

3. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.

4. Доступ к данным со стороны процесса.

5. Способы фиксации факта доступа.

6. Надежность систем ограничения доступа.

7. Электронная цифровая подпись (ЭП).

8. Программно-аппаратные средства шифрования

9. Построение аппаратных компонент криптозащиты данных.

10. Защита алгоритма шифрования.

11. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты.

12. Методы и средства ограничения доступа к компонентам ЭВМ

13. Защиты программ от несанкционированного копирования

14. Пароли и ключи, организация хранения ключей.

15. Защита программ от излучения.

16. Защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям.

17. Защита от разрушающих программных воздействий (РПВ).

18. Компьютерные вирусы как особый класс РПВ.

19. Необходимые и достаточные условия недопущения разрушающего воздействия.

20. Понятие изолированной программной среды.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-1. Способен проводить научные исследования при разработке, внедрении и сопровождении информационных технологий и систем на всех этапах жизненного цикла				
1.	Задание закрытого типа	Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой априорной информации: а) идентификация.	а	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		б) аутентификация в) процедура г) доступ		
2.		Проверка идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа); а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации а) идентификация. б) аутентификация в) процедура г) доступ	б	2
3.		Искусственные угрозы исходя из их мотивов разделяются на: а) непреднамеренные и преднамеренные б) косвенные и непосредственные в) несанкционированные и санкционированные	а	2
4.		К непреднамеренным угрозам относятся: а) ошибки в разработке программных средств КС б) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями. в) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой	а	2
5.		К умышленным угрозам относятся: а) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС); б) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.	а	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		в) ошибки пользователей КС		
6.	Задание открытого типа	Что является основой избирательной политики безопасности?	Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что: все субъекты и объекты системы должны быть идентифицированы; права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).	2
7.		Что представляет собой матрица доступа?	Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту - столбец. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как "доступ на чтение", "доступ на запись", "доступ на исполнение" и др.	2
8.		Что является основой полномочной политики безопасности?	Основу полномочной политики безопасности составляет полномочное управление доступом, которое подразумевает что: все субъекты и объекты системы должны быть однозначно идентифицированы; каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации; каждому субъекту системы присвоен уровень прозрачности,	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.	
9.		Описать процедуру "рукопожатия"	Для взаимной проверки подлинности обычно используют процедуру "рукопожатия". Эта процедура базируется на указанных выше механизмах контроля и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру рукопожатия обычно применяют в компьютерных сетях при организации сеанса связи между пользователями, пользователем и хост - компьютером, между хост - компьютерами	2
10.		Правило разграничения доступа	Правило разграничения доступа заключается в следующем: лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.	2
ПК-3. Способность выполнять работы по созданию (модификации) и сопровождению информационных систем и обеспечению их информационной безопасности				

