МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«УДМУРТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФИЛИАЛ ФГБОУ ВО «УДГУ» В Г. ВОТКИНСКЕ
СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

«УТВЕРЖДАЮ»
Зам. директора по УМР
_____Т.М. Смирнова
«20» февраля 2020г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.11 Основы информационной безопасности

09.02.04 «Информационные системы (по отраслям)»
Квалификация выпускника
Техник по информационным системам

Воткинск 2020г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО), 09.02.04 «Информационные системы (по отраслям)», учебного плана.

Организация разработчик:
Филиал ФГБОУ ВО «Удмуртский государственный университет» в г. Воткинске, кафедра Информационных и Инженерных Технологий.

Разработчики:
Раскин П.Н., преподаватель

Рабочая программа утверждена на заседании кафедры Информационных и Инженерных Технологий.
Протокол № 6 от 11.02.2020

Заведующий кафедрой _____ /Мамрыкин О.В./

Программа утверждена на заседании научно-методического совета Филиала ФГБОУ ВО «УдГУ» в г. Воткинске
Протокол № 2 от 18.02.2020г.
Председатель научно-методического совета
……/Смирнова Т.М./

ОГЛАВЛЕНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с федеральным государственным образовательным стандартом по специальности СПО 09.02.04 «Информационные системы (по отраслям)».

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

Учебная дисциплина ОП.11 «Основы информационной безопасности» относится к циклу общепрофессиональных дисциплин программы подготовки специалистов среднего звена.

1.3. Цель и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен уметь:

- выбирать средства обеспечения информационной безопасности информационной системы современного предприятия;
- ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;
- организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;
- организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;
- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;
- проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно-программных решений.

В результате освоения учебной дисциплины обучающийся должен знать:

- вопросы административного и нормативно-правового обеспечения защиты информации;
- основные системы защиты информации в России и в ведущих зарубежных странах;
- основные программно-аппаратные средства и методы защиты информации в компьютерных системах.

1.4. Перечень формируемых компетенций:

В результате освоения учебной дисциплины у обучающегося формируются:

Общие компетенции (ОК):

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

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

Профессиональные компетенции (ПК):

ПК 1.3. Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.

ПК 1.8. Консультировать пользователей информационной системы и разрабатывать фрагменты методики обучения пользователей информационной системы.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.6. Использовать критерии оценки качества и надежности функционирования информационной системы.

1.5. Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины (по ФГОС):

Максимальная учебная нагрузка обучающегося 84 часа, в том числе:
- обязательная аудиторная учебная нагрузка 56 часов,
- самостоятельная работа обучающегося 28 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	84
Обязательная аудиторная учебная нагрузка (всего)	56
в том числе:	
лекции	28
практические занятия	28
контрольные работы	5 сем
Самостоятельная работа обучающегося (всего)	28
в том числе:	
подготовка к аудиторным занятиям (составление таблиц, построение графиков, написание рефератов, эссе и пр. письменных работ)	18
подготовка к промежуточной аттестации	10
Итоговая аттестация в форме *ЭКЗАМЕНА* в 5 семестре	

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практические занятия и лабораторные работы, самостоятельная работа студента		Объем часов	Уровень освоения
1	2		3	4
Введение	**Содержание**		2	
	1.	Введение в проблему информационной безопасности, ее актуальность.		*1*
	2.	Основные объекты информационных систем, подлежащих защите. Цели и задачи обеспечения информационной безопасности для различных объектов (правоохранительные органы, медицинские учреждения, коммерческие организации и др.)		*2*
Раздел 1 Комплексный подход к обеспечению информационной безопасности			**22**	
Тема 1.1 Понятие и составляющие информационной безопасности	**Содержание**		1	
	1.	Основные понятия информационной безопасности.		*2*
	2.	Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.		*2*
	3.	Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический.		*2*
	4.	Требования к комплексным системам защиты информации.		*2*
	Самостоятельная работа		2	
	1.	Проанализировать профессионально – значимые источники информации с точки зрения основных аспектов: конфиденциальности, целостности и доступности.		
Тема 1.2 Угрозы информационной безопасности в компьютерных системах	**Содержание**		2	
	1.	Компьютерная система как объект защиты информации.		*1*
	2.	Понятие угрозы информационной безопасности в компьютерных системах.		*2*
	3.	Классификация и общий анализ угроз информационной безопасности в компьютерных системах.		*2*
	4.	Случайные угрозы информационной безопасности.		*2*
	5.	Преднамеренные угрозы информационной безопасности		*2*
	Самостоятельная работа		4	

