Воронежский колледж робототехники и компьютерных технологий

УТВЕРЖДАЮ
Директор колледжа
_____ Лукина В.Б.
«_____» _____ 2019г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

для специальности среднего профессионального образования **10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»**

Квалификация выпускника: **техник по защите информации**

Воронеж
2019

Рабочая программа составлена на основании требований:

— Федерального государственного образовательного стандарта среднего профессионального образования № 1551, утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г.;

— учебного плана Воронежского колледжа робототехники и компьютерных технологий по специальности 10.02.04 — "Обеспечение информационной безопасности телекоммуникационных систем", утвержденного Педагогическим советом от 16.12.2019 г. протокол №1

Индекс — 10.02.04 ИБ

Составитель: преподаватель _____С.С. Куликов

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Цель и планируемые результаты освоения учебной дисциплины

Место дисциплины в структуре примерной основной профессиональной образовательной программы:

Дисциплина ОП.04 Основы информационной безопасности входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

1.1.1. Перечень общих компетенций

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ПК 2.3	классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;	сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Максимальная учебная нагрузка	**60**
Обязательная учебная нагрузка	**48**
в том числе:	
теоретическое обучение	32
Лабораторные и практические занятия	16
Самостоятельные работы[1]	12

1 Самостоятельная работа в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема учебной дисциплины в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**6**	ОК 3, ОК 6, ОК 9, ПК.2.3
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**6**	ОК 3, ОК 6, ОК 9, ПК 2.3
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.		
	Практические занятия	**3**	
	Определение объектов защиты на типовом объекте информатизации.		

	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	**3**	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание учебного материала**	**5**	ОК 3, ОК 6, ОК 9, ПК.2.3
	Понятие угрозы безопасности информации Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации Уязвимости. Методы оценки уязвимости информации		
	Практическое занятие	**3**	
	Определение угроз объекта информатизации и их классификация		
Раздел 2. Методология защиты информации			
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала** Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.	**5**	ОК 3, ОК 6, ОК 9, ПК 2.3
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала** Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	**5**	ОК 3, ОК 6, ОК 9
	Практическое занятие	**3**	
	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		
Тема 2.3. Защита ин-	**Содержание учебного материала**		ОК 3, ОК 6,

формации в автоматизированных (информационных) системах	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	5	ОК 9
	Практическое занятие	**4**	
	Выбор мер защиты информации для автоматизированного рабочего места		
Всего		**60**	

1. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности лаборатории информационных технологий.

Оборудование учебного кабинета: персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия.

Оборудование лаборатории информационных технологий: посадочные места по количеству обучающихся; рабочее место преподавателя; мультимедийное оборудование.

3.2. Информационное обеспечение реализации программы

Основные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2015.

Дополнительные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016. http://www.iprbookshop.ru/10677.html

3. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2016.

4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

5. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016. http://www.iprbookshop.ru/43960.html

6. Белов Е.Б. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2017.

7. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2012.

8. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

9. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

Периодические издания:

10. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

11. Журналы Защита информации. Инсайд: Информационно-методический журнал Информационная безопасность регионов: Научно-практический журнал

12. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

13. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	**Критерии оценки**	**Формы и методы оценки**
Умения: классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;	Оценка умений осуществляется по пятибалльной шкале	Контроль знаний и умений осуществляется в ходе выполнения практических и лабораторных работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя

Знания: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности.	Оценка знаний осуществляется по пятибалльной шкале	Контроль выполняется по результатам проведения различных форм опроса, выполнения контрольных работ, тестирования, выполнения практических работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя

ПРИЛОЖЕНИЕ 1

Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ

Директор колледжа

_____ Лукина В.Б.

«_____» _____ 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

дисциплины

«ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

для специальности среднего профессионального образования **10.02.04 " Обеспечение информационной безопасности телекоммуникационных систем "**

Квалификация выпускника: **техник по защите информации**.

Воронеж
2019

Цель фонда оценочных средств. Оценочные средства предназначе-

ны для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Основы информационной безопасности». Перечень видов оценочных средств соответствует Рабочей программе дисциплины.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме индивидуальных заданий при выполнении цикла лабораторных работ и промежуточной аттестации в форме вопросов и заданий (могут быть заданы как в форме билета, так и экзаменационного теста) к экзамену.

