Департамент образования Вологодской области
бюджетное профессиональное образовательное учреждение
Вологодской области
«ВОЛОГОДСКИЙ СТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

УТВЕРЖДЕНО
приказом директора БПОУ ВО
«Вологодский строительный колледж»
№ 255 -УД от 20 июня 2017 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.15. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(базовая подготовка)

2017 г.

Рабочая программа учебной дисциплины **ОП.15. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** разработана на основе федерального государственного образовательного стандарта (далее – ФГОС) специальности среднего профессионального образования (далее СПО) **09.02.04 Информационные системы (по отраслям)**

Организация-разработчик:
БПОУ ВО «Вологодский строительный колледж»

Разработчики:

Ингеройнен Н.Л., преподаватель БПОУ ВО «Вологодский строительный колледж»

Исакова Н. А., преподаватель БПОУ ВО «Вологодский строительный колледж»

Рассмотрена на заседании предметной цикловой комиссии общепрофессиональных, специальных дисциплин и дипломного проектирования по специальностям 08.02.01 «Строительство и эксплуатация зданий и сооружений», 08.02.07 «Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции», 43.02.08 «Сервис домашнего и коммунального хозяйства» и рекомендована для внутреннего использования, протокол №11 от «13» июня 2017г

Председатель ПЦК А.В. Богданова

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.15. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.04 Информационные системы (по отраслям).

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

Дисциплина входит в **п**рофессиональный учебный цикл, относится к общепрофессиональным дисциплинам (ОП.00). Дисциплина введена из часов вариативной части.

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.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося – 123 часа, в том числе:
обязательной аудиторной учебной нагрузки обучающегося – 82 часа;
самостоятельной работы обучающегося – 41 час

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1.Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка	123
Обязательная аудиторная учебная нагрузка	82
в том числе:	
практические занятия	50
Самостоятельная работа обучающегося: *выполнение домашних работ по текущим темам* *выполнение практических заданий* *подготовка презентаций, докладов, рефератов и устных сообщений*	41
Промежуточная аттестация в форме экзамена	

2.2. Результаты освоения учебной дисциплины

Результатом освоения программы учебной дисциплины является овладение обучающимися профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
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 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий и профессиональной деятельности
ПК 1.4	Участвовать в экспериментальном тестировании информационной системы на этапе опытной эксплуатации, фиксировать выявленные ошибки кодирования в разрабатываемых модулях информационной системы.
ПК 1.10	Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

2.3. Тематический план и содержание учебной дисциплины ОП.15. Основы информационной безопасности

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		**2/2**	
Тема 1.1 Понятие национальной безопасности. Государственная информационная политика	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.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания* выучить основные понятия и определения *реферат* Понятие национальной безопасности; Информационная безопасность в системе национальной безопасности России; Государственная информационная политика	2	
Раздел 2. Сущность и понятие защиты информации		**16/8**	
Тема 2.1 Сущность и понятие информационной безопасности. Классификация информационных ресурсов	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.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания*	2	

	анализ документов образовательного учреждения *реферат* Информационная безопасность. Свойства информации как объекта защиты		
Тема 2.2 Виды и особенности угроз информационной безопасности	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.	2	2
	Практические занятия	2	
	Практическая работа 1. Анализ источников, каналов распространения и каналов утечки информации		
	Самостоятельная работа обучающихся: *выполнение домашнего задания* выучить основные понятия и определения	2	
Тема 2.3 Методы нарушения конфиденциальности, целостности и доступности информации	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.	2	2
	Практические занятия		
	Практическая работа 2. Проведение анализа информации на предмет целостности	2	
	Самостоятельная работа обучающихся: *выполнение домашнего задания* Составление последовательности действий по защите информации	2	
Тема 2.4 Методы и модели оценки уязвимости информации	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Система с полным перекрытием. Практическая реализация модели «угроза-защита».	2	3
	Практические занятия		

	Практическая работа 3. Оценка уязвимости информации	4	
	Самостоятельная работа обучающихся: *реферат* Сущность и понятие информационной безопасности; Классификация информационных ресурсов; Виды и особенности угроз информационной безопасности; Методы нарушения конфиденциальности, целостности и доступности информации.	2	
Раздел 3. Основы защиты информации		**14/6**	
Тема 3.1 Основы защиты информации**.** Функции и задачи защиты информации	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.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания* выучить основные понятия и определения *сообщение* Основы защиты информации в РФ; Анализ функций и задач защиты информации	2	
Тема 3.2 Анализ существующих методик определения требований защиты информации	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	2	3
	Практические занятия		
	Практическая работа 4. Требования к безопасности информационных систем.	2	
	Практическая работа 5. Требования к безопасности информационных систем в России.	2	
	Практическая работа 6. Оценка состояния безопасности ИС США.	2	
	Практическая работа 7. Определение классов защищенности средств вычислительной техники от несанкционированного доступа.	2	
	Практическая работа 8. Определение требований к защите информации	2	
	Самостоятельная работа обучающихся: *выполнение домашнего задания* составить таблицу классов защищённости	4	

