МИНОБРНАУКИ РОССИИ

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

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	Заведующий кафедрой математики и информатики
_____ С.Н.Бориско	_____ С.Н.Бориско
«31» августа 2023 г.	«31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Защита информации

Составитель(-и)	Литвинов Святослав Петрович, к.т.н., доцент Степанцов Сергей Валерьевич, преподаватель Бориско Сергей Николаевич, к.т.н., доцент, зав. кафедрой
Направление подготовки / специальность	**09.03.02 Информационные системы и технологии**
Направленность (профиль) ОПОП	**Проектирование и сопровождение информационных систем**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2021**
Курс	**3**
Семестр	**5**

Знаменск – 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) являются формирование у обучаемых знаний в области теоретических основ информационной безопасности, навыков практического обеспечения защиты информации от несанкционированного доступа и безопасного использования программных средств в информационных системах.

1.2. Задачи освоения дисциплины (модуля): изучение законодательных и нормативно-методических основ информационной безопасности и защиты информации, систематизация принципов государственной системы защиты информации; получение базовых навыков эксплуатации и реализации механизмов криптографических преобразований; получение навыков реализации мероприятий по обеспечению безопасности информационных систем на основе аудита журналов безопасности; изучение способов анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать средства, схемы и системы защиты информации; иметь представление о типовых моделях разграничения доступа к информации и возможностях их использования в реальных задачах создания и эксплуатации информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) относится к вариативной части (элективные дисциплины) блока 1 подготовки бакалавров. Она логически и содержательно-методически взаимосвязана с дисциплинами базовой части: Информационные технологии, Технологии программирования, Управление данными, Программирование на языке высокого уровня, Представление знаний в информационных системах, Инфокоммуникационные системы и сети, Операционные системы, и вариативной части: цифровая обработка информации, Организация ЭВМ и систем.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями): Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности. Технические средства обеспечения информационной безопасности. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Криптографические методы защиты информации. Защита информационно-программного обеспечения на уровне операционных систем. Защита информации на уровне систем управления базами данных. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях. Современные средства защиты информации от НСД.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем): Информационные технологии, Технологии программирования, Управление данными, Программирование на языке высокого уровня, Представление знаний в информационных системах, Инфокоммуникационые системы и сети, Операционные системы

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

направлению подготовки (специальности):

а) универсальных (УК): УК-1.

Таблица 1 – Декомпозиция результатов обучения

Код компетенции	Планируемые результаты освоения дисциплины (модуля)		
	Знать	Уметь	Владеть
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИУК-1.1 методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа.	ИУК-1.2 применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач.	ИУК-1.3 методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 часов.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)						Самостоят. работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	ГК	ИК	АИ		
1	Общая проблема информационной безопасности информационных систем. Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем. Технические предпосылки кризиса информационной безопасности. Этапы развития защиты информации.	5	1	2	2					4	Фронтальный опрос

	Современная постановка задачи защиты информации. Основные задачи обеспечения защиты информации.										
2	Угрозы и защита информации при реализации информационных процессов. Понятие угрозы. Виды противников или "нарушителей". Окно опасности. Классификация видов угроз информационной безопасности по различным признакам. Угрозы доступности, целостности и конфиденциальности.	5	2	2	2					4	Фронтальный опрос
3	Причины нарушения безопасности вычислительных систем Понятие Таксономии. Таксономия угроз безопасности. Уязвимость защиты. Ошибки в системах защиты. Этапы появления ошибок защиты. Компоненты систем, где чаще всего проявляются ошибки защиты.	5	3	2	2					4	Фронтальный опрос
4	Вредоносное ПО. Компьютерные вирусы и средства защиты от них Понятие компьютерного вируса. Признаки появления вируса. Классификация вирусов. Алгоритмическая особенность построения вируса. Вирусная сигнатура. Антивирусные программы.	5	4	2	2					4	Фронтальный опрос

