УТВЕРЖДАЮ

Зам. директора по УВР
УрСЭИ (филиал) ОУП ВО «АТиСО»
_____О.В. Зубкова
«10» июня 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность
(название дисциплины в соответствии с учебным планом)

СПЕЦИАЛЬНОСТЬ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

09.02.05 Прикладная информатика (по отраслям)
(код профессии, специальности СПО)

Техник-программист
(наименование квалификации)

Кафедра: Гуманитарных, естественнонаучных и математических дисциплин

Разработчики программы: Мадудин В.Н., к.т.н., доцент

Челябинск -2020

Оглавление

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 3
1.1. Область применения рабочей программы учебного предмета, курса, дисциплины (модуля) 3
1.2. Цели и задачи учебной дисциплины 3
1.3. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена 3
1.4. Требования к результатам освоения учебной дисциплины 3
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 4
2.1. Объем учебной дисциплины и виды учебной работы 4
2.2. Тематический план и содержание учебной дисциплины 4
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 5
3.1 Требования к минимальному материально-техническому обеспечению 5
3.2. Информационное обеспечение реализации программы 6
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 7
5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 9
6. ОЦЕНОЧНЫЕ СРЕДСТВА И КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ 10
6.1 Оценочные средства для проведения текущего контроля по учебной дисциплине 10
6.2 Контрольно-измерительные материалы для проведения текущего контроля по учебной дисциплине 12
7. ОЦЕНОЧНЫЕ СРЕДСТВА И КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО УЧЕБНОЙДИСЦИПЛИНЕ 13
7.1. Оценочные средства для проведения промежуточной аттестации 13
по учебной дисциплине 13
7.2. Контрольно-измерительные материалы для проведения промежуточной аттестации по учебной дисциплине 16
8. ПРОВЕРКА СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ 17

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы учебного предмета, курса, дисциплины (модуля)

Рабочая программа учебной дисциплины «Информационная безопасность» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.05 «Прикладная информатика (по отраслям)», квалификация Техник-программист.

1.2. Цели и задачи учебной дисциплины

Цель изучения учебной дисциплины: ознакомление студентов с современными способами и средствами защиты информации, реализуемыми в виде технических, программных средств или организационных мер, экономическими и правовыми принципами их функционирования, а также возможностями использования защиты в работе с информационными ресурсами в различных областях.

Задачи изучения учебной дисциплины:

- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок;
- настройка и обслуживание аппаратно-программных средств.

1.3. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена

Учебная дисциплина «Информационная безопасность» в программе подготовки специалистов среднего звена относится к общепрофессиональным дисциплинам специальности09.02.05 «Прикладная информатика (по отраслям)».

Учебная дисциплина «Информационная безопасность» основывается на знаниях, умениях и готовностях обучающегося, сформированных в процессе изучения дисциплины ОУДП.01 «Информатика».

Знания, умения и навыки, полученные студентами при изучении данной дисциплины, будут использованы при прохождении производственной и преддипломной практик.

1.4. Требования к результатам освоения учебной дисциплины

В результате освоения дисциплины обучающийся должен освоить следующие **компетенции:**

ПК 3.1. Разрешать проблемы совместимости программного обеспечения отраслевой направленности.

ПК 3.3. Проводить обслуживание, тестовые проверки, настройку программного обеспечения отраслевой направленности.

В результате изучения дисциплины студент должен:

знать:

З1 принципы информационной безопасности;
З2 основные угрозы информационной безопасности;
З3 методы и критерии оценки эффективности мероприятий по защите информации

уметь:

У1 различать правовые, организационные и технические мероприятия по защите информации;
У2 выявлять и классифицировать угрозы информационной безопасности предприятия;
У3 планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия;
У4 рассчитывать эффективность мероприятий по защите информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов 2г10м*	*Объем часов 3г10м*
Максимальная учебная нагрузка (всего)	**46**	**46**
Обязательная аудиторная учебная нагрузка (всего)	**26**	**26**
В том числе:		
теоретическое обучение	13	13
практические занятия	13	13
Самостоятельная работа обучающегося (всего)	**20**	**20**
В том числе:		
работа по темам	20	20
подготовка докладов по темам	-	-
Итоговые аттестации	**Зачет 5 семестр**	**Зачет 7 семестр**