Раздел 4. Правовое обеспечение информационной безопасности		**12/6**	
Тема 4.1 Концепция правового обеспечения информационной безопасности Российской Федерации	Законодательная база, стандарты и нормативно-методические документы РФ в области обеспечения информационной безопасности. Ответственность за нарушение законодательства в информационной сфере. ГОСТы по информационной безопасности	2	3
	Практические занятия		
	Практическая работа 9. Анализ терминов и определений информационной безопасности	2	
	Практическая работа 10. Работа с ГОСТами в области информационной безопасности	4	
	Самостоятельная работа обучающихся: *выполнение домашнего задания* выучить основные понятия и определения	2	
Тема 4.2 Зарубежные стандарты и международные соглашения в области информационной безопасности	Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания* сравнительный анализ международных стандартов и стандартов РФ	2	
Тема 4.3 Правовое регулирование информационных ресурсов	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.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания* составление глоссария "Термины и определения информационной безопасности"	2	
Раздел. 5. Организационные основы защиты информации		**10/6**	
Тема 5.1 Основные направления деятельности службы безопасности	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.	2	2

предприятия по защите информационных ресурсов	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.		
	Самостоятельная работа обучающихся: *выполнение домашнего задания* *составление таблицы* Потенциальные и реальные угрозы.	2	
Тема 5.2 Защита информации при проведении совещаний и переговоров по конфиденциальным вопросам, приеме посетителей. Защищенный документооборот	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.	2	3
	Практические занятия		
	Практическая работа 11. Составление инструкции по обработке и хранению конфиденциальных документов	2	
	Практическая работа 12. Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации	2	

	Практическая работа 13. Оценка безопасности информации на объектах ее обработки	2	
	Самостоятельная работа обучающихся: *выполнение домашнего задания* выучить основные понятия и определения *реферат* Основные направления и этапы работ по созданию комплексной системы безопасности предприятия; Методологические основы системы безопасности предприятия.	4	
Раздел 6. Обеспечение безопасности автоматизированных систем.		**28/13**	
Тема 6.1 Основные принципы построения подсистемы защиты информации	Основные подходы к созданию защиты АИС. Идентификация и аутентификация. Разграничение доступа. Контроль целостности. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Обнаружение и противодействие атакам.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания* *презентация* Идентификация и аутентификация.	2	
Тема 6.2 Методы защиты информации в АИС	Организационные, правовые, технические, программно-математические методы и их соотношение.	2	2
	Самостоятельная работа обучающихся: *выполнение домашнего задания* анализ основных методов защиты информации: преимущества и недостатки	2	
Тема 6.3 Основные принципы защиты информации от несанкционированного доступа	Источники и пути реализации несанкционированного доступа к информации в АИС. Основные принципы защиты информации от несанкционированного доступа. Средства и механизмы защиты от несанкционированного доступа.	2	3
	Самостоятельная работа обучающихся: *выполнение домашнего задания* *реферат* «Абсолютная» система защиты.	2	
Тема 6.4 Управление доступом в АИС	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	2	3

	роли.		
	Практические занятия		
	Практическая работа 14. Классификация автоматизированных систем обработки информации по классу защиты информации	2	
	Практическая работа 15. Планирование, создание и изменение учетных записей пользователей.	2	
	Практическая работа 16. Создание и администрирование групп пользователей.	2	
	Практическая работа 17. Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам.	2	
	Практическая работа 18. Наследование разрешений в NTFS.	2	
	Практическая работа 19. Изменение параметров учетных записей пользователей.	2	
	Практическая работа 20. Настройка политики учетных записей.	2	
	Практическая работа 21. Настройка параметров безопасности операционных систем.	2	
	Практическая работа 22. Настройка параметров безопасности Windows.	2	
	Практическая работа 23. Настройка параметров безопасности Интернет.	2	
	Самостоятельная работа обучающихся: *выполнение домашнего задания* выучить основные понятия и определения. Повторить весь материал.	7	
Экзамен			
	ВСЕГО:	**123**	

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 ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебной лаборатории компьютерных сетей.

Оборудование лаборатории и рабочих мест лаборатории:

1. рабочее место преподавателя;
2. персональные компьютеры для студентов;
3. мультимедийное оборудование;

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. 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
2. Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2016. — 169 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67452.html
3. Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс] : учебное пособие / К.А. Паршин. — Электрон. текстовые данные. — М. : Учебно-методический центр по образованию на железнодорожном транспорте, 2015. — 96 c. — 978-5-89035-821-9. — Режим доступа: http://www.iprbookshop.ru/45291.html

Дополнительные источники:

1. Методические указания к практическим работам по дисциплине ОП.15. Основы информационной безопасности, 2017г.
2. Методические рекомендации по организации внеаудиторной самостоятельной работы студентов по дисциплине ОП.15. Основы информационной безопасности, 2017г.

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 студентами 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 способы обеспечения информационной безопасности.	выполнение контрольных заданий, тестов, домашняя работа, практические занятия, экзамен