	Программы «сторожа», ревизоры, доктора, детекторы, вакцины.										
5	Защита информации от несанкционированного доступа Контроль доступа пользователей к ресурсам ИС. Монитор обращений. Структура монитора обращений. Идентификация и аутентификация пользователей ИС. Способы аутентификации.	5	5	2	2					4	Фронтальный опрос
6	Формальные модели безопасности Базовые представления моделей безопасности. Два основных класса моделей политики безопасности– дискреционный и мандатный. Субъекты и объекты доступа. Дискреционная модель Хариссона-Руззо-Ульмана. Мандатная модель Белла-Лападулы.	5	6	2	2					4	Фронтальный опрос
7	Стандарты информационной безопасности. Основы организационно-правового обеспечения информационной безопасности Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Классы защищенности	5	7	2	2					4	Фронтальный опрос

	компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Европейские критерии безопасности информационных технологий. Уровни безопасности системы. Рекомендации X.800. Стандарт ISO 17799 – «Управление информационной безопасностью». Основные функции организационно-правовой базы. Виды информационных ресурсов. Открытая, запатентованная и защищаемая информация. Владельцы защищаемой информации. Понятие государственная тайна. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.										

8	Криптографические методы защиты Криптографические преобразования. Шифрование и дешифрование информации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Шифрование информации с секретным ключом (симметричные алгоритмы). Сравнение симметричных и несимметричных алгоритмов шифрования. Контроль целостности данных. Цифровая подпись. Использование открытых ключей.	5	8	2	2					4	Фронтальный опрос
9	Методология построения защищенных систем Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Теория безопасных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB). Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия	5	9	2	2					4	Фронтальный опрос

	реализации заданной политике безопасности.										
	Итого	**5**		**18**	**18**					**36**	***Экзамен***

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы;

КР – курсовая работа; СР – самостоятельная работа по отдельным темам

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

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции (указываются компетенции перечисленные в п.3)*	*Σ ОБЩЕЕ КОЛИЧЕСТВО КОМПЕТЕНЦИЙ*
		УК-1	
Общая проблема информационной безопасности информационных систем Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем. Технические предпосылки кризиса информационной безопасности. Этапы развития защиты информации. Современная постановка задачи защиты информации. Основные задачи обеспечения защиты информации.	*8*	+	*1*
Угрозы и защита информации при реализации информационных процессов Понятие угрозы. Виды противников или "нарушителей". Окно опасности. Классификация видов угроз информационной безопасности по различным признакам. Угрозы доступности, целостности и конфиденциальности.	*8*	+	*1*
Причины нарушения безопасности вычислительных систем. Понятие Таксономии. Таксономия угроз безопасности. Уязвимость защиты. Ошибки в системах защиты. Этапы появления ошибок защиты. Компоненты систем, где чаще всего проявляются ошибки защиты.	*8*	+	*1*
Вредоносное ПО. Компьютерные вирусы и средства защиты от них Понятие компьютерного вируса. Признаки появления вируса. Классификация вирусов. Алгоритмическая особенность построения вируса. Вирусная сигнатура. Антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины.	*8*	+	*1*

Защита информации от несанкционированного доступа Контроль доступа пользователей к ресурсам ИС. Монитор обращений. Структура монитора обращений. Идентификация и аутентификация пользователей ИС. Способы аутентификации.	*8*	+	*1*
Формальные модели безопасности Базовые представления моделей безопасности. Два основных класса моделей политики безопасности– дискреционный и мандатный. Субъекты и объекты доступа. Дискреционная модель Хариссона-Руззо-Ульмана. Мандатная модель Белла-Лападулы.	*8*	+	*1*
Стандарты информационной безопасности. Основы организационно-правового обеспечения информационной безопасности Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Европейские критерии безопасности информационных технологий. Уровни безопасности системы. Рекомендации X.800. Стандарт ISO 17799 – «Управление информационной безопасностью». Основные функции организационно-правовой базы. Виды информационных ресурсов. Открытая, запатентованная и защищаемая информация. Владельцы защищаемой информации. Понятие государственная тайна. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.	*8*	+	*1*
Криптографические методы защиты Криптографические преобразования. Шифрование и дешифрование информации. Симметричные схемы аутентификации	*8*	+	*1*

субъекта. Несимметричные схемы аутентификации (с открытым ключом). Шифрование информации с секретным ключом (симметричные алгоритмы). Сравнение симметричных и несимметричных алгоритмов шифрования. Контроль целостности данных. Цифровая подпись. Использование открытых ключей.			
Методология построения защищенных систем Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Теория безопасных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB). Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.	*8*	+	*1*

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

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

Основные формы занятий по данной дисциплине являются практические (семинарские) занятия.