Структура и содержание заданий - задания разработаны в соответствии с рабочей программой дисциплины «Основы информационной безопасности».

1. Паспорт фонда оценочных средств

Результатом освоения учебной дисциплины являются предусмотренные ФГОС по специальности умения и знания, направленные на формирование общих и профессиональных компетенций.

Таблица 1

№ п/п	Код компетенции	Содержание компетенции	Планируемые результаты обучения	Наименование оценочного средства
1	ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования **Знания:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	**Задание** на выполнение индивидуального варианта лабораторной работы
2	ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	**Умения:** описывать значимость своей специальности **Знания:** сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности	**Задание** на выполнение индивидуального варианта лабораторной работы
3	ОК 09	Использовать информационные технологии в профессиональной деятельности.	**Умения:** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение **Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы

4	ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями..	**Знания:** возможных угроз безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.	**Задание** на выполнение индивидуального варианта лабораторной работы
			Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	

Формой промежуточной аттестации по учебной дисциплине является

зачет (дифференцированный)

указать форму аттестации, предусмотренную учебным планом

2. Формы контроля и оценивания элементов учебной дисциплины

В результате текущей аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Таблица 2

Раздел / тема дисциплины	**Проверяемые У, З, ОК, ПК**	**Форма текущего контроля и оценивания**
Раздел 1. Теоретические основы информационной безопасности	ОК 3, ОК 6, ОК 9, ПК.2.3	Самостоятельная работа
Тема 1.1. Основные понятия и задачи информационной безопасности	ОК 3, ОК 6, ОК 9, ПК.2.3	Самостоятельная работа
Тема 1.2. Основы защиты информации	ОК 3, ОК 6, ОК 9, ПК.2.3	Практическое занятие №№ 1,2
Тема 1.3. Угрозы безопасности защищаемой информации.	ОК 3, ОК 6, ОК 9, ПК.2.3	Практическое занятие №№ 3
Раздел 2. Методология защиты информации	ОК 3, ОК 6, ОК 9	Самостоятельная работа
Тема 2.1. Методологические подходы к защите информации	ОК 3, ОК 6, ОК 9	Самостоятельная работа
Тема 2.2. Нормативно правовое регулирование защиты информации	ОК 3, ОК 6, ОК 9	Практическое занятие №№ 1
Тема 2.3. Защита информации в автоматизированных (информационных) системах	ОК 3, ОК 6, ОК 9	Практическое занятие №№ 2

3. Оценка освоения учебной дисциплины

3.1 Тематика курсовых работ

Курсовая работа по дисциплине не предусмотрена учебным планом

4. Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине

Оценка освоения дисциплины предусматривает проведение экзамена

указать форму аттестации, предусмотренную учебным планом

4.1. Вопросы (задания) к экзамену по дисциплине:

1. Понятие информации и информационной безопасности.

2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации». Понятие «риска информационной безопасности».
5. Примеры преступлений в сфере информации и информационных технологий.
6. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
7. Целостность, доступность и конфиденциальность информации.
8. Классификация информации по видам тайны и степеням конфиденциальности.
9. Понятия государственной тайны и конфиденциальной информации.
10. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
11. Цели и задачи защиты информации. Основные понятия в области защиты информации.
12. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.
13. Понятие угрозы безопасности информации
14. Системная классификация угроз безопасности информации.
15. Каналы и методы несанкционированного доступа к информации
16. Уязвимости. Методы оценки уязвимости информации
17. Анализ существующих методик определения требований к защите информации.
18. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
19. Виды мер и основные принципы защиты информации.
20. Организационная структура системы защиты информации
21. Законодательные акты в области защиты информации.
22. Российские и международные стандарты, определяющие требования к защите информации.
23. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации

5. Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Индикаторы компетенции	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
Полнота знаний	Уровень знаний ниже минимальных требований. Лабораторные работы выполнены не в полном объеме	Минимально допустимый уровень знаний. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки, лабораторные работы выполнены в полном объеме
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи. Индивидуальные задачи решены по типовому шаблону.	Продемонстрированы все основные умения. Решены типовые задачи. Выполнены индивидуальные задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи, выполнены все индивидуальные задания в полном объеме.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Ниже среднего	Средний	Высокий