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала	Объем часов 2г10м/3г10м	Теоретические занятия	Практические занятия	Самостоятельная работа студента	Уровень освоения	Коды формируемых компетенций
Тема 1. Основные положения теории информационной безопасности	**Содержание учебного материала** **Лекционные занятия** Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. **Практические занятия** Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.	11	3	3	5	1	ПК 3.1. ПК 3.3.
Тема 2.	**Содержание учебного материала**	11	3	3	5	2	ПК

Технические средства и методы защиты информации	**Лекционные занятия** Инженерная защита объектов. Защита информации от утечки по техническим каналам. **Практические занятия** Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.Использование средств стеганографии для защиты файлов. **Самостоятельная работа** изучение теоретического материала, составление опорного конспекта по теме «Создание защищенного канала связи средствами виртуальной частной сети»						3.1. ПК 3.3.
Тема 3. Программно-аппаратные средства и методы обеспечения информационной безопасности	**Содержание учебного материала** **Лекционные занятия** Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз **Практические занятия** Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. **Самостоятельная работа** Изучение настроек средств антивирусной защиты информации.	11	3	3	5	2	ПК 3.1. ПК 3.3.
Тема 4. Криптографические методы защиты информации	**Содержание учебного материала** **Лекционные занятия** Симметричные и ассиметричные системы шифрования. Цифровые подписи. Инфраструктура открытых ключей. Криптографические протоколы. **Практические занятия** Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. **Самостоятельная работа** изучение теоретического материала, составление опорного конспекта по теме «Электронная цифровая подпись»	13	4	4	5	2	ПК 3.1. ПК 3.3.
Всего		46	13	13	20		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – **ознакомительный или минимальный уровень** (узнавание ранее изученных объектов, свойств);

2. – **репродуктивныйили базовый уровень** (выполнение деятельности по образцу, инструкции или под руководством)

3. – продуктивный или высокий уровень **(планирование и самостоятельное выполнение деятельности, решение проблемных задач)**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины предусмотрены оборудованные помещения.

Основное оборудование учебной аудитории для лекционных занятий:

- рабочие места обучающихся;
- рабочее место преподавателя;
- маркерная (или меловая) доска.
- мультимедийное оборудование.

Программное обеспечение:
- ОС MicrosoftWindows;
- Пакет приложений MicrosoftOffice (Open Office, Libre Office).

Основное оборудование учебной аудитории для практических (лабораторных) занятий:
- рабочие места обучающихся;
- автоматизированные рабочие места обучающихся;
- рабочее место преподавателя;
- маркерная (или меловая) доска.
- мультимедийное оборудование.

Программное обеспечение:
- ОС Microsoft Windows;
- Пакет приложений Microsoft Office (Open Office, Libre Office).
- Microsoft Visual Studio;
- СУБД: SQLServer, MySQL, PostgreSQL;
- Notepad++;
- Git;
- MicrosoftVisio(DIA).

3.2. Информационное обеспечение реализации программы

Основная литература

1. Ковалев, Д.В. Информационная безопасность / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL:http://biblioclub.ru/index.php?page=book&id=493175

2. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

3. Основы национальной безопасности / Н.Д. Эриашвили, Е.Н. Хазов, Л.Т. Чихладзе и др. ; под ред. Е.Н. Хазова, Н.Д. Эриашвили. – Москва : Юнити-Дана, 2018. – 335 с. – Режим доступа: по подписке. – URL:http://biblioclub.ru/index.php?page=book&id=473285

4. Петров, С. В. Информационная безопасность [Электронный ресурс] : учебное пособие / С. В. Петров, П. А. Кисляков. — Электрон. текстовые данные. — Саратов : Ай Пи Ар Букс, 2015. — 326 c. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

5. Суворова, Г. М. Информационная безопасность [Электронный ресурс] : учебное пособие / Г. М. Суворова. — Электрон. текстовые данные. — Саратов : Вузовское образование, 2019. — 214 c. — 978-5-4487-0585-4. — Режим доступа: http://www.iprbookshop.ru/86938.html

Дополнительная литература

6. Информационная безопасность [Электронный ресурс] : лабораторный практикум / сост. Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Электрон. текстовые данные. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — 978-5-85219-007-9. — Режим доступа: http://www.iprbookshop.ru/86357.html

7. Шилов, А.К. Управление информационной безопасностью / А.К. Шилов ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный

университет», Институт компьютерных технологий иинформационной безопасности. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=500065

8. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499170

9. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа,2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557

