МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Тобольский педагогический институт им. Д.И. Менделеева (филиал)
Тюменского государственного университета

УТВЕРЖДАЮ
Директор
_____ Шилов С.П
«28» мая 2020 г.

ОП.15 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
рабочая программа дисциплины для обучающихся по программе подготовки
специалистов среднего звена
09.02.05 Прикладная информатика (по отраслям)
(базовая подготовка)
Форма обучения – очная

Маковийчук Л.Ф. ОП.15 Методы и средства защиты информации. Рабочая программа дисциплины для обучающихся по программе подготовки специалистов среднего звена 09.02.05 Прикладная информатика (по отраслям). Форма обучения – очная. Тобольск, 2020.

Рабочая программа дисциплины разработана на основе ФГОС СПО по специальности 09.02.05 Прикладная информатика (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 13 августа 2014 года, № 1001.

Рабочая программа учебной дисциплины опубликована на сайте Тобольского пединститута им. Д.И. Менделеева (филиал) ТюмГУ: Методы и средства защиты информации. [электронный ресурс] / Режим доступа: https://tobolsk.utmn.ru/sveden/education/#

Содержание

Y

1. Паспорт рабочей программы учебной дисциплины

1.1. Область применения программы

Рабочая программа дисциплины – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.05 Прикладная информатика (по отраслям).

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Дисциплина Методы и средства защиты информации входит в профессиональный учебный цикл.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен **уметь**:

– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

– применять основные правила и документы системы сертификации Российской Федерации;

– классифицировать основные угрозы безопасности информации.

в результате освоения дисциплины обучающийся должен **знать**:

– сущность и понятие информационной безопасности, характеристику ее составляющих;

– место информационной безопасности в системе национальной безопасности страны;

– современные средства и способы обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК.3.4. Работать с системами управления взаимоотношениями с клиентами.

1.4. Количество часов на освоение дисциплины:

Семестр(ы) 8;

Максимальной учебной нагрузки обучающегося 90 часов, в том числе:

обязательной аудиторной нагрузки обучающегося 70 часа;

самостоятельной работы обучающегося 10 часов.

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	90
Обязательная аудиторная учебная нагрузка (всего)	70
в том числе:	
лабораторные занятия	40
практические занятия	-
Самостоятельная работа обучающегося (всего)	10
Форма промежуточной аттестации по дисциплине – Экзамен	

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	**2**	**3**	**4**
Раздел 1. Информационная безопасность		**4**	
Тема 1.1 Понятие национальной безопасности. Государственная информационная политика	**Содержание учебного материала**	2	1
	Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание Информационные права граждан. Соперничество в информационной сфере, информационные войны. Информационная безопасность как институт информационного права. Основные задачи и уровни реализации информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности РФ. Первоочередные мероприятия по реализации государственной политики обеспечения ИБ РФ.		
	Самостоятельная работа обучающихся:	2	3
	Подготовка доклада на одну из тем: • Понятие национальной безопасности; • Информационная безопасность в системе национальной безопасности России; • Государственная информационная политика		
Раздел 2. Сущность и понятие защиты информации		**20**	
Тема 2.1 Сущность и понятие информационной безопасности. Классификация информационных ресурсов	**Содержание учебного материала**	2	1
	Понятие информационной безопасности. Характеристика составляющих информационной безопасности. Источники и содержание угроз в информационной сфере. Состояние информационной безопасности России и основные задачи по ее обеспечению. Принципы обеспечения информационной безопасности. Общеметодологические принципы обеспечения информационной безопасности. Концептуальная модель информационной безопасности Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов.		

	Информационно- правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы.		
	Самостоятельная работа обучающихся	1	3
	Анализ документов образовательного учреждения		
Тема 2.2 Виды и особенности угроз информационной безопасности	**Содержание учебного материала**	2	1
	Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки. Понятие и методы аналитической работы. Легальные способы получения ценной и конфиденциальной информации, их состав. Нелегальные (противоправные, незаконные) способы получения ценной и конфиденциальной информации, их состав. Понятия злоумышленника, постороннего и случайного лица. Понятие и классификация источников конфиденциальной информации.		
	Лабораторные работы	2	2
	Анализ источников, каналов распространения и каналов утечки информации		
Тема 2.3 Методы нарушения конфиденциальности, целостности и доступности информации	**Содержание учебного материала**	2	1
	Классы каналов несанкционированного получения информации: непосредственно с объекта, с каналов отображения информации, получение по внешним каналам, подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные. Функции защиты информации. Стратегии защиты информации: оборонительная стратегия, наступательная стратегия, упреждающая стратегия.		
	Лабораторные работы	2	2
	Проведение анализа информации на предмет целостности		
	Самостоятельная работа обучающихся:	1	3
	Составление последовательности действий по защите информации		
Тема 2.4 Методы и модели оценки уязвимости информации	**Содержание учебного материала**	2	1
	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Система с полным перекрытием. Практическая реализация модели «угроза-защита».		

