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
«23» мая 2023 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ
_____ Р.Ю. Демина
от «23» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информационных процессов в компьютерных системах

Составитель(-и)	**Выборнова О.Н., доцент кафедры информационной безопасности; Шукралиева Д.Э., старший преподаватель кафедры информационной безопасности**
Направление подготовки	**10.03.01 Информационная безопасность**
Направленность (профиль) ОПОП	**«Организация и технологии защиты информации»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2021**
Курс	**3**
Семестр	**6**

Астрахань, 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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

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

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Защита информационных процессов в компьютерных системах» относится к части, формируемая участниками образовательных отношений и осваивается в 6-м семестре.

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

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

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

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

Навыки: поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.), выявления и уничтожения компьютерных вирусов; владения методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации.

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

Дисциплина «Защита информационных процессов в компьютерных системах» поможет студентам при написании бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

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

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации	ИПК 2.1. Знать: технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности информации	ИПК 2.2. Уметь: проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.	ИПК 2.3. Владеть: методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем	ИПК-3.1. Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации основные меры по защите информации в автоматизированных системах, нормативные правовые акты в области защиты информации	ИПК-3.2. Уметь: администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы,	ИПК-3.3. Владеть: методикой анализа структурных и функциональных схем защищенной автоматизированной системы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) в зачетных единицах **3 зачетные единицы**. Всего 108 часов: 68 часов выделено на контактную работу обучающихся с преподавателем (лекции –17 часов, лабораторные работы – 51), 40 часов – на самостоятельную работу обучающихся:

Таблица 2 – Структура и содержание дисциплины (модуля)

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.Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность.	6	2		6		4	Лабораторная работа, устный опрос
2.Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.		2		6		4	Лабораторная работа, устный опрос
3.Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.		2		6		4	Лабораторная работа, устный опрос
4.Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Основные протоколы, службы, функционирование, средства обеспечения		2		6		4	Лабораторная работа, устный опрос

безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.							
5.Политика безопасности. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.		2		6		4	Лабораторная работа, устный опрос
6. Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети.		2		6		4	Лабораторная работа, устный опрос
7. Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.		1		6		4	Лабораторная работа, устный опрос
8. Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов.		2		6		4	Лабораторная работа. устный опрос
9.Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет.		2		3		8	Контрольная работа, устный опрос
ИТОГО		**17**		**51**		**40**	**экзамен**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная

работа; КР – курсовая работа; СР – самостоятельная работа.

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

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции*		*Общее количество компетенций*
		ПК 2	ПК 3	
1.Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность.	12	+	+	2
2.Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.	12	+	+	2
3.Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	12	+	+	2
4.Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.	12	+	+	2
5.Политика безопасности. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.	12	+	+	2
6.Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети.	12	+	+	2
7.Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	11	+	+	2
8.Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов.	12	+	+	2
9.Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные	13	+	+	2

сети. Контроль и анализ обеспечения безопасности подключения к Интернет.				
Итого	108			

Краткое содержание дисциплины

Тема 1

Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность.

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

Типы компьютерных систем, как элементов информационных технологий. Основные принципы успешного функционирования информационной (компьютерной) системы. Основные принципы и методы защиты информационных процессов в компьютерных системах.

Основные подходы, используемые при проектировании защищенных информационных технологий. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении. Стандарт ITIL.

Тема 2

Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.

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

Тема 3

Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.

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

Тема 4

Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.

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

Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности. Содержание политики безопасности. Подход к безопасности компьютерных систем в CC и базовые концепции.

Тема 5

Политика безопасности. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.

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

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

Тема 6

Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети.

Каналы утечки и их анализ в системе общих критериев.

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

Безопасное функционирование в системе общих критериев

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

Изучение способов и методов защиты информации в операционной системе Unix.

Тема 7

Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.

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

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

Тема 8

Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов.

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

Государственная политика в области безопасности компьютерных систем

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

Тема 9

Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет.

Разработка политик безопасности для защищенных компьютерных систем.

