Министерство образования и науки Российской Федерации
Нижнетагильский государственный социально-педагогический институт (филиал)
федерального государственного автономного образовательного учреждения
высшего образования
«Российский государственный профессионально-педагогический университет»

Факультет естествознания, математики и информатики
Кафедра информационных технологий

УТВЕРЖДАЮ
Зам. директора по УМР

_____ Л. П. Филатова

«____»_____2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования	Бакалавриат
Направления подготовки	09.03.03 Прикладная информатика
Профили	«Прикладная информатика в экономике»
Формы обучения	Очная, заочная

Нижний Тагил
2018

Рабочая программа дисциплины «Информационная безопасность». Нижний Тагил : Нижнетагильский государственный социально-педагогический институт (филиал) ФГАОУ ВО «Российский государственный профессионально-педагогический университет», 2018. – 17 с.

Настоящая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика.

Автор: кандидат педагогических наук, доцент кафедры информационных технологий Е. С. Васева

Рецензент Зам. Директора по ИТ МУП «НТТС» Д.В. Виноградов

Одобрена на заседании кафедры информационных технологий 21 июня 2018 г., протокол № 12.

Заведующая кафедрой М. В. Мащенко

Председатель методической комиссии ФЕМИ В. А. Гордеева

Рекомендована к печати методической комиссией факультета естествознания, математики и информатики 13 сентября 2018 г., протокол № 1.

Декан ФЕМИ Н. В. Жуйкова

Зав отделом АВТ и МТО научной библиотеки О. В. Левинских

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины: формирование компетенций в области обеспечения информационной безопасности в процессе решения профессиональных задач.

Задачи:

1. Познакомить студентов с правовыми основами обеспечения информационной безопасности.

2. Раскрыть понятийный аппарат фундаментального и прикладного аспектов курса.

3. Сформировать целостную систему знаний о современных моделях обеспечения безопасности управления информационными ресурсами.

4. Познакомить студентов с технологиями обеспечения информационной безопасности средствами систем обеспечения безопасности информации.

5. Сформировать умения использования соответствующих инструментальных программных средств обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» является частью учебного плана по направлению подготовки 09.03.03 Прикладная информатика. Дисциплина включена в Блок Б.1 «Дисциплины (модули)» и является составной частью раздела Б1.Б. «Базовая часть». Реализуется кафедрой информационных технологий.

Дисциплина базируется на компетенциях, полученных при изучении дисциплин «Информатика и программирование», «Информационные системы и технологии», «Теория систем и системный анализ», «Вычислительные системы, сети и телекоммуникации» и ряда других дисциплин.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование и развитие следующих компетенций:

ОПК-4 – способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ПК-1 – способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.

В результате освоения дисциплины обучающийся должен:

знать:

З1. основные понятия курса.

З2. административное и организационно-правовое обеспечение защиты информации.

З3. основные методологические положения защиты информации.

З4. основные сервисы современных информационных систем обеспечения информационной безопасности.

З5. основные программно-аппаратные средства защиты цифровой информации.

З6. особенности работы с антивирусными программами.

З7. достоинства и недостатки, перспективы развития современных систем защиты информации.

уметь:

У1. ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему.

У2. организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа.

У3. организовывать безопасную работу в Интернет.

У4. выполнять резервное копирование, восстановление данных в различных информационных системах.

У5. использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

владеть навыками:

В1. установки и настройки сервисов программного обеспечения.

В2. анализа деятельности организации на соответствие нормативно-правовым актам в области информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоемкость дисциплины составляет 5 зач. ед. (180 часов), их распределение по видам работ представлено в таблице.

Распределение трудоемкости дисциплины по видам работ

Вид работы	**Форма обучения**	
	очная	**заочная**
	Кол-во часов	**Кол-во часов**
Общая трудоемкость дисциплины по учебному плану	**180**	**180**
Контактная работа, в том числе:	**62**	**20**
Лекции	22	6
Лабораторные занятия	40	14
Самостоятельная работа, в том числе:	**118**	**160**
Самоподготовка к текущему контролю знаний	64	147
Подготовка к зачету	9	4
Подготовка к экзамену	45	9

4.2. Содержание и тематическое планирование дисциплины

4.2.1. Тематический план для очной формы обучения

Наименование разделов и тем дисциплины (модуля)	**Всего часов**	**Вид контактной работы, час**			**Самостоятельная работа, час**	**Формы текущего контроля успеваемости**
		Лекции	**Лаб. работы**	**Из них в интерактивной форме**		
Введение в проблему информационной безопасности	5	1		1	4	