10. Горюхина, Е. Ю. Информационная безопасность [Электронный ресурс] : учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. — Электрон. текстовые данные. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72672.html

Ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины (модуля)

№ п/п	Интернет ресурс (адрес)	Описание ресурса
1.	http://citforum.ru/	IT-портал «Сервер Информационных Технологий»;
2.	https://habrahabr.ru/	ресурс для IT-специалистов
3.	http://stackoverflow.com/	сайт вопросов и ответов для IT-специалистов;
4.	http://Standartgost.ru	Открытая база ГОСТов
5.	https://www.sql-ex.ru/	Веб тренажер языка SQL.
6.	http://citforum.ru/	Учебники и статьи по базам данным.
7.	http://www.firststeps.ru	Первые шаги – Сайт, посвященный начинающим программистам. Учебники и инструкции для по языкам программирования, алгоритмам и используемым протоколам. Вопросы безопасности.
8.	http://www.proklondike.com	Programmer'sKlondike - Бесплатная электронная библиотека. Книги по алгоритмам и дискретной математике. Учебники и статьи.
9.	http://www.intuit.ru	Интернет-университет информационных технологий (ИНТУИТ)
10.	https://msdn.microsoft.com/ru-ru/	MSDN – сеть разработчиков Microsoft
11.	https://mva.microsoft.com/	Виртуальная академия Microsoft

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙДИСЦИПЛИНЫ

Результаты обучения, подлежащие проверке	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины:	«Отлично» - теоретическое содержание курса освоено	Письменный и устный опросы

З1 принципы информационной безопасности; З2 основные угрозы информационной безопасности; З3 методы и критерии оценки эффективности мероприятий по защите информации *Перечень умений, осваиваемых в рамках дисциплины:* У1 различать правовые, организационные и технические мероприятия по защите информации; У2 выявлять и классифицировать угрозы информационной безопасности предприятия; У3 планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; У4 рассчитывать эффективность мероприятий по защите информации.	полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Тестирование Оценка выполнения практического задания
В результате освоения дисциплины обучающийся должен освоить следующие **компетенции:** ПК 3.1. Разрешать проблемы совместимости программного обеспечения отраслевой направленности. ПК 3.3. Проводить обслуживание, тестовые проверки, настройку программного обеспечения отраслевой направленности.		

Описание показателей и критериев оценивания компетенций

Показатели оценивания	Критерии оценивания компетенций	Шкала оценивания
Понимание смысла компетенции	Имеет базовые общие знания в рамках диапазона выделенных задач (1 балл) Понимает факты, принципы, процессы, общие понятия в пределах области исследования. В большинстве случаев способен выявить достоверные источники информации, обработать, анализировать информацию. (2 балла) Имеет фактические и теоретические знания в пределах области исследования с пониманием границ применимости (3 балла)	Минимальный уровень Базовый уровень Высокий уровень

Освоение компетенции в рамках изучения учебной дисциплины	Наличие основных умений, требуемых для выполнения простых задач. Способен применять только типичные, наиболее часто встречающиеся приемы по конкретной сформулированной (выделенной) задаче (1 балл) Имеет диапазон практических умений, требуемых для решения определенных проблем в области исследования. В большинстве случаев способен выявить достоверные источники информации, обработать, анализировать информацию. (2 балла) Имеет широкий диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем. Способен выявлять проблемы и умеет находить способы решения, применяя современные методы и технологии. (3 балла)	Минимальный уровень Базовый уровень Высокий уровень
Способность применять на практике знания, полученные в ходе изучения дисциплины	Способен работать при прямом наблюдении. Способен применять теоретические знания к решению конкретных задач. (1 балл) Может взять на себя ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. Затрудняется в решении сложных, неординарных проблем, не выделяет типичных ошибок и возможных сложностей при решении той или иной проблемы (2 балла) Способен контролировать работу, проводить оценку, совершенствовать действия работы. Умеет выбрать эффективный прием решения задач по возникающим проблемам. (3 балла)	Минимальный уровень Базовый уровень Высокий уровень

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по выполнению лекционных занятий

Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

Методические указания по выполнению практических занятий

Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом (указать текст из источника и др.). Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.

Методические указания по выполнению лабораторных работ/индивидуальных заданий

Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме. Составление

аннотаций к прочитанным литературным источникам и др.

Методические указания по подготовке к экзамену.