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

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

Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

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

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

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

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

Таблица 4 – Содержание самостоятельной работы обучающихся

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

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

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

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

6.1. Образовательные технологии

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

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
1.Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
2.Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
3.Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
4.Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
5.Политика безопасности. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы

шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.			
6.Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
7.Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
8.Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
9.Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет.	Лекция - презентация	Не предусмотрено	выполнение контрольной работы

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

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

6.2. Информационные технологии

– 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 Электронное образование) или иных информационных систем, сервисов и мессенджеров

Название информационной технологии	Темы, разделы дисциплины	Краткое описание применяемой технологии
Использование возможностей Интернета в учебном процессе	1-9	Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения)
Работа с электронными ресурсами	1-9	• Web-сервер Федеральной службы по техническому и экспортному контролю (ФСТЭК России) (правоприемник Государственной технической комиссии при Президенте Российской Федерации) http://www.fstec.ru/ • Два портала по информационной безопасности: http://infosecurity.report.ru/ http://www.void.ru/ • Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности http://www.jetinfo.ru
Использование возможностей электронной почты преподавателя	1-9	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1-9	Использование мультимедийной презентации

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

6.3.1. Программное обеспечение

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

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Chrome	Браузер
Microsoft Office	Офисная программа
7-zip	Архиватор
Microsoft Windows	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
NetWare Administrator	Программа для выполнения лабораторных работ

6.3.2. Современные профессиональные базы данных и информационные справочные системы

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

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО

«Информ-систем»: https://library.asu.edu.ru.

2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.

3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/

4. Электронно-библиотечная система elibrary. http://elibrary.ru

5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

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

7.1. Паспорт фонда оценочных средств

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

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

Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1.Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность.	ПК 2, ПК 3	Лабораторная работа
2.Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.	ПК 2, ПК 3	Лабораторная работа
3.Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	ПК 2, ПК 3	Лабораторная работа
4.Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.	ПК 2, ПК 3	Лабораторная работа
5.Политика безопасности. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению	ПК 2, ПК 3	Лабораторная работа

политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности.		
6.Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети.	ПК 2, ПК 3	Лабораторная работа
7.Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	ПК 2, ПК 3	Лабораторная работа
8.Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов.	ПК 2, ПК 3	Лабораторная работа
9.Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет.	ПК 2, ПК 3	Контрольная работа. 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

Шкала оценивания	Критерии оценивания
	выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания

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

Тема «Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность»

Вопросы для обсуждения:

Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак, информационных технологий и информационных систем. Рекомендации по построению системы защиты. Типы компьютерных систем, как элементов информационных технологий. Основные принципы успешного функционирования информационной (компьютерной) системы. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений. Основные принципы и методы защиты информационных процессов в компьютерных системах. Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении. CASE-технологии создания информационных систем. Стандарт ITIL.

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

Тема «Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами»

Вопросы для обсуждения:

Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Критерии определения безопасности компьютерных систем (Оранжевая книга). Понятие гарантии защиты. Критерии оценки защищенности баз данных. Содержание классов защищенности. Требования по защите информации, предъявляемые в каждом классе защищенности. Стандарт COBIT. ITIL и ITSM. ISO/IEC 27XXX. ISO/IEC 15408. Серия NIST SP 800.

Тема «Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях»

Вопросы для обсуждения:

Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Европейский стандарт по защите информации ITSEC. Понятие гарантии защиты в соответствии с европейским стандартом. Критерии

оценки защищенности. Содержание классов защищенности. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения защищенных информационных систем. Изучение способов и методов защиты информации в сетях Novell NetWare.

1. **Лабораторная работа 1.** Защита информационных процессов в операционной системе Nowell Netware. Установка программного комплекса.

Тема «Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений»

Вопросы для обсуждения

Сетевые операционные системы (ОС) NetWare, Windows, UNIX. Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности. Содержание политики безопасности.

Тема «Политика безопасности. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности»

Вопросы для обсуждения:

Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Классы защищенности. Понятие аудита политики безопасности. Требования к подсистемам аудита. Подсистемы подтверждения подлинности отправки и получения сообщения. Подсистемы разграничения доступа. Подсистемы идентификации и аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы. Подсистемы защиты связи. Требования к подсистемам, предъявляемые в каждом классе защищенности. Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

Лабораторная работа 2. Защита информационных процессов в операционной системе Nowell Netware. Выполнение практических заданий.

Тема «Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети»

Вопросы для обсуждения:

Каналы утечки и их анализ в системе общих критериев. Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации. Безопасное функционирование в системе общих критериев

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

Изучение способов и методов защиты информации в операционной системе Unix.

Тема «Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.»

Вопросы для обсуждения:

Основные угрозы информации в компьютерных системах. Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. Специфика возникновения угроз в открытых сетях. Особенности защиты информации на узлах компьютерной сети. Анализ рисков. Модель противника, возможности противника. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

Лабораторная работа 3. Защита информационных процессов в операционной системе Unix.