	Лабораторные работы	2	2
	Оценка уязвимости информации		
	Самостоятельная работа обучающихся: Подготовка доклада на одну из тем: • Сущность и понятие информационной безопасности; Классификация информационных ресурсов; • Виды и особенности угроз информационной безопасности; • Методы нарушения конфиденциальности, целостности и доступности информации.	1	3
Раздел 3. Основы защиты информации		**16**	
Тема 3.1 Основы защиты информации**.** Функции и задачи защиты информации	**Содержание учебного материала**	2	1
	Информация, сообщения, информационные процессы как объекты информационной безопасности. Цели и задачи защиты информации. Классификационная схема понятий в области защиты информации. Концептуальные основы защиты информации. Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояние и функции защиты информации.		
	Самостоятельная работа обучающихся:	1	3
	Подготовить сообщение: Основы защиты информации в РФ; Анализ функций и задач защиты информации		
Тема 3.2 Анализ существующих методик определения требований защиты информации	**Содержание учебного материала**	2	1
	Требования к безопасности информационных систем в США. Классы защищенности средств вычислительной техники от несанкционированного доступа. Оценка состояния безопасности ИС Франции. Факторы, влияющие на требуемый уровень защиты информации. Критерии оценки безопасности		
	Лабораторные работы		2
	Требования к безопасности информационных систем.	2	
	Требования к безопасности информационных систем в России.	2	
	Оценка состояния безопасности ИС США.	2	
	Определение классов защищенности средств вычислительной техники от несанкционированного доступа.	2	

	Определение требований к защите информации	2	
Раздел 4. Правовое обеспечение информационной безопасности		**16**	
Тема 4.1 Концепция правового обеспечения информационной безопасности Российской Федерации	**Содержание учебного материала**	2	1
	Законодательная база, стандарты и нормативно-методические документы РФ в области обеспечения информационной безопасности. Ответственность за нарушение законодательства в информационной сфере. ГОСТы по информационной безопасности		
	Лабораторные работы		2
	Анализ терминов и определений информационной безопасности	2	
	Работа с ГОСТами в области информационной безопасности	4	
Тема 4.2 Зарубежные стандарты и международные соглашения в области информационной безопасности	**Содержание учебного материала**	2	1
	Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью.		
	Самостоятельная работа обучающихся: Сравнительный анализ международных стандартов и стандартов РФ	1	3
Тема 4.3 Правовое регулирование информационных ресурсов	**Содержание учебного материала**	2	1
	Защита информации институтом интеллектуальной собственности. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Объекты интеллектуальной собственности. Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Распоряжение сведениями, составляющими государственную тайну. Рассекречивание сведений и их носителей. Защита государственной тайны.		
	Самостоятельная работа обучающихся:	1	3
	составление глоссария «Термины и определения информационной безопасности»		

Раздел. 5. Организационные основы защиты информации		**10**	
Тема 5.1 Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	**Содержание учебного материала**	2	1
	Понятие, цели и задачи системы защиты конфиденциальной информации. Принципы построения системы, ее технологичность, иерархичность и факторы эффективности. Компьютерные технологии и формирование основ системы защиты информации. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала с документами, вычислительной и организационной техникой, средствами связи. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций		
Тема 5.2 Защита информации при проведении совещаний и переговоров по конфиденциальным вопросам, приеме посетителей. Защищенный документооборот	**Содержание учебного материала**	2	1
	Угрозы безопасности информации и задачи ее защиты в процессе проведения совещаний и переговоров, приеме посетителей. Документирование информации, оформление стенограмм, протоколов и итоговых документов. Порядок использования аудио- и видеозаписи. Инженерно-технические требования к помещениям, их охране. Порядок лицензирования помещений. Понятие и задачи защищённого документооборота Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков. Понятие, принципы, цели и задачи защищенного документооборота как совокупности документопотоков. Типовая структура технологических стадий входного, выходного и внутреннего потоков конфиденциальных документов. Учет носителей конфиденциальной информации. Особенности конвертования (пакетирования) отправляемых конфиденциальных документов, доставки их адресатам. Особенности направления на исполнение изданных внутренних документов. Особенности передачи адресатам по незащищенным линиям связи факсимильных, электронных документов, телеграмм, телексов. Порядок работы с шифрованной перепиской. Учет документов, находящихся		