Наиболее ответственным этапом в обучении студентов является экзаменационная сессия. На ней студенты отчитываются о выполнении учебной программы, об уровне и объеме полученных знаний. Это государственная отчетность студентов за период обучения, за изучение учебной дисциплины.

Залогом успешного прохождения контроля являются систематические, добросовестные занятия студента. Однако это не исключает необходимости специальной работы перед сессией и в период сдачи зачета. Специфической задачей студента в период экзаменационной сессии являются повторение, обобщение и систематизация всего материала.

В процессе повторения анализируются и систематизируются все знания, накопленные при изучении программного материала: данные учебника, записи лекций, конспекты прочитанных книг, заметки, сделанные во время консультаций или семинаров, и др.

Консультации, которые проводятся для студентов в период экзаменационной сессии, необходимо использовать для углубления знаний, для восполнения пробелов и для разрешения всех возникших трудностей.

При подготовке к контролю необходимо еще раз проверить себя на предмет усвоения основных категорий и ключевых понятий курса.

6. ОЦЕНОЧНЫЕ СРЕДСТВА И КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

6.1. Оценочные средства для проведения текущего контроля по учебной дисциплине

Тема 1. Основные положения теории информационной безопасности (ПК 3.1., ПК 3.3.)

Вопросы к обсуждению:

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Какие основные законы в области защиты информации в РФ?
6. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
7. Что такое концепция информационной безопасности?
8. Что такое конфиденциальная информация?
9. Что такое персональные данные?
10. В каких случаях возможно использовать персональные данные без согласия обладателя?
11. Какие основные международные стандарты в области информационной безопасности существуют?
12. Что такое "Единые критерии"
13. Как связаны международные стандарты и стандарты РФ?

Практические занятия:

1. Основные стандарты в области обеспечения информационной безопасности.
2. Политика безопасности. Экономическая безопасность предприятия.

Тема 2. Технические средства и методы защиты информации (ПК 3.1., ПК 3.3.)

Вопросы к обсуждению:

1. Что такое инженерная защита объектов?
2. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?

3. Что такое технические каналы утечки информации?
4. Перечислите основные виды технических каналов утечки информации?
5. Перечислите методы защиты информации от утечки по визуальному каналу.
6. Перечислите методы защиты информации от утечки по воздушному каналу.
7. Перечислите методы защиты информации от утечки по вибрационному каналу.
8. Перечислите методы защиты информации от утечки по индукционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Практические занятия:

1. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.
2. Использование средств стеганографии для защиты файлов.

*Самостоятельная работа*изучение теоретического материала, составление опорного конспекта по теме «Создание защищенного канала связи средствами виртуальной частной сети»

Тема 3. Программно-аппаратные средства и методы обеспечения информационной безопасности (ПК 3.1., ПК 3.3.)

Вопросы к обсуждению:

1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?

Практические занятия: Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.

Самостоятельная работа: Изучение настроек средств антивирусной защиты информации

Тема 4. Криптографические методы защиты информации (ПК 3.1., ПК 3.3.)

Вопросы к обсуждению:

1. Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?
4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?
9. Какие основные криптографические протоколы используются в сетях?

Практические занятия: Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

Самостоятельная работа: изучение теоретического материала, составление опорного конспекта по теме «Электронная цифровая подпись»

Тематика контрольных работ:

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации.
9. Атаки на систему безопасности и современные методы защиты

6.2. Контрольно-измерительные материалы для проведения текущего контроля по учебной дисциплине

Шкала оценки для проведения текущего контроля по учебной дисциплине в устной форме

№ п/п	Оценка за ответ	Характеристика ответа
1	Отлично	- полно раскрыто содержание материала; - материал изложен грамотно, в определенной логической последовательности; - точно используется терминология; - показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; - продемонстрированные знания и умения позволяют самостоятельно решать поставленные задачи; - ответ прозвучал самостоятельно, без наводящих вопросов; - продемонстрирована способность творчески применять знание теории к решению профессиональных задач; - допущены одна - две неточности при освещении второстепенных вопросов, которые исправляются по замечанию. - количество баллов за освоение компетенций от 8 до 9
2	Хорошо	- вопросы излагаются систематизировано и последовательно; - продемонстрированные знания и умения позволяют самостоятельно решать поставленные задачи, однако требуют определенного контроля; - продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; - ответ удовлетворяет в основном требованиям на оценку «отлично», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие содержание ответа; приобретенный практический опыт, знания и умения требуют не значительной корректировки в процессе выполнения задания; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя. - количество баллов за освоение компетенций от 5 до 7
3	Удовлетво-рительно	- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и проде-