Практическое (семинарское) занятие - это особая форма учебно-теоретических занятий, которая, как правило, служит дополнением к лекционному курсу. Его отличительной особенностью является активное участие самих студентов в объяснении вынесенных на рассмотрение проблем, вопросов. Преподаватель дает возможность студентам свободно высказаться по обсуждаемому вопросу и только помогает им правильно построить обсуждение. Студенты заблаговременно знакомятся с планом семинарского занятия и литературой, рекомендуемой для изучения данной темы, чтобы иметь возможность подготовиться к семинару. При подготовке к занятию необходимо: проанализировать его тему, подумать о цели и основных проблемах, вынесенных на обсуждение; внимательно прочитать конспект лекции по этой теме; изучить рекомендованную литературу, делая при этом конспект прочитанного или выписки, которые понадобятся при обсуждении на семинаре; постараться сформулировать свое мнение по каждому вопросу и аргументировано его обосновать. Практическое (семинарское) занятие помогает студентам глубоко овладеть предметом, способствует развитию умения самостоятельно работать с учебной литературой и документами, освоению студентами методов научной работы и приобретению навыков научной аргументации, научного мышления. Преподавателю же работа студентов на семинаре позволяет судить о том, насколько успешно они осваивают материал курса.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Самостоятельная работа студентов является одним из основных видов учебной деятельности и предполагает изучение вопросов, не вошедших в основной план занятий.

Внеаудиторная самостоятельная работа студентов в вузе не менее важна, чем обязательные учебные занятия. Ее успешность во многом определяется тем, насколько умело, рационально сам учащийся сможет организовать свои индивидуальные занятия, насколько регулярными и своевременными они будут.

Задания и методические указания для различных видов самостоятельной работы разрабатываются с учетом её специфики, особенностей изучаемых тем, наличия учебной и методической литературы.

Систематическое освоение студентами необходимого учебного материала, своевременное выполнение предусмотренных учебных заданий, регулярное посещение лекционных и практических занятий позволяют подготовиться к успешному прохождению промежуточной аттестации по данной дисциплине.

В ходе самостоятельной работы студенты должны осуществлять:

-подготовку к занятиям, включая изучение лекций и литературы по теме занятия (используют

-выполнение индивидуальных домашних заданий по теме прошедшего занятия;

-подготовку реферата (индивидуальные задания по слабоусвоенным темам), в том числе сам электронные ресурсы), доклада.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер раздела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	Общая проблема информационной безопасности информационных систем. Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем. Технические предпосылки кризиса информационной безопасности. Этапы развития защиты информации. Современная постановка задачи защиты информации. Основные задачи обеспечения защиты информации.	4	Конспектирование, Подготовка докладов по вопросам семинарского (практического) занятия
2	Угрозы и защита информации при реализации информационных процессов. Понятие угрозы. Виды противников или "нарушителей". Окно опасности. Классификация видов угроз информационной безопасности по различным признакам. Угрозы доступности, целостности и конфиденциальности.	4	Конспектирование, Подготовка реферата
3	Причины нарушения безопасности вычислительных систем Понятие Таксономии. Таксономия угроз безопасности. Уязвимость защиты. Ошибки в системах защиты. Этапы появления ошибок защиты. Компоненты систем, где чаще всего проявляются ошибки защиты.	4	Конспектирование, Подготовка докладов по вопросам семинарского (практического) занятия
4	Вредоносное ПО. Компьютерные вирусы и средства защиты от них. Понятие компьютерного вируса. Признаки появления вируса. Классификация вирусов. Алгоритмическая	4	Конспектирование, Подготовка докладов по вопросам

