Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ
ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ

Учебно-методическая документация

УТВЕРЖДАЮ
Директор колледжа
_____ В. А. Шульцев
(подпись)
«26» сентября 2017 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность:
09.02.01 Компьютерные системы и комплексы

Квалификация выпускника: техник по компьютерным системам

(базовая подготовка)

Согласовано:

Зам. начальника УМУ НовГУ по СПО
_____ М. В. Никифорова
(подпись)
«25» сентября 2017 г.

Заместитель директора по УМ и ВР
_____ Л. Н. Иванова
(подпись)
«22» сентября 2017 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) (приказ Министерства образования и науки РФ от 28.07.2014 года № 849) по специальности среднего профессионального образования (далее – СПО) 09.02.01 Компьютерные системы и комплексы в соответствии с учебными планами.

Организация-разработчик: Федеральное государственное бюджетное образовательное учреждение высшего образования «Новгородский государственный университет имени Ярослава Мудрого» Многопрофильный колледж Политехнический колледж

Разработчик (и): Цымбалюк Алексей Евгеньевич, преподаватель

Рабочая программа принята на заседании предметной (цикловой) комиссии общепрофессиональных дисциплин колледжа протокол № 1 от 04.09.2017 г.

Председатель предметной (цикловой) комиссии _____ / Л. Н. Цымбалюк
(подпись)

Рецензент: преподаватель дисциплин профессионального цикла Политехнического колледжа НовГУ им. Ярослава Мудрого Цымбалюк Л. Н.

2

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
«Информационная безопасность»

1.1. Область применения рабочей программы

Рабочая программа дисциплины является частью основной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы.

1.2. Место учебной дисциплины в структуре основной образовательной программы

Учебная дисциплина «Информационная безопасность» относится к общепрофессиональному циклу.

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

В результат освоения учебной дисциплины обучающийся должен **уметь:**

- классифицировать угрозы информационной безопасности;
- проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- производить установку и настройку средств защиты;
- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- выполнять тестирование систем с целью определения уровня защищенности;
- использовать программные продукты для защиты баз данных;
- применять криптографические методы защиты информации;

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

- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей;
- возможные способы несанкционированного доступа;
- нормативно-правовые и законодательные акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- собственные средства защиты различных операционных систем и сред;
- способы и методы шифрования информации

1.4. Перечень формируемых компетенций

Техник по компьютерным системам должен обладать общими компетенциями, включающими в себя способность:

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 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 в профессиональной деятельности.

Техник по компьютерным системам должен обладать профессиональными компетенциями, соответствующими видам деятельности:

ПК 1 Выполнять тестирование программных модулей.

ПК 2 Осуществлять оптимизацию программного кода модуля.

ПК 3 Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.

ПК 4 Решать вопросы администрирования базы данных.

ПК 5 Реализовывать методы и технологии защиты информации в базах данных.

1.5 Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины:

Максимальная учебная нагрузка обучающегося 79 часов, в том числе:

- обязательная аудиторная учебная нагрузка обучающегося 54 часа;
- самостоятельная работа обучающегося 25 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	***79***
Обязательная аудиторная учебная нагрузка (всего)	***54***
в том числе:	
лекции	*20*
лабораторные работы	*-*
практические занятия	*34*
контрольные работы	*-*
курсовая работа (проект)	*-*
Самостоятельная работа обучающегося (всего)	***25***
Итоговая аттестация в форме дифференцированного зачета в 8 семестре	

2.2. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Основы информационной безопасности		**8**	
Тема 1.1. Понятие информационной безопасности, угрозы ИБ	**Содержание учебного материала**	4	**2**
	Понятие информационной безопасности, характеристика ее составляющих. Место информационной безопасности в системе национальной безопасности. Концептуальная модель защиты информации. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации. Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. Виды уязвимости информации и формы ее проявления.		
Тема 1.2. Конфиденциальная информация	**Содержание учебного материала**	*1*	**2**
	Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне). Уровни информационной безопасности - законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации.		
	Самостоятельная работа студентов №1. Разработка проектов документов по организации защиты конфиденциальной информации.	*3*	**2**
Раздел 2. Правовое обеспечение		**13**	

информационной безопасности			
Тема 2.1 Нормативно-правовые основы информационной безопасности в РФ.	**Содержание учебного материала**	*2*	
	Информация как объект права. Нормативно-правовые основы информационной безопасности в РФ. Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. Конституционные гарантии прав граждан в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Система защиты государственной тайны, правовой режим защиты государственной тайны.		
	Практическое занятие: **1)** Использование законов подзаконных актов для обеспечения защиты информации в организации **2)** Изучение программного обеспечения по защите информации для компьютерных систем и сетей	*2* *2*	
Тема 2.2 Лицензирование и сертификация	**Содержание учебного материала**	*1*	
	Лицензирование и сертификация в области защиты информации. Стандартизация информационной безопасности.		
	Практические занятия: **3)** Нормативно-правовые акты информационной безопасности по лицензированию и сертификации	*2*	
	Самостоятельная работа студентов №2 Изучение международных нормативно-правовых актов в области обеспечения информационной безопасности	*4*	
Раздел 3. Организационное обеспечение информационной безопасности		***12***	
Тема 3.1 Понятие организационного обеспечения ИБ	**Содержание учебного материала**	*2*	
	Сущность и сферы действия организационной защиты информации. Механизмы обеспечения информационной безопасности. Разработка политики безопасности.		