	1.	Для выбранного объекта защиты информации (например, почтовый сервер, одиночно стоящий компьютер в бухгалтерии, телефонная база ограниченного пользования на электронных носителях и др.) провести анализ защищенности объекта по следующим пунктам: вид угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия; определить класс защиты информации.		
Тема 1.3 Законодательный уровень информационной безопасности	**Содержание**		2	
	1.	Значимость уровня в комплексном подходе. Меры законодательного уровня.		*2*
	2.	Законодательная и нормативно – правовая база РФ в области информатизации и защиты информации.		*3*
	3.	Ответственность за нарушение законодательства в информационной сфере.		*2*
	4.	Обзор зарубежного законодательства в области информационной безопасности.		*3*
	Практические занятия		4	
	1.	Изучение Доктрины информационной безопасности Российской Федерации.		
	2.	Изучение основных законов в области информационной безопасности.		
	Самостоятельная работа		2	
	1.	Составить перечень основный понятий и определений, используемых в нормативно – правовых документах.		
Тема 1.4 Административный уровень информационной безопасности	**Содержание**		2	
	1.	Основные понятия.		*2*
	2.	Политика безопасности.		*2*
	3.	Программа безопасности.		*2*
	4.	Синхронизация программы безопасности с жизненным циклом систем.		*2*
Тема 1.5 Процедурный уровень информационной безопасности	**Содержание**		2	
	1.	Основные классы мер процедурного уровня.		*2*
	2.	Управление персоналом.		*2*
	3.	Физическая защита.		*2*
	4.	Поддержание работоспособности.		*2*
	5.	Реагирование на нарушения режима безопасности.		*2*
	6.	Планирование восстановительных работ.		*2*
Тема 1.6	**Содержание**		1	

Программно-технический уровень информационной безопасности	1.	Основные понятия и меры уровня.		*2*
	2.	Особенности современных информационных систем.		*2*
	3.	Архитектурная безопасность.		*2*
Раздел 2 Методы и средства обеспечения безопасности информации			**30**	
Тема 2.1 Защита информации от утечки по техническим каналам	**Содержание**		2	
	1.	Основные виды технических каналов утечки информации. Техника промышленного шпионажа.		*2*
	2.	Противодействие наблюдению.		*2*
	3.	Противодействие прослушиванию.		*2*
	4.	Методы и средства защиты от побочных электромагнитных излучений и наводок.		*2*
Тема 2.2 Защита информации от несанкционированного доступа	**Содержание**		4	
	1.	Способы несанкционированного доступа к информации в компьютерных системах.		*2*
	2.	Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа.		*2*
	3.	Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация.		*2*
	4.	Управление доступом: основные понятия, мандатного и ролевого управления доступом виды разграничения доступа, особенности дискреционного,		*2*
	5.	Защита программных средств от несанкционированного копирования и исследования.		*2*
	6.	Протоколирование и аудит: основные понятия, активный аудит.		*2*
	7.	Общая характеристика компонентов системы защиты операционной системы Windows XP.		*3*
	8.	Защита информации от несанкционированного доступа в операционных системах семейства Unix.		*2*
	Практические занятия		6	
	1.	Методы аутентификации, использующие пароли.		
	2.	Изучение политики безопасности операционной системы Windows XP.		
	3.	Управление шаблонами безопасности в Windows 2000 (XP).		
	4.	Разграничение полномочий и доступа к объектам операционной системы Unix.		
	5.	Построение системы разграничения доступа в базе данных на основе ролевой модели.		
	Самостоятельная работа		4	