	особенность построения вируса. Вирусная сигнатура. Антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины.		семинарского (практического) занятия, упражнения
5	Защита информации от несанкционированного доступа Контроль доступа пользователей к ресурсам ИС. Монитор обращений. Структура монитора обращений. Идентификация и аутентификация пользователей ИС. Способы аутентификации.	4	Конспектирование, Подготовка докладов по вопросам семинарского (практического) занятия
6	Формальные модели безопасности. Базовые представления моделей безопасности. Два основных класса моделей политики безопасности– дискреционный и мандатный. Субъекты и объекты доступа. Дискреционная модель Хариссона-Руззо-Ульмана. Мандатная модель Белла-Лападулы.	4	Конспектирование, Подготовка докладов по вопросам семинарского (практического) занятия
7	Стандарты информационной безопасности. Основы организационно-правового обеспечения информационной безопасности Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Европейские критерии безопасности информационных технологий. Уровни безопасности системы. Рекомендации X.800. Стандарт ISO 17799 – «Управление информационной безопасностью». Основные функции организационно-правовой базы. Виды информационных ресурсов. Открытая, запатентованная и защищаемая информация. Владельцы защищаемой информации. Понятие государственная тайна. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.	4	Конспектирование, Подготовка реферата
8	Криптографические методы защиты Криптографические преобразования. Шифрование и дешифрование информации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Шифрование информации с секретным ключом (симметричные алгоритмы).	4	Конспектирование, Подготовка докладов по вопросам семинарского (практического) занятия,

	Сравнение симметричных и несимметричных алгоритмов шифрования. Контроль целостности данных. Цифровая подпись. Использование открытых ключей.		упражнения
9	Методология построения защищенных систем Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Теория безопасных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB). Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.	4	Подготовка реферата, Конспектирование
	Итого	**36**	

Упражнения лежат в основе приобретения тех или иных умений и навыков. В различных условиях обучения упражнение либо единственная процедура, в рамках которой осуществляются все компоненты процесса учения: уяснение содержания действия, его закрепление, обобщение и автоматизация,− либо одна из процедур наряду с объяснением и заучиванием (упражнение в этом случае обеспечивает завершение уяснения и закрепления).

К самостоятельной работе студентов также относятся: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление и разработка терминологического словаря; составление библиографии (библиографической картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, контрольной работе, зачету, экзамену); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, задачи, тесты; выполнение творческих заданий).

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

Важное место в структуре самостоятельной подготовки к занятиям принадлежит студенческим докладам и рефератам.

Доклад (сообщение) представляет собой развернутое сообщение на какую-либо тему, сделанное публично. Обычно в качестве тем для докладов предлагается тот материал учебного курса, который не освещается в лекциях, а выносится на самостоятельное изучение студентами. Поэтому доклады, сделанные студентами на практических занятиях, с одной стороны, позволяют дополнить лекционный материал, а с другой - дают преподавателю возможность оценить умение студентов самостоятельно работать с учебной и научной литературой.

Построение доклада, как и любой другой научной работы, традиционно включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается его логическая связь с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор литературы, на материале которых раскрывается тема и т. п. В заключении обычно подводятся итоги, формулируются выводы. Основная часть также должна иметь четкое логическое построение. Изложение материала должно быть связным, последовательным,

доказательным, лишенным ненужных отступлений и повторений. Таким образом, работа над докладом не только позволяет студенту приобрести новые знания, но и способствует формированию важных научно-исследовательских умений, освоению методов научного познания, приобретению навыков публичного выступления.

Реферат — письменная работа объемом 10-18 печатных страниц, выполняемая студентом в течение длительного срока (от одной недели до месяца). Реферат — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу. Реферат отвечает на вопрос — что содержится в данной публикации (публикациях). Однако реферат — не механический пересказ работы, а изложение ее существа. В настоящее время, помимо реферирования прочитанной литературы, от студента требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата может предложить преподаватель или сам студент, в последнем случае она должна быть согласованна с преподавателем. В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания. Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Конспектирование. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:

−План-конспект – это развернутый детализированный план, в котором достаточно подробные

−Текстуальный конспект – это воспроизведение наиболее важных положений и фактов источ

−Свободный конспект – это четко и кратко сформулированные (изложенные) основные полож

−Тематический конспект – составляется на основе изучения ряда источников и дает более или

Требования к оформлению письменных работ указаны в методических рекомендация.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