	у исполнителя. Порядок работы исполнителей со средствами вычислительной и организационной техники, средствами связи.		
	Лабораторные работы		2
	Составление инструкции по обработке и хранению конфиденциальных документов	2	
	Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации	2	
	Оценка безопасности информации на объектах ее обработки	2	
Раздел 6. Обеспечение безопасности автоматизированных систем.	Основные подходы к созданию защиты АИС. Идентификация и аутентификация. Разграничение доступа. Контроль целостности. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Обнаружение и противодействие атакам.	**20**	
Тема 6.1 Методы защиты информации в АИС	**Содержание учебного материала**	2	1
	Организационные, правовые, технические, программно-математические методы и их соотношение.		
	Самостоятельная работа обучающихся: Анализ основных методов защиты информации: преимущества и недостатки	1	3
Тема 6.2 Основные принципы защиты информации от несанкционированного доступа	**Содержание учебного материала**	2	1
	Источники и пути реализации несанкционированного доступа к информации в АИС. Основные принципы защиты информации от несанкционированного доступа. Средства и механизмы защиты от несанкционированного доступа.		
Тема 6.4 Управление доступом в АИС	**Содержание учебного материала**	2	1
	Правила разграничения доступа к элементам защищаемой информации. Разграничение доступа по уровням секретности, специальным спискам, матрицам полномочий, мандатам. Принципы организации разноуровневого доступа в АИС. Понятия клиента, прав доступа, объекта доступа. Учетные записи пользователей АИС. Понятие группы и роли.		
	Лабораторные работы		
	Классификация автоматизированных систем обработки	2	2
	информации по классу защиты информации	2	
	Планирование, создание и изменение учетных записей пользователей.	2	

	Создание и администрирование групп пользователей.	2	
	Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам. Наследование разрешений в NTFS. Изменение параметров учетных записей пользователей. Настройка политики учетных записей. Настройка параметров безопасности операционных систем. Настройка параметров безопасности Windows. Настройка параметров безопасности Интернет.	4	
	Самостоятельная работа обучающихся: выполнение домашнего задания выучить основные понятия и определения.	1	3
	Консультации	**10**	
	Всего	**90**	

Примечание - для характеристики уровня освоения учебного материала используются следующие обозначения:
1. - Ознакомительный (узнавание ранее изученных объектов, свойств);
2. - Репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. - Продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. Условия реализации дисциплины

3.1. Требования к минимальному материально-техническому обеспечению

Реализация дисциплины требует наличия лаборатории обработки информации отраслевой направленности оснащенную следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и мультимедийное аудиовизуальное оборудование, планшетные компьютеры.
На ПК установлено следующее программное обеспечение:
— Офисное ПО: операционная система iOS.
— Специализированное ПО: Adobe Photoshop Extended CS5, Adobe Design Premium CS4, MathCAD 14.0, ИКАР Notebook, GIMP, Inkscape.
Обеспечено беспроводное подключение планшетных компьютеров к локальной сети и сети Интернет.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий: основной и дополнительной литературы, интернет-ресурсов.

Основная литература:

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1087948 (дата обращения: 12.04.2020). – Режим доступа: по подписке.

Дополнительная литература:

1. Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-466-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1058219 (дата обращения: 12.04.2020). – Режим доступа: по подписке.
2. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты информации: учебник / В.П. Зверева, А.В. Назаров. — Москва : КУРС: ИНФРА-М, 2017. — 320 с. - ISBN 978-5-906818-92-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/635130 (дата обращения: 12.04.2020). – Режим доступа: по подписке.

Интернет-ресурсы:

1. Знаниум - https://new.znanium.com/
2. Лань - https://e.lanbook.com/
3. IPR Books - http://www.iprbookshop.ru/
4. Elibrary - https://www.elibrary.ru/
5. Национальная электронная библиотека (НЭБ) - https://rusneb.ru/
6. Межвузовская электронная библиотека (МЭБ) - https://icdlib.nspu.ru/
7. "ИВИС" (БД периодических изданий) - https://dlib.eastview.com/browse
8. Электронная библиотека Тюмгу - https://library.utmn.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: Платформа для электронного обучения MicrosoftTeams.

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
• Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; • Применять основные правила и документы системы сертификации Российской федерации; • Классифицировать основные угрозы безопасности информации.	практические занятия, выполнение индивидуальных заданий
Знания	
• Сущность и понятие информационной безопасности, характеристику ее составляющих; • Место информационной безопасности в системе национальной безопасности страны; • Современные средства и способыобеспечения информационной безопасности.	выполнение контрольных заданий, тестов, домашняя работа, практические занятия, экзамен