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
1.	Задание закрытого типа	Существуют три причины использования распределенных атак злоумышленником. Какая из перечисленных лишняя: а. сокрытие. б. мощность. в. сбор информации. г. отсутствие последствий после вторжения	г	2
2.		Укажете два основных метода анализа, связанных с выявлением атак в системах обнаружения вторжений. а. сигнатурный метод и метод, связанный с выявлением аномального поведения. б. сигнальный метод и метод, связанный с выявлением аномального поведения. в. сигнатурный и сигнальный методы. г. структурный и сигнальный методы.	а	2
3.		Если пользователи создают свои собственные пароли, каких рекомендаций они должны придерживаться (выберите все возможные варианты)? а. использовать максимально возможное количество символов в пароле; б. использовать в качестве пароля имя супруга/супруги, ребенка или кличку собаки (чтобы не забыть пароль); в. использовать хотя бы одну прописную букву, один символ нижнего регистра, одну цифру и один допустимый не алфавитно-цифровой символ; г. использовать пароль, который трудно угадать по смыслу.	в, г	2
4.		Уязвимость информации — это: а. Возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. б. Событие или действие, которое	б	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. в. Это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.		
5.		Под угрозой безопасности информации в компьютерной системе (КС) понимают: а) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. б) Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. с) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости	с	2
6.	Задание открытого типа	Основные задачи при эксплуатации механизмов аутентификации	При эксплуатации механизмов аутентификации основными задачами являются: генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.	2
7.		Что понимается под системой защиты от несанкционированного использования и копирования	Под системой защиты от несанкционированного использования и копирования понимается комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			информационных ресурсов.	
8.		Что должен выполнить для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы?	Для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы должен выполнить следующие функции: − анализ аппаратно-программной среды компьютера, на котором должна будет выполняться инсталлируемая программа, и формирование на основе этого анализа эталонных характеристик среды выполнения программы; − запись криптографически преобразованных эталонных характеристик аппаратно-программной среды компьютер на винчестер.	2
9.		Основные компоненты системы защиты программных продуктов от несанкционированного копирования	Основные компоненты системы защиты программных продуктов от несанкционированного копирования: модуль проверки ключевой информации (некопируемой метки на дистрибутивном диске, уникального набора характеристик компьютера, идентифицирующей информации для легального пользователя) – может быть добавлен к исполнимому коду защищаемой программы по технологии компьютерного вируса, в	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			виде отдельного программного модуля или в виде отдельной функции проверки внутри защищаемой программы; модуль защиты от изучения алгоритма работы системы защиты; модуль согласования с работой функций защищаемой программы в случае ее санкционированного использования; модуль ответной реакции в случае попытки несанкционированного использования (как правило, включение такого модуля в состав системы защиты нецелесообразно по морально-этическим соображениям).	
10.		Основные требования, предъявляемые к системе защиты от копирования	Основные требования, предъявляемые к системе защиты от копирования: обеспечение некопируемости дистрибутивных дисков стандартными средствами (для такого копирования нарушителю по требуется тщательное изучение структуры диска с помощью специализированных программных или программно-аппаратных средств); обеспечение невозможности применения стандартных отладчиков без дополнительных действий над машинным кодом программы или без применения специализированных программно-аппаратных средств (нарушитель должен быть	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			специалистом высокой квалификации); обеспечение некорректного дисассемблирования машинного кода программы стандартными средствами (нарушителю потребуется использование или разработка специализированных дисассемблеров); обеспечение сложности изучения алгоритма распознавания индивидуальных параметров компьютера, на котором установлен программный продукт, и его пользователя или анализа применяемых аппаратных средств защиты (нарушителю будет сложно эмулировать легальную среду запуска защищаемой программы).	

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)

Отчет по лабораторно-практической работе

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

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

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

Отчет не может быть принят и подлежит доработке в случае:

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

В отчете по выполненной практической работе должны быть указаны:

- тема практической работы,

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

Критерии оценки по лабораторно-практическим работам:

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

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

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

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

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

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

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Критерии оценки контрольных работ:

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

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

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

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

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

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.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине на экзамен во втором семестре отводится 100 баллов (40 баллов на текущие формы контроля, 10 баллов на бонусы и 50 баллов отводится на экзамен),

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.

Критерии оценок на экзамене:

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

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

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

20-22 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала. 1

1-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки. 1

0 баллов – ответ студента правилен лишь частично, при разъяснении материала до-

пускаются серьезные ошибки.

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

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

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

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	6/3	18	По расписанию
2.	*Выполнение контрольной работы*	6/3	18	
3.	*Тест*	2/2	4	
Всего			**40**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*	1	3	
5.	*Своевременное выполнение всех заданий*	1	3	
6.	*Активность студента на занятии*	1	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)	
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 «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

8.1. Основная литература

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М. : Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html

8.2. Дополнительная литература

1. Проскурин В.Г., Защита в операционных системах [Электронный ресурс] : Учебное пособие для вузов / Проскурин В.Г. - М. : Горячая линия - Телеком, 2014. - 192 с. - ISBN 978-5-9912-0379-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203791.html

2. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М. : Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204811.html

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 «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

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

Материально-техническое обеспечение дисциплины включает в себя учебные лаборатории и классы, оснащенные современными компьютерами, объединенными локальными вычислительными сетями с выходом в Интернет. Учащимся предоставляется возможность практической работы на ЭВМ различной архитектуры (на базе одноядерных, многоядерных, параллельных процессоров).

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).