6.1. Образовательные технологии

Совместная работа малой командой; проектная деятельность студентов, развивающая межличностные коммуникации, способность принятия решений, лидерские качества; интерактивные лекции; групповые дискуссии; ролевые и деловые игры; тренинги; анализ ситуаций и имитационных моделей; преподавание дисциплин (модулей) в форме: курсов, симуляции, технологии open space/открытое пространство, мастерская будущего, peer education/равный обучает равного; экспресс-семинары, проектные семинары; бизнес-тренинги (business training), кейс-стади (case-study), обучение действием («action learning»), метафорическая игра, педагогические игровые упражнения (в качестве коллективного задания), мозговой штурм (эстафета), ситуационные методы, тематические дискуссии, игровое проектирование, групповой тренинг, групповая консультация и др.).

6.2. Информационные технологии

Информационные технологии, используемые при реализации различных видов учебной и внеучебной работы:

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

- использование электронных учебников и различных информационных сайтов (электронные библиотеки, журналы и т.д.) как источник информации;

- использование средств представления учебной информации (электронных учебных пособий и практикумов, электронных тренажеров, презентаций и т.д.);

- использование интерактивных средств взаимодействия участников образовательного процесса (технологии дистанционного или открытого обучения в

глобальной сети: веб-конференции, вебинары, форумы, учебно-методические материалы и др.);

- использование интегрированной образовательной среды университета moodle.

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

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
Notepad++	Текстовый редактор
OpenOffice	Пакет офисных программ
Opera	Браузер
Paint .NET	Растровый графический редактор
Scilab	Пакет прикладных математических программ
Microsoft Security Assessment Tool. - Режим доступа: http://www.microsoft.com/ru-ru/download/details.aspx?id=12273 (Free) Windows Security Risk Management Guide Tools and Templates. - Режим доступа: http://www.microsoft.com/en-us/download/details.aspx?id=6232 (Free)	Программы для информационной безопасности
MathCad 14	Система компьютерной алгебры из класса систем автоматизированного проектирования, ориентированная на подготовку интерактивных документов с вычислениями и визуальным сопровождением
1С: Предприятие 8	Система автоматизации деятельности на предприятии
KOMPAS-3D V21	Создание трёхмерных ассоциативных моделей отдельных элементов и сборных конструкций из них
Blender	Средство создания трёхмерной компьютерной графики
PyCharm EDU	Среда разработки
R	Программная среда вычислений
VirtualBox	Программный продукт виртуализации операционных систем
VLC Player	Медиапроигрыватель
Microsoft Visual Studio	Среда разработки

Наименование программного обеспечения	Назначение
Cisco Packet Tracer	Инструмент моделирования компьютерных сетей
CodeBlocks	Кроссплатформенная среда разработки
Eclipse	Среда разработки
Lazarus	Среда разработки
PascalABC.NET	Среда разработки
VMware (Player)	Программный продукт виртуализации операционных систем
Far Manager	Файловый менеджер
Sofa Stats	Программное обеспечение для статистики, анализа и отчётности
Maple 18	Система компьютерной алгебры
WinDjView	Программа для просмотра файлов в формате DJV и DjVu
MATLAB R2014a	Пакет прикладных программ для решения задач технических вычислений
Oracle SQL Developer	Среда разработки
VISSIM 6	Программа имитационного моделирования дорожного движения
VISUM 14	Система моделирования транспортных потоков
IBM SPSS Statistics 21	Программа для статистической обработки данных
ObjectLand	Геоинформационная система
КРЕДО ТОПОГРАФ	Геоинформационная система
Полигон Про	Программа для кадастровых работ

6.3.2. Современные профессиональные базы данных и информационные справочные системы