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час			Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы	Из них в интерактивной форме		
Угрозы информационной безопасности и методы их реализации	8	2	2	1	4	тест, отчет по лабораторной работе
Правовые и организационные аспекты защиты информации	7	1	2	1	4	тест, отчет по лабораторной работе
Административный уровень обеспечения информационной безопасности	8	2	2	1	4	тест, отчет по лабораторной работе
Процедурный уровень обеспечения информационной безопасности	7	1	2	1	4	тест, отчет по лабораторной работе
Программно-технический уровень обеспечения информационной безопасности	37	3	14	1	20	тест, отчет по лабораторной работе
Криптография	35	6	10	1	19	тест, отчет по лабораторной работе
Стеганография	12	2	4	1	6	тест, отчет по лабораторной работе
Методы защиты информации в вычислительных сетях	25	4	4	1	17	тест, отчет по лабораторной работе
Зачет	9				9	
Экзамен	27				27	выполнение заданий на экзамене
Итого	**180**	**22**	**40**	**9**	**118**	

4.2.2. Тематический план для заочной формы обучения

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час			Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы	Из них в интерактивной форме		
Введение в проблему информационной безопасности	5	0,5			4,5	тест

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час			Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы	Из них в интерактивной форме		
Угрозы информационной безопасности и методы их реализации	8	0,5		1	7,5	тест, отчет по лабораторной работе
Правовые и организационные аспекты защиты информации	7	0,5	1	1	5,5	тест, отчет по лабораторной работе
Административный уровень обеспечения информационной безопасности	8	0,5	1	1	6,5	тест, отчет по лабораторной работе
Процедурный уровень обеспечения информационной безопасности	7	0,5	1	1	5,5	тест, отчет по лабораторной работе
Программно-технический уровень обеспечения информационной безопасности	43	1	6	1	36	тест, отчет по лабораторной работе
Криптография	36	1	2	1	33	тест, отчет по лабораторной работе
Стеганография	18	0,5	1		16,5	тест, отчет по лабораторной работе
Методы защиты информации в вычислительных сетях	35	1	2	1	32	тест, отчет по лабораторной работе
Зачет	4				4	
Экзамен	9				9	выполнение заданий на экзамене
Итого	**180**	**6**	**14**	**8**	**160**	

4.3. Содержание тем дисциплины

Тема 1. Введение в проблему информационной безопасности.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.

Тема 2. Угрозы информационной безопасности и методы их реализации.

Виды возможных нарушений информационной системы. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы наруше-

ния секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Тема 3. Правовые и организационные аспекты защиты информации.

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления.

Тема 4. Административный уровень обеспечения информационной безопасности.

Основные понятия. Концепция безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Анализ рисков информационной системы предприятия. Стратегии управления рисками.

Тема 5. Процедурный уровень обеспечения информационной безопасности.

Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Тема 6. Программно-технический уровень обеспечения информационной безопасности.

Основные сервисы программно-технического уровня обеспечения информационной безопасности. Идентификация и аутентификация. Парольная аутентификация. Логическое управление доступом. Компьютерные вирусы, классификация. Признаки заражения компьютера вредоносным программным обеспечением. Средства защиты от компьютерных вирусов. Протоколирование и аудит. Криптографические средства защиты. Экранирование.

Тема 7. Криптография.

Классификация криптографических систем. Шифры замены. Шифры перестановки. Шифры гаммирования. Основные методы шифрования. Схема режима шифрования DES-ECB. Схема режима шифрования DES-CBC. Схема режима шифрования DES-CPB и DES-OFB. Тройной DES. Сферы применения различных режимов DES.Схема режима шифрования простой замены ГОСТ 28147-89. Шифрование с открытым ключом. Алгоритм шифрования RSA. Алгоритм шифрования Эль-Гамаля. Алгоритм шифрования на основе задачи об укладке ранца. Хэш-функции. Криптографические протоколы. Протоколы обмена ключами. Протоколы аутентификации. Протокол идентификации/аутентификации на основе шифрования с открытым ключом. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП. Протоколы контроля целостности. Электронные платежи. Криптоанализ и атаки на криптосистемы.

Тема 8. Стеганография.