		монстрированы умения, достаточные для дальнейшего усвоения материала; - при неполном знании теоретического материала выявлен недостаточный уровень знаний и умений; студент не может применить теоретические знания на практике; - количество баллов за освоение компетенций от 3 до 4
4	Неудовлетво-рительно	- не раскрыто основное содержание учебного материала; - обнаружено незнание или непонимание большей или наиболее важной части учебного материала; - допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов - отсутствуют практический опыт, знания и умения по предлагаемым ситуационным вопросам или задачам, количество баллов за освоение компетенций менее 3. - отказ от ответа или отсутствие ответа

Шкала оценки для проведения текущего контроля по учебной дисциплине в письменной форме

№ п/п	Оценка за ответ	Характеристика ответа
1	Отлично	Материал раскрыт полностью, изложен логично, без существенных ошибок, выводы доказательны и опираются на теоретические знания Количество баллов за освоение материала от 8 до 9
2	Хорошо	Основные положения раскрыты, но в изложении имеются незначительные ошибки выводы доказательны, но содержат отдельные неточности Количество баллов за освоение материала от 5 до 7
3	Удовлетво-рительно	Изложение материала не систематизированное, выводы недостаточно доказательны, аргументация слабая. Количество баллов за освоение материала от 3 до 4
4	Неудовлетво-рительно	Не раскрыто основное содержание материала, обнаружено не знание основных положений темы. Не сформированы компетенции, умения и навыки. Количество баллов за освоение компетенций менее 3 Ответ на вопрос отсутствует

7. ОЦЕНОЧНЫЕ СРЕДСТВА И КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

7.1. Оценочные средства для проведения промежуточной аттестации по учебной дисциплине

Контрольные вопросы для подготовки к контролю при проведении промежуточной аттестации по учебной дисциплине:

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.

8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Итоговый тест

Вопрос	Контро-лируемые компе-тенции
1. Основная масса угроз информационной безопасности приходится на: а) Троянские программы б) Шпионские программы в) Черви	ПК 3.1., ПК 3.3.
2. Какой вид идентификации и аутентификации получил наибольшее распространение: а) системы PKI б) постоянные пароли в) одноразовые пароли	ПК 3.1., ПК 3.3.
3. Под какие системы распространение вирусов происходит наиболее динамично: а) Windows б) Mac OS в) Android	ПК 3.1., ПК 3.3.
4. Заключительным этапом построения системы защиты является: а) сопровождение б) планирование в) анализ уязвимых мест	ПК 3.1., ПК 3.3.
5. Какие угрозы безопасности информации являются преднамеренными: а) ошибки персонала б) открытие электронного письма, содержащего вирус в) не авторизованный доступ	ПК 3.1., ПК 3.3.
6. Какой подход к обеспечению безопасности имеет место: а) теоретический	ПК 3.1., ПК 3.3.

б) комплексный в) логический	
7. Системой криптографической защиты информации является: а) BFox Pro б) CAudit Pro в) Крипто Про	ПК 3.1., ПК 3.3.
8. Какие вирусы активизируются в самом начале работы с операционной системой: а) загрузочные вирусы б) троянцы в) черви	ПК 3.1., ПК 3.3.
9. Stuxnet – это: а) троянская программа б) макровирус в) промышленный вирус	ПК 3.1., ПК 3.3.
10. Таргетированная атака – это: а) атака на сетевое оборудование б) атака на компьютерную систему крупного предприятия в) атака на конкретный компьютер пользователя	ПК 3.1., ПК 3.3.
11. Процедурой называется: а) пошаговая инструкция по выполнению задачи б) обязательные действия в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах	ПК 3.1., ПК 3.3.
12. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании: а) проведение тренингов по безопасности для всех сотрудников б) поддержка высшего руководства в) эффективные защитные меры и методы их внедрения	ПК 3.1., ПК 3.3.
13. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков: а) когда риски не могут быть приняты во внимание по политическим соображениям б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски в) когда стоимость контрмер превышает ценность актива и потенциальные потери	ПК 3.1., ПК 3.3.
14. Что такое политика безопасности: а) детализированные документы по обработке инцидентов безопасности б) широкие, высокоуровневые заявления руководства в) общие руководящие требования по достижению определенного уровня безопасности	ПК 3.1., ПК 3.3.
15. Какая из приведенных техник является самой важной при выборе конкретных защитных мер: а) анализ рисков б) результаты ALE в) анализ затрат / выгоды	ПК 3.1., ПК 3.3.
16. Что лучше всего описывает цель расчета ALE: а) количественно оценить уровень безопасности среды б) оценить потенциальные потери от угрозы в год в) количественно оценить уровень безопасности среды	ПК 3.1., ПК 3.3.