Наименование современных профессиональных баз данных, информационных справочных систем
Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС» https://dlib.eastview.com/login *Имя пользователя: AstrGU* *Пароль: AstrGU*
Электронные версии периодических изданий, размещённые на сайте информационных ресурсов https://www.polpred.com/
Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем» https://library.asu.edu.ru/catalog/
Электронный каталог «Научные журналы АГУ» https://journal.asu.edu.ru/
Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС) – сводная база данных, содержащая полную аналитическую роспись 1800 названий журналов по разным отраслям знаний. Участники проекта предоставляют друг другу электронные копии отсканированных статей из книг, сборников, журналов, содержащихся в фондах их библиотек. http://mars.arbicon.ru/
Справочная правовая система КонсультантПлюс. Содержится огромный массив справочной правовой информации, российское и региональное законодательство, судебную практику, финансовые и кадровые консультации, консультации для бюджетных организаций, комментарии законодательства, формы документов, проекты нормативных правовых актов, международные правовые акты, правовые акты, технические нормы и правила. https://www.consultant.ru/

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

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) 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, темы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1	Общая проблема информационной безопасности информационных систем. Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем. Технические предпосылки кризиса информационной безопасности. Этапы развития защиты информации. Современная постановка задачи защиты информации. Основные задачи обеспечения защиты информации.	УК-1	Фронтальный опрос
2	Угрозы и защита информации при реализации информационных процессов. Понятие угрозы. Виды противников или "нарушителей". Окно опасности. Классификация видов угроз информационной безопасности по различным признакам. Угрозы доступности, целостности и конфиденциальности.	УК-1	Фронтальный опрос
3	Причины нарушения безопасности вычислительных систем Понятие Таксономии. Таксономия угроз безопасности. Уязвимость защиты. Ошибки в системах защиты. Этапы появления ошибок защиты. Компоненты систем, где чаще всего проявляются ошибки защиты.	УК-1	Фронтальный опрос
4	Вредоносное ПО. Компьютерные вирусы и средства защиты от них Понятие компьютерного вируса. Признаки появления вируса. Классификация вирусов. Алгоритмическая особенность построения вируса. Вирусная сигнатура. Антивирусные	УК-1	Фронтальный опрос

	программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины.		
5	Защита информации от несанкционированного доступа Контроль доступа пользователей к ресурсам ИС. Монитор обращений. Структура монитора обращений. Идентификация и аутентификация пользователей ИС. Способы аутентификации.	УК-1	Фронтальный опрос
6	Формальные модели безопасности Базовые представления моделей безопасности. Два основных класса моделей политики безопасности – дискреционный и мандатный. Субъекты и объекты доступа. Дискреционная модель Хариссона-Руззо-Ульмана. Мандатная модель Белла-Лападулы.	УК-1	Фронтальный опрос
7	Стандарты информационной безопасности. Основы организационно-правового обеспечения информационной безопасности Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Европейские критерии безопасности информационных технологий. Уровни безопасности системы. Рекомендации X.800. Стандарт ISO 17799 – «Управление информационной безопасностью». Основные функции организационно-правовой базы. Виды информационных ресурсов. Открытая, запатентованная и защищаемая информация. Владельцы защищаемой информации. Понятие государственная тайна. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.	УК-1	Фронтальный опрос
8	Криптографические методы защиты Криптографические преобразования. Шифрование и дешифрование информации.	УК-1	Фронтальный опрос

	Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Шифрование информации с секретным ключом (симметричные алгоритмы). Сравнение симметричных и несимметричных алгоритмов шифрования. Контроль целостности данных. Цифровая подпись. Использование открытых ключей.		
9	Методология построения защищенных систем Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Теория безопасных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB). Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.	УК-1	Фронтальный опрос

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

Для оценивания результатов обучения в виде знаний используются следующие типы контроля:

- тестирование;
- индивидуальное собеседование,
- письменные ответы на вопросы.

Для оценивания результатов обучения в виде умений и владений используются следующие типы контроля:

- практические контрольные задания (далее – ПКЗ), включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить.

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

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

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

Темы рефератов:

1. Угроза, атака, источники угроз. Что такое окно опасности. Критерии классификации угроз.
2. Наиболее распространенные угрозы доступности.
3. Программные угрозы доступности.
4. Основные угрозы целостности. Статическая и динамическая целостность.
5. Основные угрозы конфиденциальности.
6. Таксономия угроз безопасности. Что такое уязвимость защиты?. Таксономия угроз безопасности. Ошибки в системах защиты.
7. Что такое компьютерный вирус? Признаки проявления вируса.
8. Классификация компьютерных вирусов – по среде обитания, по степени воздействия, по способам заражения среды обитания, по алгоритмической особенности построения.
9. Что такое антивирусная программа? Вирусная сигнатура. Виды антивирусных программ.
10. Основополагающие принципы решения задачи закрытия каналов несанкционированного доступа.
11. Понятие политики и модели безопасности. Структура монитора обращений.
12. Методы идентификации и аутентификации. Способы аутентификации – пользователь «знает», пользователь «имеет» и пользователь «есть».
13. Базовые представления моделей безопасности. Субъекты, объекты и доступ.
14. Произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. Модель Харрисона-Руззо-Ульмана..