Классическая стеганография. Компьютерная стеганография. Использование специальных свойств компьютерных форматов. Использование избыточности аудио и визуальной информации. Сравнительная характеристика методов компьютерной стеганографии. Использование стеганографии в управлении системами мониторинга и сетевыми ресурсами, анализе контента, камуфлировании программного обеспечения, защите авторских прав.

Тема 9. Методы защиты информации в вычислительных сетях.

Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика (анализ сетевого трафика, подмена доверенного объекта, ложный объект, отказ в обслуживании). Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.

Содержание лабораторных работ по курсу

Тема занятия	Количество часов (очная форма обучения)	Количество часов (заочная форма обучения)
1. Анализ угроз информационной безопасности.	2	
2. Анализ основных нормативных документов в области информационной безопасности.	2	1
3. Политика информационной безопасности организации. Частная модель угроз.	2	1
4. Разработка локальных нормативных актов	2	1
5. Обеспечение безопасности при работе с документами.	2	
6. Возможности защиты информации в операционной системе Windows.	2	1
7. Управление правами пользователей.	2	1
8. Основные признаки присутствия на компьютере вредоносных программ.	2	1
9. Установка и предварительная настройка антивирусной программы.	2	1
10. Работа с реестром.	2	1
11. Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации	2	1
12. Изучение симметричных алгоритмов шифрования	2	1
13. Изучение ассиметричных алгоритмов шифрования	2	1
14. Стандарты шифрования	2	
15. Реализация протокола шифрования с помощью одного из языков программирования	4	
16. Защита программного обеспечения методами стеганографии	2	1
17. Работа с командной строкой. Сетевая активность.	2	1
18. Защита от несанкционированного доступа	4	1

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Представленный курс предусматривает наличие теоретических лекционных занятий, на которых студенты знакомятся с фундаментальными основами и принципами защиты информации на современном этапе развития информационных технологий студенты формируют навыки безопасной работы с различными видами информации.

Основными методами, используемыми при объяснении теоретического материала, являются:

– активные лекции;
– лекции с использованием презентаций;
– лекции с использованием демонстрационных материалов.

Основными методами, используемыми для практических занятий, являются:

– практикум с использованием демонстрационных примеров.

6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Планирование самостоятельной работы (очная форма обучения)

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. Работы		
Введение в проблему информационной безопасности	5	1	4	Самостоятельное изучение теоретических вопросов – п.1,2 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к тесту	Обсуждение тезисов, тест
Угрозы информационной безопасности и методы их реализации	8	4	4	Самостоятельное изучение теоретического вопроса – п.5 (список прилагается). Подготовка таблицы по видам угроз информационной безопасности. Подготовка к тесту.	Проверка таблицы по видам угроз информационной безопасности. Обсуждение на занятии. Тест
Правовые и организационные аспекты защиты информации	7	3	4	Самостоятельное изучение теоретических вопросов – п.3,4 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к лабораторному занятию. Выполнение домашней работы №1. Подготовка к тесту	Обсуждение тезисов, отчет по лабораторной работе, тест
Административный уровень обеспечения информационной безопасности	8	4	4	Подготовка к лабораторной работе, тесту	Отчет по лабораторной работе, тест
Процедурный уровень обеспечения информационной безопасности	7	3	4	Подготовка к лабораторной работе, тесту	Отчёт по лабораторной работе, тест
Программно-технический уровень обеспечения информационной безопасности	37	17	20	Выполнение домашней работы №2, 3. Подготовка к лабораторной работе, тесту	Обсуждение домашней работы. Отчёт по лабораторной работе, тест
Криптография	35	16	19	Выполнение до-	тест, отчет по

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. Работы		
				машней работы №4. Подготовка к тесту	лабораторной работе
Стеганография	12	6	6	Подготовка к лабораторной работе. Подготовка к тесту	тест, отчет по лабораторной работе
Методы защиты информации в вычислительных сетях	25	8	17	Подготовка к лабораторной работе. Подготовка к тесту	тест, отчет по лабораторной работе
Зачет	9		9		
Экзамен	27		27	Подготовка к лабораторной работе. Подготовка к тесту	Выполнение заданий на экзамене
Всего	**180**	**62**	**118**		

6.2. Планирование самостоятельной работы (заочная форма обучения)