	1.	Рассмотреть неотъемлемые характеристики человека и особенности поведения, используемые при биометрической аутентификации пользователей.		
Тема 2.3 Криптографические методы защиты информации	**Содержание**		4	
	1.	Развитие криптографических систем. Основные понятия криптологии.		*2*
	2.	Классификация криптографических средств.		*2*
	3.	Симметричные криптосистемы: DES и ее модификации, ГОСТ 28147 – 89, принципы их построения.		*2*
	4.	Ассиметричные криптосистемы: однонаправленные функции, RSA, принципы построения.		*2*
	5.	Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные.		*2*
	6.	Функция хэширования.		*2*
	7.	Электронная цифровая подпись и ее применение для контроля целостности программ и данных.		*2*
	8.	Компьютерная стеганография и ее применение.		*2*
	Практические занятия		6	
	1.	Использование функций криптографического интерфейса (CryptoAPI) операционной системы Windows для защиты информации.		
	2.	Шифрующая файловая система EFS и управление сертификатами в Windows (2000) XP.		
	Самостоятельная работа		4	
	1.	Рассмотреть особенности и принципы работы стандартных и специализированных программных средств шифрования и компьютерной стеганографии.		
Раздел 3 Компьютерные вирусы и средства антивирусной защиты			**16**	
Тема 3.1 Вирусы как угроза ИБ	**Содержание**		2	
	1.	Общие сведения о компьютерных вирусах.		1
	2.	Классификация компьютерных вирусов.		1
	3.	Жизненный цикл вирусов.		*3*
	4.	Основные каналы распространения вирусов.		*3*
	5.	Вредоносные программы и их классификация.		*3*
	Самостоятельная работа		6	
	1.	Разработать контролирующий, диагностический или демонстрационный материал по теме 3.1 (кроссворд, тест, ребусы, презентация и др.).		
Тема 3.2 Средства	**Содержание**		2	

антивирусной защиты	1.	Методы и средства защиты от компьютерных вирусов.		*1*
	2.	Методы обнаружения и удаления вирусов.		*1*
	3.	Профилактика заражения вирусами компьютерных систем.		*1*
	4.	Программные закладки и методы защиты от них.		*2*
	5.	Антивирусные программные комплексы.		*3*
	Практические занятия			
	1.	Антивирусные программные комплексы.	4	
	2.	Восстановление зараженных файлов. Профилактика проникновения «троянских программ».		
	Самостоятельная работа			
	1.	Построить схему системы антивирусной защиты корпоративной сети (на примере).	2	
Раздел 4 Стандарты защищенности информации в компьютерных системах			**14**	
Тема 4.1 Стандарты и спецификации в области информационной безопасности	**Содержание**			
	1.	Характеристика систем стандартизации в области защиты информации.		*2*
	2.	Оценочные стандарты и технические спецификации: «Оранжевая книга».		*3*
	3.	Информационная безопасность распределенных систем. Рекомендации X.800.	2	*3*
	4.	Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».		*3*
	5.	Европейские критерии безопасности информационных технологий.		*3*
	6.	Документы Гостехкомиссии России по защите информации.		*3*
	Практические занятия			
	1.	Для выбранного объекта защиты информации предложить анализ увеличения защищенности по следующим пунктам: определить требования к защите информации, определить факторы, влияющие на требуемый уровень защиты информации, выбрать или разработать способы и средства защиты информации, построить архитектуру систем защиты информации, сформулировать рекомендации по увеличению уровня защищенности.	8	
	Самостоятельная работа			
	1.	Составить перечень понятий и определений, используемых в стандартах и спецификациях.	4	
		Всего:	**84**	