15. Мандатная модель Белла-Лападулы. Свойство простой безопасности. Свойства ограничения. Свойство самостоятельной защиты. Правила перехода.

16. Какая главная задача стандартов информационной безопасности? «Оранжевая книга» США. Базовые требования безопасности. Четыре группы критериев безопасности.

17. Европейские критерии безопасности информационных технологий. Адекватность средств защиты. Уровни безопасности системы.

Вопросы для контроля

1. Основные понятия информационной безопасности. Защита информации. Управление информационной безопасностью. Модель безопасности. Прямое воздействие.
2. Понятие защищенной системы.
3. Как изменялся подход к задаче защите информации? Три этапа развития защиты информации.
4. Теория защиты информации. Основные составные части теории защиты информации.
5. Современная постановка задачи защиты информации.
6. Угроза, атака, источники угроз. Что такое окно опасности. Критерии классификации угроз.
7. Наиболее распространенные угрозы доступности.
8. Программные угрозы доступности.
9. Основные угрозы целостности. Статическая и динамическая целостность.
10. Основные угрозы конфиденциальности.
11. Таксономия угроз безопасности. Что такое уязвимость защиты?. Таксономия угроз безопасности. Ошибки в системах защиты.
12. Что такое компьютерный вирус? Признаки проявления вируса.
13. Классификация компьютерных вирусов – по среде обитания, по степени воздействия, по способам заражения среды обитания, по алгоритмической особенности построения.
14. Что такое антивирусная программа? Вирусная сигнатура. Виды антивирусных программ.
15. Основополагающие принципы решения задачи закрытия каналов несанкционированного доступа.
16. Понятие политики и модели безопасности. Структура монитора обращений.
17. Методы идентификации и аутентификации. Способы аутентификации – пользователь «знает», пользователь «имеет» и пользователь «есть».
18. Базовые представления моделей безопасности. Субъекты, объекты и доступ.
19. Произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. Модель Харрисона-Руззо-Ульмана..
20. Мандатная модель Белла-Лападулы. Свойство простой безопасности. Свойства ограничения. Свойство самостоятельной защиты. Правила перехода.
21. Какая главная задача стандартов информационной безопасности? «Оранжевая книга» США. Базовые требования безопасности. Четыре группы критериев безопасности.
22. Европейские критерии безопасности информационных технологий. Адекватность средств защиты. Уровни безопасности системы.
23. Основные руководящие документы Гостехкомиссии по вопросам защиты от несанкционированного доступа к информации. Классы защищенности.
24. ГОСТ Р ИСО МЭК 15048-2002 «Общие критерии оценки безопасности информационных технологий». Профиль защиты. функции безопасности. Предложения безопасности.

25. Основные функции организационно-правовой базы защиты информации. Виды информационных ресурсов. Какую информацию относят к защищаемой?

26. Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна».

27. Криптографические механизмы и примитивы. Базовые методы преобразования информации используемые в криптографии. Основные группы методов защитных преобразований. Методы перестановки, подстановки, аддитивные и комбинированные.

28. Криптография с симметричными ключами. Алгоритм DES, ГОСТ 28147-80., IDEA. Преимущества и недостатки криптографии с симметричными ключами.

29. Ассиметричные алгоритмы шифрования. Криптосистема с открытым ключом RSA. ХЕШ-функция. Понятие односторонней функции. Коллизия хэш-функции.

30. Иерархический метод разработки защищенных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB).

31. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

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

Грубыми считаются ошибки, свидетельствующие о том, что студент:

- не овладел основным материалом дисциплины
- не может применять на практике полученные знания

Не грубыми ошибками являются

- неточно сформулированный вопрос или пояснение при ответе

Недочетами считаются

- отдельные погрешности в формулировке вопроса или ответа
- небрежное выполнение записей.

Преподаватель, реализующий дисциплину (модуль), в зависимости от уровня подготовленности обучающихся может использовать иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

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

8.1. Основная литература

1) Малюк А.А., «Информационная безопасность : концептуальные и методологические основы защиты информации», -М. : Горячая линия-Телеком, 2004г.
2) Мельников В.П. «Информационная безопасность и защита информации», -М.: Академия, 2009г.
3) Садердинов А.А. и др. «Информационная безопасность предприятия», -М. : Дашков и К, 2005г.
4) Семененко В.А. «Информационная безопасность», -М : МГИУ, 2005г.39 экз.

8.2. Дополнительная литература

1) Малюк А. А. Введение в защиту информации в автоматизированных системах: Учебное пособие для студентов вузов - М.: ГОРЯЧАЯ ЛИНИЯ - ТЕЛЕКОМ, 2005.
2) Мельников В.П. «Информационная безопасность», -М.: Академия, 2005г.
3) Мельников В.П. и др. «Информационная безопасность», -М. : Академия, 2005г.
4) А. А. Снытников Лицензирование и сертификация в области защиты информации. - Гелиос АРВ, 2009.
5) Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : рек. УМО вузов по университетскому политехническому образованию в качестве учеб. пособ. для вузов... по специальности "Информатика и вычислительная техника" . - М. : Академия, 2005. - 256 с. - (Высшее профессиональное образование).

6) Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы : рек. М-вом образования РФ в качестве учеб. пособ. для вузов... по направлению - "Информатика и вычислительная техника" и по специальностям "Вычислительные машины,комплексы, системы и сети", "Программое обеспечение вычислительной техники и автоматизированных систем". - 3-е изд. - СПб. : Питер, 2006. - 958 с. : илл. - (Учебник для вузов).
7) Олифер, В.Г. Сетевые операционные системы : доп. М-вом образования РФ в качестве учеб. пособ. для вузов... "Информатика и вычислительная техника" . - СПб. : Питер, 2006. - 539 с. - (Учебник для вузов).

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

8.3.1 Перечень электронно-библиотечных систем (ЭБС)

1) **Электронная библиотечная система IPRbooks**
www.iprbookshop.ru
2) **Электронно-библиотечная система BOOK.ru**
https://book.ru
3) **Электронная библиотечная система издательства ЮРАЙТ, раздел «Легендарные книги»**
www.biblio-online.ru, https://urait.ru/
4) **Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех»**
https://biblio.asu.edu.ru
Учётная запись образовательного портала АГУ
5) **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента»**
Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через Интернет к учебной литературе и дополнительным материалам, приобретённым на основании прямых договоров с правообладателями. Каталог содержит более 15 000 наименований изданий.
www.studentlibrary.ru
Регистрация с компьютеров АГУ
6) **Электронная библиотечная система «Университетская библиотека онлайн»**
www.biblioclub.ru

8.3.2 Перечень общедоступных официальных интернет-ресурсов

1) Единое окно доступа к образовательным ресурсам
http://window.edu.ru
2) Министерство науки и высшего образования Российской Федерации
https://minobrnauki.gov.ru
3) Министерство просвещения Российской Федерации
https://edu.gov.ru
4) Федеральное агентство по делам молодёжи (Росмолодёжь)
https://fadm.gov.ru
5) Федеральная служба по надзору в сфере образования и науки (Рособрнадзор)
http://obrnadzor.gov.ru
6) Сайт государственной программы Российской Федерации «Доступная среда»
http://zhit-vmeste.ru
7) Российское движение школьников
https://рдш.рф

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Мультимедийное оборудование. На аудиторных занятиях (лекциях) СИТ используются для организованного представления преподавателями и обучающимися материала в формате презентаций PowerPoint, работы по формированию и развитию навыков работы с документами и программами, имеющими прикладное значение. Лекции обеспечены слайдами и видеоматериалами. Имеются классные доски, наглядные пособия (стенды, макеты, плакаты и т.п.).

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).