Тема «Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет»

Вопросы для обсуждения:

Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации. Государственная политика в области безопасности компьютерных систем

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

Тема «Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов»

Вопросы для обсуждения:

Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности. Политика мандатного доступа. Политика защиты целостности информационных ресурсов. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Лабораторная работа 4 (по вариантам). Создание рефератов по курсу «Защита информационных процессов в компьютерных системах».

Варианты:

1. Классификация сетевых атак.
2. Типовые и специфические сетевые атаки.
3. Примеры реализации атак на «отказ в обслуживании» и способы противодействия им.
4. Анализ защищенности стандартных сетевых протоколов. Примеры атак с их использованием.
5. Подходы к решению задачи распределения ключей в сети. Анализ защищенности криптографических сетевых протоколов.
6. Анализ и сравнение защитных свойств известных сетевых ОС.
7. Решение задачи выбора сетевой ОС.
8. Модели применения межсетевых экранов.
9. Примеры построения политики безопасности.
10. Оценка безопасности сетевой автоматизированной системы.

Примерный план проведения лабораторно-практического занятия

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

7. Руководителями каждой группы излагаются позиции по совершенствованию рекомендуемых мероприятий защиты информации

8. Подводятся итоги занятия с объявлением окончательных оценок участников занятия.

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

Перечень вопросов к экзамену

1. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак..
2. Информационные технологии и их поддержка. Проектирование и разработка защищенных информационных технологий.
3. Основные принципы успешного функционирования информационной (компьютерной) системы. Основные принципы и методы защиты информационных процессов в компьютерных системах.
4. Основные подходы, используемые при проектировании защищенных информационных технологий. Стандарт ITIL.
5. Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД.
6. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа.
7. Электронная цифровая подпись и пакетное шифрование.
8. Криптографические сетевые протоколы. Управление ключами.
9. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
10. Содержание классов защищенности. Требования по защите информации, предъявляемые в каждом классе защищенности.
11. Регламентирующие документы в области безопасности вычислительных сетей. Правовые основы защиты информации в сетях.
12. Стандарты безопасности вычислительных сетей и их компонентов. Вопросы гарантий и эффективности в европейском стандарте ITSEC.
13. Изучение способов и методов защиты информации в сетях Novell NetWare.
14. Сетевые операционные системы (ОС) NetWare, Windows, UNIX.
15. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.
16. Понятие профиля защиты. Функции поддержки политики безопасности.
17. Требования по безопасности информационных технологий. Компоненты подсистем поддержки политики безопасности.
18. Содержание политики безопасности. Подход к безопасности компьютерных систем в CC и базовые концепции.
19. Политика безопасности. Типовые элементы политики безопасности.
20. Рекомендации по построению политики безопасности. Поддержание и модификация политики безопасности.
21. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.
22. Понятие аудита политики безопасности. Требования к подсистемам аудита.
23. Понятие гарантии безопасности. Уровни гарантий.
24. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
25. Защита каналов связи в Интернет. Виды используемых в Интернет-каналов связи.
26. Использование межсетевых экранов. Виртуальные частные сети.
27. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев

28. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.
29. Изучение способов и методов защиты информации в операционной системе Unix.
30. Уязвимости и защита базовых протоколов и служб.
31. Протоколы маршрутизации. Семейство TCP/IP.
32. Службы поиска. Безопасность WWW и электронной почты.
33. Технология построения защищенных компьютерных систем.
34. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.
35. Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в открытых сетях.
36. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных. Анализ рисков.
37. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.
38. Модель угроз. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации.
39. Защита рабочего места пользователя сети Интернет. Защита программного окружения рабочей станции.
40. Защита персональных данных. Защита от вирусов.
41. Государственная политика в области безопасности компьютерных систем.
42. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
43. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа.
44. Комплексная защита подключения к Интернет. Безопасность различных типов подключения к Интернет.
45. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет.
46. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.
47. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.
48. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации.
49. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
50. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

