Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А. Панфилов
«__» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

для специальности среднего профессионального образования
технического профиля
09.02.04 «Информационные системы (по отраслям)»

Владимир,2017 г.

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

Кафедра-разработчик: кафедра Информационных систем и программной инженерии ИСПИ ВлГУ.

Рабочую программу составил: Жигалов Илья Евгеньевич профессор кафедры ИСПИ.

Программа рассмотрена и одобрена на заседании кафедры Информационных систем и программной инженерии протокол № 10 от 2.06.16

Заведующий кафедрой ИСПИ_____Жигалов И.Е.

Программа рассмотрена на заседании УМК КИТП протокол № 11 от 27.06.16

Директор КИТП_____Корогодов Ю.Д.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

1.1. Область применения примерной программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности **09.02.04** Информационные системы (по отраслям)

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина входит в профессиональный цикл как общепрофессиональная дисциплина.

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

Цель рабочей программы учебной дисциплины:
В результате освоения учебной дисциплины обучающийся должен **уметь:**

- Формулировать тему, проблему, ставить цель и задачи, обосновывать актуальность проблемы, определять гипотезу, доказывать или опровергать ее.
- Изготовлять продукт исследовательской деятельности.
- Составлять содержание работы и план своих действий на каждом этапе.
- Составлять структуру своего исследования.
- Проводить исследование и делать вывод по его результам.
- Работать с различными источниками информации, используя разные формы защиты информации.
- Выявлять вирусы.
- Использовать современные средства защиты информации.

В результате освоения учебной дисциплины обучающийся должен **знать:**

- Современные методы защиты информации;
- Основные виды угроз;
- Виды продуктов вирусов;
- Формы защиты информации в сети ЭВМ;
- Требования к защите информации, критерии оценки угроз.

1.4. Количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 122 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 81 часа;
самостоятельной работы обучающегося 41 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	**122**
Обязательная аудиторная учебная нагрузка (всего)	**81**
в том числе:	
лекции	40
практические занятия	41
Самостоятельная работа обучающегося	**41**
В т.ч. внеаудиторная самостоятельная работа	41
Итоговая аттестация в форме:	**дифференцированного зачета**

2.2. Тематический план и содержание учебной дисциплины: Информационная безопасность и защита информации

Наименование разделов и тем	Содержание учебного материала, лекции и практические занятия, самостоятельная работа обучающихся.	Объем часов	Уровень освоения
1	**2**	**3**	**4**
Раздел 1.	**Общие вопросы информационный безопасности.**	**24**	
Тема 1.1. Международные стандарты информационного обмена	**Содержание учебного материала**	**4**	**1**
	1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. 2. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная.		
	Практические занятия: Защита документооборота в вычислительных системах	**4**	**2**
	Самостоятельная работа обучающихся: 1. Проведение анализа информационной системы. 2. Доклад на тему «Защита информации, тайна»	**4**	**3**
Тема 1.2 Понятия и угрозы.	**Содержание учебного материала**	**4**	**1**
	1. Основные понятия. Механизмы безопасности. Классы безопасности. 2. Основные определения и критерии классификации угроз		
	Практическая работа Криптографические методы защиты	**4**	**2**
	Самостоятельная работа обучающихся: 1. Выявление угроз и уязвимостей, каналов утечки информации 2. Презентация по теме «Основные угрозы»	**4**	**3**
Раздел 2.	**Государственная система информационной безопасности**	**12**	
Тема 2.1	**Содержание учебного материала**	**4**	**1**

Информационная безопасность в условиях функционирования в России глобальных сетей.	1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации 2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.		
	Практические занятия: Шифрование методом IDEA	**4**	**2**
	Самостоятельная работа обучающихся: 1. Краткий конспект по теме «Концепция информационной безопасности.» 2. Исследовательская работа	**4**	**3**
Раздел 3.	**Угрозы безопасности**	**12**	
Тема 3.1 Угрозы безопасности.	**Содержание учебного материала**	**4**	**1**
	1. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения 2. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации		
	Практические занятия: Шифрование методом RC6	**4**	**2**
	Самостоятельная работа обучающегося: 1. Виды противников или «нарушителей». Понятие о видах вируса 2. Краткий конспект по теме «Причины нарушения целостности информации.»	**4**	**3**
Раздел 4.	**Теоретические основы методов защиты информационных систем**	**12**	
Тема 4.1 Теоретические основы методов защиты информационных систем	**Содержание учебного материала**	**4**	**1**
	1. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности 2. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей		