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. работы		
Введение в проблему информационной безопасности	5	0,5	4,5	Самостоятельное изучение теоретических вопросов – п.1,2 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к тесту	Обсуждение тезисов, тест
Угрозы информационной безопасности и методы их реализации	8	0,5	7,5	Самостоятельное изучение теоретического вопроса – п.5 (список прилагается). Подготовка таблицы по видам угроз информационной безопасности. Подготовка к тесту.	Проверка таблицы по видам угроз информационной безопасности. Обсуждение на занятии. Тест
Правовые и организационные аспекты защиты информации	7	1,5	5,5	Самостоятельное изучение теоретических вопросов – п.3,4 (список прилагается), подготовка тезисов по	Обсуждение тезисов, отчет по лабораторной работе, тест

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. работы		
				изученному материалу. Подготовка к лабораторному занятию. Выполнение домашней работы №1. Подготовка к тесту	
Административный уровень обеспечения информационной безопасности	8	1,5	6,5	Подготовка к лабораторной работе, тесту	Отчет по лабораторной работе, тест
Процедурный уровень обеспечения информационной безопасности	7	1,5	5,5	Подготовка к лабораторной работе, тесту	Отчёт по лабораторной работе, тест
Программно-технический уровень обеспечения информационной безопасности	43	7	36	Выполнение домашней работы №2, 3. Подготовка к лабораторной работе, тесту	Обсуждение домашней работы. Отчёт по лабораторной работе, тест
Криптография	36	3	33	Выполнение домашней работы №4. Подготовка к тесту	тест, отчет по лабораторной работе
Стеганография	18	1,5	16,5	Подготовка к лабораторной работе. Подготовка к тесту	тест, отчет по лабораторной работе
Методы защиты информации в вычислительных сетях	35	3	32	Подготовка к лабораторной работе. Подготовка к тесту	тест, отчет по лабораторной работе
Зачет	4		4	Подготовка к лабораторной работе. Подготовка к тесту	Выполнение заданий на экзамене
Экзамен	9		9		
Всего	**180**	**20**	**160**		

6.3. Задания и методические указания по организации самостоятельной работы

Список вопросов, выносимых на самостоятельное изучение

1. История развития систем защиты информации.
2. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах.
3. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
4. Компьютерные преступления.
5. Основные методы реализации угроз информационной безопасности.

Задания для самостоятельной работы (домашние задания)

В рамках самостоятельной работы студентов предусмотрено выполнение творческих домашних заданий. Их цель – закрепление знаний, полученных на практических занятиях.

Домашнее задание №1.

Найти и проанализировать статистических данные об атаках, которым подвергаются компьютерные системы и потерях банков.

Домашнее задание №2.

Проанализировать компьютерные средства реализации защиты в информационных системах вуза, выявить недостатки и предложить пути их решения.

Домашнее задание №3.

Выполнить анализ эффективности 2-3 антивирусных программ.

Домашнее задание №4.

− На основе схемы жизненного цикла криптографических ключей по стандарту ISO/IEC 11770 покажите схемы жизненного цикла секретных и открытых ключей асимметричных криптосистем. Чем они различаются?

− На основе схемы жизненного цикла криптографических ключей по стандарту ISO/IEC 11770 покажите схемы жизненного цикла общих секретных ключей симметричных криптосистем и персональных секретных ключей асимметричных криптосистем. Чем они различаются?

− Предположим, что, используя доступные на сегодняшний день на рынке аппаратные компоненты, возможно собрать компьютер стоимостью около 200 долларов США, который осуществляет опробование около 1 миллиарда ключей алгоритма ГОСТ Р 34.12-2015 в секунду. Предполагая, что конкуренты (или злоумышленники) хотят осуществить поиск одного 256-битного ключа алгоритма ГОСТ Р 34.12-2015 методом тотального опробования и имеют возможность потратить на закупку техники около 4 триллионов долларов США (что на самом деле превышает годовой бюджет США), рассчитайте, какое время займет (в среднем) тотальное опробование для поиска одного 256битного ключа с использованием закупленной техники? (Дополнительные расходы, такие как электроэнергия и тех. поддержка, не принимаются во внимание).

Домашнее задание №5.

Составить схему классификации систем цифровой стеганографии.

Домашнее задание №6.