	Практические занятия: **4)** Построение схемы СВТ и ТК в помещении	*2*	
	Самостоятельная работа студентов №3 Планирование информационной безопасности	*4*	
Тема 3.2 **Модели защиты информационных систем**	**Содержание учебного материала**	*2*	
	Проведение анализа угроз и расчета рисков в области информационной безопасности. Выбор механизмов и средств обеспечения информационной безопасности. Модели защиты информационных систем. Правила организации работ подразделений защиты информации. Разработка инструкций по работе со средствами защиты. Организация работы персонала с конфиденциальной информацией.		
	Практические занятия: **5)** Разработка должностной инструкции специалиста по защите информации.	*2*	**2**
Раздел 4. **Программно-аппаратные средства защиты информации**		***26***	
Тема 4.1. **Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях.**	**Содержание учебного материала**	*2*	
	Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях. Структурные схемы систем защиты информации в типовых информационных системах. Показатели защищенности телекоммуникационных систем. Сервисы, обеспечивающие информационную безопасность в телекоммуникационных системах и информационно-коммуникационных сетях связи: ограничение физического доступа к автоматизированным системам; идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит); криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности.		

	Практические занятия: **6)** Практическая отработка навыков с аудитом ресурсов и событий в сетевых операционных системах **7)** Методы разграничения доступа в сетевых операционных системах. **8)** Настройка разрешений файловой системы. **9)** Настройка брандмауэра. **10)** Конфигурирование политик безопасности.	*10*	
Тема 4.2. Антивирусная защита информации	**Содержание учебного материала**	*2*	
	Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы. Построение систем антивирусной защиты телекоммуникационных систем и сетей.		
	Практические занятия: **11)** Установка антивируса Касперского и организация защищенной сети с помощью сервера администрирования **12)** Применение антивирусной защиты в информационных системах.	*4*	
	Самостоятельная работа студентов Самостоятельная работа № 4. Анализ современных антивирусных средств защиты информации. Самостоятельная работа № 5. Анализ обеспечения антивирусной защиты в колледже	*4* *4*	**3**
Раздел 5. Администрирование телекоммуникационных систем		***20***	
Тема 3.1 Технологии защиты данных	**Содержание учебного материала**	*2*	
	Технологии защиты данных. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография). Различные технологий аутентификации. Технологии защиты межсетевого обмена данных.		
Тема 3.2 Технология обеспечения безопасности сетевых операционных систем.	**Содержание учебного материала**	*2*	
	Технология обеспечения безопасности сетевых операционных систем. Основы технологии виртуальных защищенных сетей VPN. Технология обнаружения вторжений (анализ защищенности и		

	обнаружения сетевых атак). Требования по защите от несанкционированного доступа.		
	Практические занятия: **13)** Установка и настройка СЗИ «Аура». **14)** Шифрование методом Цезаря и Аффинной системой. **15)** СКЗИ КриптоПРО. Установка и настройка. **16)** СКЗИ КриптоПро. Работа с контенерами и сертификатами **17)** Настройка параметров безопасности СКЗИ. Генерация ключей и получение сертификата при помощи УЦ	*10*	
	Самостоятельная работа студентов Самостоятельная работа № 6. Шифрование. Анализ программ шифрования данных Самостоятельная работа № 7. Технологии виртуальных защищенных сетей VPN Самостоятельная работа № 8. Различные технологий аутентификации	 *2* *2* *2*	**3**
	Всего	**79**	

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 кабинета «Информатики».

Оборудование учебного кабинета:

– технические средства обучения: персональные компьютеры, локальная сеть, коммутатор для подключения в сети Internet, мультимедиа-проектор, принтер, сканер.

– используемое программное обеспечение:

- Программа ОС Windows XP/7
- Антивирусные программы: Kaspersky AntiVirus
- MS Office
- Браузер Internet Explorer
- MS Visio

3.2. Информационное обеспечение обучения

Основные источники:

1. Организация сетевого администрирования, М.-2017, Инфра-м, 384с. Баранчиков П.А.

2. Дроздов С.Н. Операционные системы: учебное пособие, Ростов н/ДЖ Феникс, 2016, 361с.

3. Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования, М. Академия, 2015. 256с. Г.Н. Богомазова

4. Модернизация программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования, М. Академия, 2015. 192с. Г.Н. Богомазова

Дополнительные источники:

1. Windows 7, скрипты, автоматизация и командная строка. СПб, Питер, 2012, 784с.

2. Сетевые операционные системы, В.Г. Олифер, СПб, Питер, 2002, 544с.

3. Информационная архитектура в сети Интернет, 3-е издание, Морвиль П., СПб, Символ-Плюс, 2010, 608с.

4. Колисниченко Д.Н., Командная строка Linux и автоматизация рутинных задач, СПб.: БХВ-Петербург, 2014, 368с

5. Гришина Н.В. Комплексная защита информации на предприятии, Форум, 2011, 240с.

6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей М. Форум – Инфра-м, 2012, 416с.

7. Эксплуатация объектов сетевой инфраструктуры, М. Академия, 2014. 368с. Под редакцией А.В. Назарова

Сайты дистанционного обучения:

http://intuit.ru

http://java.sun.com/

http://www.perl.org/
http://www.php.net/

Отечественные журналы

1. Мир ПК
2. Первая миля
3. Электросвязь
4. Сети
5. Мир связи
6. Технологии и средства связи
7. Радио
8. Мир ПК+СД
9. Мобильные компьютеры +СД
10. Системный администратор
11. Системы безопасности.
12. Сети и системы связи
13. Мобильные телекоммуникации
14. Технологии и средства связи
15. Радиомастер. Практическая радиоэлектроника
16. Ремонт электронной техники
17. Мир связи Connect
18. Мобильные системы

Интернет-ресурсы:

1. http://www.guardofinform.narod.ru/bibl_3.htm
2. www.minsvyaz.ru Официальный сайт Министерства информационных технологий и связи.
3. www.sotovik.ru Информационный сайт, посвященный телекоммуникациям: обзоры рынка, новости операторов.
4. www.telecomru.ru Экспертный портал "Телекоммуникации России" - независимое сетевое СМИ.
5. www.comnews.ru Новости рынка телекоммуникаций России и СНГ.
6. www.mobail-review.com Сайт, посвященный мобильным устройствам и технологиям, новостям операторов связи, рекламным акциям.
7. www.gptelecom.ru Законы РФ, постановления Правительства, документы Министерства связи и массовых коммуникаций РФ, технические документы и т. д.
8. www.osp.ru , www.pcmag.ru ,
9. www.crn.ru , www.elrussia.ru , www.kit-e.ru , www.globus-telecom.com , www.d-link.ru ,
10. www.intuit.ru , www.connect.ru , www.qwerty.ru ,
11. www.elsv.ru , www.ccc.ru Информационно-справочные системы.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателями в процессе проведения практических занятий, тестирования.

Оценка качества освоения профессионального модуля включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины.

Текущий контроль проводится в форме устного опроса, компьютерного тестирования.

Итоговая аттестация по модулю проводится в форме дифференцированного зачета в 8 семестре.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате изучения учебной дисциплины «Информационная безопасность» обучающийся должен: **знать** – каналы утечки информации; – - назначение, классификацию и принципы работы специализированного оборудования; – принципы построения информационно-коммуникационных сетей; – возможные способы несанкционированного доступа; – - нормативно-правовые и законодательные акты в области информационной безопасности; – правила проведения возможных проверок; – этапы определения конфиденциальности документов объекта защиты; – технологии применения программных продуктов; – возможные способы, места установки и настройки программных продуктов; – конфигурации защищаемых сетей; – алгоритмы работы тестовых программ; – собственные средства защиты различных операционных систем и сред; – способы и методы шифрования информации	**Формы контроля обучения:** - устный опрос, - компьютерное тестирование; - контрольные работы; - домашнее задание творческого характера; - практические задания; **Методы оценки результатов обучения:** - традиционная система отметок в баллах за каждую выполненную работу, на основе которых выставляется итоговая отметка
уметь – классифицировать угрозы информационной безопасности; – проводить выборку средств защиты в соответствии с выявленными угрозами; – определять возможные виды атак; – осуществлять мероприятия по проведению аттестационных работ; – разрабатывать политику безопасности объекта; – выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта; – использовать программные продукты, выявляющие недостатки систем защиты;	**Формы контроля обучения:** - устный опрос, - домашнее задание творческого характера; - практические задания **Формы контроля обучения:** - устный опрос, - домашнее задание творческого характера;

– производить установку и настройку средств защиты; – конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; – выполнять тестирование систем с целью определения уровня защищенности; – использовать программные продукты для защиты баз данных; – применять криптографические методы защиты информации;	- практические задания

5. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изме-нения	Номер листа				Всего листов в документе	ФИО и подпись ответственного за внесение изменения	Дата внесения изменения	Дата введения изменения
	измененного	замененного	нового	изъятого				