	Практические занятия: Шифрование методом SAFER K-64	**4**	**2**
	Самостоятельная работа обучающегося: 1. Три вида возможных нарушений информационной системы. 2. Доклад по теме «Права доступа Take-Grant»	**4**	**3**
Раздел 5.	**Методы защиты средств вычислительной техники**	**12**	
Тема 5.1 Методы защиты средств вычислительной техники	**Содержание учебного материала**	**4**	**1**
	1. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. 2. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.		
	Практические занятия: Криптосистема Эль-Гамаля	**4**	**2**
	Самостоятельная работа обучающегося 1. Виды защиты 2. Выявление угроз и уязвимостей	**4**	**3**
Раздел 6.	**Основы криптографии**	**12**	
Тема 6.1	**Содержание учебного материала**	**4**	**1**
Основы криптографии	1. Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. 2. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы.		
	Практические занятия Шифрование методом Вернам	**4**	**2**
	Самостоятельная работа обучающегося: 1. Презентация по теме «Криптоанализ» 2. Презентация по теме «Электронно-цифровая подпись»	**4**	**3**
Раздел 7.	**Архитектура защитных экономических систем**	**12**	
Тема 7.1 Архитектура защитных экономических систем	**Содержание учебного материала**	**4**	**1**
	1. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации.		

	2. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.		
	Практические занятия Шифрование методом аналитических преобразований	**4**	**2**
	Самостоятельная работа обучающегося: 1. Краткий конспект «Функции защиты информации» 2. Доклад на тему «Стратегии защиты информации»	**4**	**3**
Раздел 8.	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**	**12**	
Тема 8.1 Алгоритмы и привязки программного обеспечения к аппаратному окружению	**Содержание учебного материала**	**4**	**1**
	1. Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. 2. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода		
	Практические занятия Сокрытие информации методом стеганографии	**4**	**2**
	Самостоятельная работа обучающегося: 1. Презентация на тему «Технология spyware» 2. Составить алгоритм программного обеспечения	**4**	**3**
Раздел 9.	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**	**14**	
Тема 9.1 Алгоритмы безопасности в компьютерных сетях	**Содержание учебного материала**	**4**	**1**
	1. Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. 2. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.		
	Практические занятия Сокрытие информации методом стеганографии	**5**	**2**
	Самостоятельная работа обучающегося: 1. Составить алгоритм безопасности 2. Проектирование МЭ	**5**	**3**
ВСЕГО		**122**	

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.

Оборудование учебного кабинета:

- сетевой компьютерный класс с выходом в Интернет;
- комплекты «столы-стулья» (2 к 1) в количестве не менее 15 шт.;
- шкафы для методической литературы;
- огнетушитель;
- информационные стенды

Технические средства обучения:

- интерактивная доска;
- проектор;
- компьютерное рабочее место для преподавателя;
- принтер;
- сканер.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, интернет ресурсов, дополнительной литературы

Основные источники:

1) Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. : БИНОМ, 2015. - (Программисту). - http://www.studentlibrary.ru/book/ISBN9785996329526.html Электронное издание на основе: Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ.-3-е изд. (эл.).-Электрон. текстовые дан. (1 файл pdf : 482 с.).- М. : БИНОМ. Лаборатория знаний, 2015.- (Программисту).-Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-9963-2952-6.
2) Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html Электронное издание на основе: Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN 978-5-94275-667-3.

3) Информатика 2015 [Электронный ресурс] : учебное пособие / Алексеев А.П. - М. : СОЛОН-ПРЕСС, 2015. - http://www.studentlibrary.ru/book/ISBN9785913591586.html Электронное издание на основе: Информатика 2015: учебное пособие/ Алексеев А.П.- 2015. - 400 с., илл. - ISBN 978-5-91359-158-6.

Дополнительные источники:

1) Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2012.

2) Соколов А. В., Степанюк О. М. Защита от компьютерного терроризма. Справоч-ное пособие. - СПб.: БХВ - Петербург, Арлит, 2012.- 496с.:ил.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Программа составлена в соответствии с требованиями ФГОС СПО для специальностей технического профиля

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1. выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	Выполнение и защита заданий по практическим работам.
2. осуществлять диагностику и поиск неисправностей технических средств;	Выполнение и защита заданий по практическим работам.
3. тестировать кабели и коммуникационные устройства;	Выполнение и защита заданий по практическим работам.
4. правильно оформлять техническую документацию;	Выполнение и защита заданий по практическим работам.
5. наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	Выполнение и защита заданий по практическим работам.
6. устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	Выполнение и защита заданий по практическим работам.

Программа составлена в соответствии с требованиями ФГОС СПО для специальностей технического профиля.

Разработчики:
ВлГУ кафедра ИСПИ, профессор Жигалов И.Е.

Рецензент (эксперт): _____

ООО, Системный подход | Директор департамента | Шиповских Р.Б.

(место работы) (занимаемая должность) (ФИО, подпись)