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

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

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

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

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

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		4. Кибервойна		
2.		Диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна	4	2
3.		Монитор обращений (по стандарту «Критерии оценки надежности компьютерных систем») должен обладать следующими качествами: 1. Изолированность 2. Полнота 3. Верифицируемость 4. Надежность 5. Безопасность 6. Подлинность	1, 2, 3	2
4.		Назовите средства радиоэлектронной борьбы 1. аппаратные средства 2. средства подавления связи 3. оперативные технические средства 4. средства борьбы с системами управления противника 5. программные средства 6. экономические средства	1, 2, 3	2
5.		В «Оранжевой книге» рассматривается несколько видов гарантированности 1. операционная 2. технологическая 3. информационная 4. техническая 5. безопасная 6. подлинная	1, 2	2
6.	Задание открытого типа	Аспекты ИБ в соответствии со стандартом BS 7799	Аспектами ИБ в соответствии со стандартом BS 7799 являются: • Политика безопасности. • Организация защиты. • Классификация и управление	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			информационными ресурсами. • Управление персоналом. • Физическая безопасность. • Администрирование компьютерных систем и сетей. • Управление доступом к системам. • Разработка и сопровождение систем. • Планирование бесперебойной работы организации. • Проверка системы на соответствие требованиям ИБ.	
7.		Какие тома должны входить в комплект документации надежной системы согласно «Оранжевой книге»?	Согласно «Оранжевой книге», в комплект документации надежной системы должны входить следующие тома: • Руководство пользователя по средствам безопасности. • Руководство администратора по средствам безопасности. • Тестовая документация. • Описание архитектуры.	2
8.		Элементы, которые должна обязательно включать в себя политика безопасности согласно «Оранжевой книге»	Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы: • произвольное управление доступом; • безопасность повторного использования объектов; • метки безопасности; • принудительное управление доступом.	2
9.		Согласно «Оранжевой книге» дать определение политики безопасности	Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности,	2

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

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

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

Методические рекомендации по выполнению лабораторных и контрольных

работ, проведению экзамена

Отчет по лабораторной работе

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

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

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

Отчет не может быть принят и подлежит доработке в случае:

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

В отчете по выполненной лабораторной работе должны быть указаны:

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

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

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

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

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

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

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

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

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	4/4	16	По расписанию
2.	*Выполнение контрольной работы*	1/24	24	
Всего			**40**	-
Блок бонусов				
3.	*Посещение занятий без пропусков*	1	3	
4.	*Своевременное выполнение всех заданий*	1	1	
5.	*Активность студента на занятии*	1	6	
Всего			**10**	-
Дополнительный блок				
6.	**Экзамен**		**50**	
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

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

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

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

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

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

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

8.2. Дополнительная литература

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202572.html (ЭБС «Консультант студента»).
2. Интеллектуальные системы защиты информации : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785942756673.html (ЭБС «Консультант студента»).
3. Интеллектуальные интерактивные системы и технологии управления удаленным доступом (Методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intranet): Учебное пособие / Ботуз С.П. - 3-е изд., доп. - М. : СОЛОН-ПРЕСС, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785913591326.html (ЭБС «Консультант студента»).
4. Куприянова, А.И. Основы защиты информации : доп. УМО по образованию в области авиации, ракетостроения и космоса в качестве учеб.пособ. для студ., обуч. по спец. «Радиоэлектронные системы», «Средства радиоэлектронной борьбы» и «Информационные системы и технологии» / А. И. Куприянова, Сахаров, А.В., Шевцов, В.А. - - М. : Академия, 2008. - 256 с. (11 экз.)
5. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: Рек. УМО вузов по университетскому п/тех. образованию в качестве учеб. пособ. для вузов... по специальности «Информатика и вычислительная техника» / П. Б. Хорев,. - М.: Акдемия, 2005. - 256 с. (69 экз.)
6. Садердинов, А.А. Информационная безопасность предприятия: Учеб. пособ. - 2-е изд. - М.: Дашков и К, 2005. - 336 с. (45 экз.)
7. Девянин, П.Н. Модели безопасности компьютерных систем : Доп. УМО объединением вузов по образованию в области информационной безопасности в качестве учеб. пособ. для вузов... по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» / П. Н. Девянин. - М. : Академия, 2005. - 144 с. (50 экз.)
4. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html (ЭБС «Консультант студента»).
8. Галатенко, В.А. Основы информационной безопасности : Курс лекций. Учебное пособие. Рек. для вузов ... по специальностям в области информационных технологий / В. А. Галатенко ; Под ред. В.Б. Бетелина. - Изд. 3-е. - М. : ИНТУИТ. РУ «Интернет-университет Информационных Технологий», 2004 - 264 с. (45 экз.)

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

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

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

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

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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