7.2. Контрольно-измерительные материалы для проведения промежуточной аттестации по учебной дисциплине

Шкала оценки для проведения промежуточной аттестации по учебной дисциплине в устной форме

№ п/п	Оценка за ответ	Характеристика ответа
1	Отлично	- полно раскрыто содержание материала; - материал изложен грамотно, в определенной логической последовательности; - точно используется терминология; - показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; - продемонстрированные знания и умения позволяют самостоятельно решать поставленные задачи; - ответ прозвучал самостоятельно, без наводящих вопросов; - продемонстрирована способность творчески применять знание теории к решению профессиональных задач; - допущены одна - две неточности при освещении второстепенных вопросов, которые исправляются по замечанию. - количество баллов за освоение компетенций от 8 до 9
2	Хорошо	- вопросы излагаются систематизировано и последовательно; - продемонстрированные знания и умения позволяют самостоятельно решать поставленные задачи, однако требуют определенного контроля; - продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; - ответ удовлетворяет в основном требованиям на оценку «отлично», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие содержание ответа; приобретенный практический опыт, знания и умения требуют не значительной корректировки в процессе выполнения задания; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя. - количество баллов за освоение компетенций от 5 до 7
3	Удовлетворительно	- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; - при неполном знании теоретического материала выявлен недостаточный уровень знаний и умений; студент не может применить теоретические знания на практике; - количество баллов за освоение компетенций от 3 до 4

4	Неудовлетво-рительно	- не раскрыто основное содержание учебного материала; - обнаружено незнание или непонимание большей или наиболее важной части учебного материала; - допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов - отсутствуют практический опыт, знания и умения по предлагаемым ситуационным вопросам или задачам, количество баллов за освоение компетенций менее 3. - отказ от ответа или отсутствие ответа

Шкала оценки для проведения промежуточной аттестации по учебной дисциплине в письменной форме

№ п/п	Оценка за ответ	Характеристика ответа
1	Отлично	Материал раскрыт полностью, изложен логично, без существенных ошибок, выводы доказательны и опираются на теоретические знания Количество баллов за освоение материала от 8 до 9
2	Хорошо	Основные положения раскрыты, но в изложении имеются незначительные ошибки выводы доказательны, но содержат отдельные неточности Количество баллов за освоение материала от 5 до 7
3	Удовлетвори-тельно	Изложение материала не систематизированное, выводы недостаточно доказательны, аргументация слабая. Количество баллов за освоение материала от 3 до 4
4	Неудовлетво-рительно	Не раскрыто основное содержание материала, обнаружено незнание основных положений темы. Не сформированы компетенции, умения и навыки. Количество баллов за освоение компетенций менее 3 Ответ на вопрос отсутствует

Критерии формирования оценок по тестам

Оценка	Требования к знаниям
отлично	80%-100%
хорошо	65-80%
удовлетворительно	50-65%
неудовлетворительно	менее 50%
зачтено	50% и более
не зачтено	менее 50%

8. ПРОВЕРКА СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

ПК 3.1., ПК 3.3.

Вариант 1

Задание 1. Настройте политику учетных записей на компьютере и убедитесь, что: данные параметры вступили в силу.

1. С помощью оснастки Group Policy (Групповая политика) задайте параметры политики учетных записей:

о пользователь должен сменить минимум пять паролей, прежде чем повторно применить старый;
о после обновления пароля пользователь может его снова сменить не ранее, чем через 24 часа;
о пользователь должен менять пароль каждые три недели.
Какие параметры вам понадобились, чтобы выполнить требования этого списка?
2. Закройте оснастку Group Policy.
3: убедитесь, что новые параметры политики учетных записей работают

Задание 2. Настройте и проверьте параметры безопасности:

1. Войдите в систему по учетной записи Administrator (Администратор).

2. Раскройте меню Пуск\Программы\Администрирование и щелкните Group Policy (Групповая политика).