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета программирования и баз данных.
Оборудование: Доска универсальная, 5-ти секционная, Комплект учебной мебели, набор демонстрационного оборудования (проектор, экран), учебно-наглядные пособия (презентации по дисциплине), 16 компьютеров с выходом в сеть Интернет и в ЭИОС вуза
Программное обеспечение: Kaspersky Endpoint Security, Microsoft Office, Microsoft Windows.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Васильков, А.В. Информационные системы и их безопасность : учеб. пособие для ссузов / А.В. Васильков, А.А. Васильков, И.А. Васильков. - Москва : Форум, 2013
2. Нестеров С.А. — Основы информационной безопасности: учебное пособие.-СПб: Лань, 2018.-Режим доступа: https://e.lanbook.com/book/103908
3. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html
4. Нестеров, С. А. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-07979-1. — Режим доступа : www.biblio-online.ru/book/1997F695-44FF-4570-BF5D-882F5286AE77.

Дополнительные источники:

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html
2. Камалова, Г. Г. Информационное право в схемах, определениях и заданиях : учеб. пособие / Г. Г. Камалова, М-во образования и науки РФ, ФГБОУ ВО "Удмуртский государственный университет", Ин-т права, соц. упр. и безопасности, Каф. криминалистики и судеб. экспертиз. - Ижевск : Удмуртский университет, 2017.
3. Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для СПО / О. П. Новожилов. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 320 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-06372-1. — Режим доступа : www.biblio-online.ru/book/AA24B00F-EE29-4D83-B935-01A3776DCFD3.
4. Новожилов, О. П. Информатика в 2 ч. Часть 2 : учебник для СПО / О. П. Новожилов. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 302 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-06374-5. — Режим доступа : www.biblio-online.ru/book/C9811C60-1073-4857-AF64-2288A7D443A1.
5. 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 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html
6. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html
7. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон. текстовые данные. — М. : Интернет-

Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52160.html
8. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие/В.Ф. Шаньгин.- Москва: Форум: Инфра-м, 2018
9. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

Периодические издания:

1. Журнал для пользователей персональных компьютеров «Мир ПК» (архив номеров в свободном доступе на официальном сайте издательства http://www.osp.ru/pcworld/archive/)
2. «Сети/NetworkWorld» - журнал о технологиях, услугах и решениях для организации всех видов связи и коммуникаций на предприятиях. (архив номеров в свободном доступе на официальном сайте издательства http://www.osp.ru/nets/archive/)

Интернет-ресурсы:

1. iXBT.com (http://www.ixbt.com) — специализированный российский информационно-аналитический сайт сферы IT. На сайте ежедневно освещаются вопросы цифровых технологий и современных решений на их базе.
2. http://www.scrf.gov.ru
3. http://www.intuit.ru
4. https://edugalaxy.intel.ru

Программное обеспечение:

1. Операционная система Windows XP.
2. Офисные программы Microsoft 2007: Word, Excel, PowerPoint.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения

практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины.

Текущий контроль проводится в форме устного опроса.

5. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Реализация дисциплины для лиц с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Для маломобильных групп населения имеется необходимое материально-техническое обеспечение (пандусы, оборудованные санитарные комнаты, кнопки вызова персонала, оборудованные аудитории для лекционных и практических занятий)

Для адаптации программы освоения дисциплины используются следующие методы:

- Для лиц с нарушениями слуха используются методы визуализации информации (презентации, использование компьютера для передачи текстовой информации и др.)
- Для лиц с нарушениями зрения используются такие методы, как увеличение текста и картинки (в программах Windows), программы-синтезаторы речи, в том числе в ЭБС.

Форма проведения текущей и промежуточной аттестации для инвалидов и лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на

компьютере, в форме тестирования и т.п.), при необходимости выделяется дополнительное время на подготовку.

6. КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Смотреть Приложение 1.