Перечислите наиболее важные факторы и условия, которые следует учесть при разработке методов по защите информации в информационной среде. Проиллюстрируйте ваш ответ на конкретном примере информационной среды (школа, библиотека, ваша семья, супермаркет, кинотеатр, любая другая среда на ваш выбор).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Курило А.П. Основы управления информационной безопасностью. [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.].– М.: Горячая линия-Телеком, 2012. 244 с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5178

2. Малюк А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. М.: Горячая линия-Телеком, 2012. 288 с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5171

3. Милославская Н.Г. Управление рисками информационной безопасности [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Тол-

стой. М.: Горячая линия-Телеком, 2012. 130 с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5179

4. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. Прохорова. Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. Режим доступа: http://www.iprbookshop.ru/43183.html

Дополнительная литература

5. Васильев, В.И. Интеллектуальные системы защиты информации [Электронный ресурс] : учебное пособие / В.И. Васильев. М.: Машиностроение, 2013. — 172 с. Режим доступа: https://e.lanbook.com/book/5792

6. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 266 с. Режим доступа: http://www.iprbookshop.ru/52209.html

7. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 154 с. Режим доступа: http://www.iprbookshop.ru/52160.html

8. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. М.: Горячая линия-Телеком, 2012. – 616 с. Режим доступа: https://e.lanbook.com/book/5154

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория 201А: 35 посадочных мест для студентов, 11 рабочих мест для студентов, рабочее место преподавателя, маркерная доска, интерактивная доска, 12 компьютеров, стационарный мультимедиакомплекс, учебный сервер.

9. ТЕКУЩИЙ КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Качество усвоения учебного материала осуществляется по результатам выполнения заданий для самостоятельной работы на занятии, домашних работ. Особое место в контроле качества занимают отчеты по вопросам, выносимым на самостоятельное изучение. Целесообразно использование следующих форм текущего контроля:

- промежуточный контроль на практических занятиях для оценки самостоятельной работы студента при подготовке к ним;
- обсуждение результатов работы на занятиях и дома;

По результатам текущего контроля принимается решение на допуск студента к итоговому контролю (экзамену).

10. ИТОГОВАЯ АТТЕСТАЦИЯ

Итоговая аттестация выпускников представляет собой форму контроля (оценки) освоения выпускниками программы «Информационная безопасность» в соответствии с требованиями, установленными к содержанию, структуре и условиям реализации программы.

Перечень обязательных видов работы студента, необходимых для получения допуска к экзамену:

- Посещение лекционных занятий.
- Ответы на теоретические вопросы на лабораторных занятиях.
- Решение практических задач на лабораторных занятиях, выполнение заданий для самостоятельной работы.

− Выполнение домашних работ.

Критерии оценки:

«Отлично» выставляется студентам, успешно сдавшим экзамен и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими примерами, пра-вильно и без ошибок выполнивших практическое задание.

«Хорошо» выставляется студентам, сдавшим экзамен с незначительными замечаниями, показавшим глубокое знание теоретического вопроса, умение проиллюстрировать изложение практическими примерами, выполнившим практическое задание в целом верно, допустившим незначительные ошибки, указывающие на наличие несистематичности и пробелов в знаниях.

«Удовлетворительно» выставляется студентам, сдавшим экзамен со значительными замечаниями, показавшим знание основных положений теории при наличии существенных пробелов, испытывающим затруднения при выполнении практической работы.

«Неудовлетворительно» выставляется, если студент показал существенные пробелы в знаниях основных положений теории, не умеет применять теоретические знания на практике, не выполнил практическое задание.

Примерные теоретические вопросы

1. Проблема информационной безопасности. Основные понятия.
2. Угрозы информационной безопасности.
3. Уровни обеспечения информационной безопасности.
4. Правовое обеспечение информационной безопасности. Основные нормативные документы.
5. ФЗ «О персональных данных».
6. Концепция информационной безопасности предприятия.
7. Политика информационной безопасности предприятия.
8. Анализ рисков информационной системе предприятия.
9. Стратегии управления рисками.
10. Процедурные меры обеспечени информационной безопасности.
11. Основные сервисы программно-технического уровня обеспечения информационной безопасности.
12. Идентификация и аутентификация.
13. Парольная аутентификация.
14. Биометрическая аутентификация.
15. Логическое управление доступом.
16. Компьютерные вирусы, классификация.
17. Признаки заражения компьтера вредоносным программным обеспечением.
18. Средства защиты от компьютерных вирусов.
19. Протоколирование и аудит.
20. Экранирование.
21. Классификация криптографических систем.
22. Симметричные алгоритмы шифрования.
23. Асимметричные алгоритмы шифрования.
24. Криптографические протоколы.
25. Электронная цифровая подпись.
26. Защита информации в сервисах электронных платежей.
27. Криптоанализ и атаки на криптосистемы.
28. Классическая стеганография.
29. Компьютерная стеганография.
30. Удаленные угрозы в вычислительных сетях.
31. Принципы защиты распределенных вычислительных сетей.