3. В дереве консоли Group Policy по мере необходимости, последовательно раскройте узлы Local Computer Policy\Computer Configuration\Windows Settings\Security Settings (Локальная политика безопасности\ Параметры компьютера\ Параметры Windows\ параметры безопасности),а затем – Account Policies (Политики учетных записей).

4. Настройте политику безопасности на компьютере так, чтобы пользователи:

- должны были входить в систему, чтобы иметь возможность выключить компьютер;
- должны были нажимать Ctrl+Alt+Delete для входа в систему;
- не смогли увидеть в окне Windows Security имя последнего пользователя.

5. Выйдите из системы.

6. Обратите внимание, что теперь для регистрации нужно нажать Ctrl+Alt+Delete.

7. Нажмите Ctrl+Alt+Delete.

8. В диалоговом окне Log On To Windows (Вход в Windows) поле User Name (Пользователь) пустое и кнопка Shutdown (Выключить) неактивна. Если вы не видите кнопку Shutdown, щелкните Options (Параметры).

Вариант 2

Задание 1. Настройте параметры политики блокировки учетных записей и убедитесь, что изменения вступили в силу.

1. Войдите в систему под учетной записью Administrator (Администратор).

2. Раскройте меню Пуск\Программы\Администрирование, а затем щелкните Group Policy (Групповая политика).

3. В дереве консоли Group Policy последовательно раскройте узлы: (Локальная политика безопасности), (Управление компьютером), Windows Settings (Параметры Windows), Security Settings (Параметры безопасности), а затем Policies (Политики учетных записей).

4. Щелкните Account Lockout Policy (Политика блокировки учетных записей).

5. Настройте параметры Account Lockout Policy так, чтобы: учетная запись пользователя блокировалась после четырех неудачных попыток войти в систему;

6. разблокировать учетную запись мог только администратор.

7. Выйдите из системы.

Задание 2. Настройте минимальную длину пароля, а затем поэкспериментируйте с длиной пароля, чтобы убедиться, что выбранные параметры вступили в силу.

Задача 1: настройка минимальной длины пароля

1. Войдите в систему под учетной записью Administrator (Администратор)

2. В консоли MMC создайте дополнительную консоль с оснасткой Group Policy (Групповая политика).

3. Открыв консоль Group Policy, последовательно щелкните узлы: (Локальная

политика безопасности), (Параметры компьютера), Windows Settings (ПараметрыWindows), Security Settings (Параметры безопасности) и (Политики учетных записей).

4. В дереве консоли щелкните Password Policy (Политика паролей).

5. В правой панели щелкните правой кнопкой мыши Minimum Password Length (Минимальная длина пароля) и выберите в контекстном меню Security (Безопасность).

6. В поле Characters (Длина пароля) введите 6 и щелкните ОК.

7. Закройте окно Local Security Settings (Параметры локальной безопасности).

Задача 2: проверьте, изменилась ли минимальная длина пароля

1. Нажмите Ctrl+Alt+Delete, а затем в диалоговом окне Windows Security (Безопасность Windows) щелкните Change Password (Изменить пароль).

2. В поле Old Password (Старый пароль) введите password, а в поля New Password (Новый пароль) и Confirm Password (Подтверждение) введите water.

Информационное окно Change Password (Изменение пароля) сообщит, что новый пароль должен содержать не менее шести символов. Таким образом, параметр Minimum Password Length настроен верно.

ПК 3.1., ПК 3.3.

Вариант 1

Задание 1. Вы руководитель фирмы Вам необходимо организовать конфиденциальное делопроизводство. Опишите процесс организации.

Задание 2. Необходимо провести анализ и составить отчет защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель политики безопасности в компьютерной системе?

Вариант 2

Задание 1. Вы руководитель фирмы и Вам необходимо организовать технологическую систему обработки конфиденциальных документов. Опишите процесс организации.

Задание 2. Необходимо провести анализ и составить отчет защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы

1. Что такое информационный риск?
2. В чем заключается задача управления информационными рисками?
3. Какие существуют методики оценки рисков и управления ими?
4. Какие формулы используются при количественной оценке информационных рисков?

ЛИСТ СОГЛАСОВАНИЯ

№п/п	Подразделение	Фамилия	Подпись	Дата
1	Кафедра ГЕиМД	И.О. Тимофеева		10.06.2020
2	Учеб.-метод. отдел	М.О. Дерябичева		10.06.2020
3	Библиотека	Г.В. Шпакова		10.06.2020