Примерные практические задания

Задание 1.

Выполните поиск и анализ перечисленных документов в одной из справочно-информационных систем, заполните следующую таблицу:

№ п.п.	Название нормативно-правового документа	Дата принятия	Краткий обзор документа
	Об информации, информатизации и защите информации		

Задание 2.

Разработайте кроссворд по основным понятиям информационной безопасности. Установите пароль на изменение файла, пользователь, имеющий право на изменение может вносить записи только в ячейки кроссворда, не изменяя структура и формулировку вопросов. Установите пароль на открытие файла. Добавьте видимую цифровую подпись к документу.

Задание 3.

В программе Microsoft Excel создайте тест (4-5 вопросов) по теоретическим основам информатики. При вводе правильного ответа соответствующая ячейка должна загораться зеленым цветом. Организуйте защиту файла таким образом, чтобы отвечающему не были доступны сведения, необходимые для проверки ответов.

Задание 4.

С официального сайта GoogleChrome скачайте и установите плагин, позволяющий настроить белый список сайтов, настройте его для работы школьников по теме «Алгоритмизация и программирование», при анализе информационных ресурсов используйте федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Задание 5.

Создайте нового пользователя «Бухгалтер» в операционной системе, назначьте ему группу пользователя, выбор обоснуйте. Для пользователя «Бухгалтер» настройте главное меню и рабочий стол так, чтобы доступ открывался только к рабочим файлам, настройки осуществляйте с учетной записи администратора.

Задание 6.

Выберите и установите на компьютер утилиту, позволяющую осуществить чистку реестра компьютера. Отключите автозапуск программ, обоснуйте выбор отключаемых программ. Найдите на компьютере все файлы дубликаты.

Задание 7.

Выберите и установите на компьютер антивирусное программное обеспечение. Выполните следующие настройки:

- Установить пароль, сделать общедоступными «Общий доступ к программе» и «Контроль обновлений», все остальные варианты включить в защиту.
- Добавить в исключения сайт https://www.ntspi.ru/ , а в усиленный режим сканирования добавить одну из программ, установленных на компьютере.
- Настроить выгрузку отчетов для веб-экранов в формате HML , в отчет включить: зараженные файлы, серьезные ошибки и файлы, не прошедшие проверку.
- Ограничить доступ с компьютера к трем сайтам. Попробовать перейти на эти сайты.
- Просканировать одну из папок, находящуюся на компьютере.

Задание 8.

Одна фирма предложила устройство для автоматической проверки пароля. Паролем может быть любой непустой упорядоченный набор букв в алфавите *{a, b, c}*. Будем обозначать такие наборы большими латинскими буквами. Устройство перерабатывает введенный в него набор *P* в набор *Q = F(P)*. Отображение *F* держится в секрете, однако про него известно, что оно определено не для каждого набора букв и обладает следующими свойствами. для любого набора букв *P*

1) *F(aP) = P*;

2) *F (bP) = F (P)a F(P)*;

3) набор *F(cP)* получается из набора *F(P)* переписыванием его букв в обратном порядке.

Устройство признает предъявленный пароль верным, если *F(P) =P*. Например, трехбуквенный набор *bab*является верным паролем, так как *F(bab) = F(ab) a F(ab) = bab*.

Подберите верный пароль, состоящий более чем из трех букв.

Задание 9.

Злоумышленник хочет получить доступ к банковской ячейке, защищенной кодовым замком. Комбинация из трех цифр (u,v,w), отпирающая замок, ему не известна. Злоумышленнику удалось изготовить проксимити-карты со следующей информацией: на первой карте записаны цифры (1,5,8), на второй – (7,4,9), на третьей – (9,7,6), на четвертой – (3,2,4). При прикладывании карты с информацией (a,b,c) к считывающему устройству банковской ячейки, ее кодовый замок из состояния (i,j,k) переходит в состояние (i+a,j+b,k+c). (Если какая-либо сумма превосходит 9, то она заменяется ее остатком от деления на 10.) Как только замок оказывается в состоянии (u,v,w), он немедленно открывается. Какое наименьшее количество из имеющихся карт следует использовать, чтобы гарантированно открыть ячейку, независимо от установленной отпирающей комбинации (u,v,w) и начального состояния замка?