ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

РАБОЧАЯ ПРОГРАММА
учебной дисциплины
ОП.04 Основы информационной безопасности
(наименование учебной дисциплины)

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код, наименование профессии/специальности)

2024

Рассмотрено и согласовано цикловой комиссией компьютерных дисциплин. Протокол № 2 от «02» сентября 2024 г.

Разработана на основе ФГОС СПО РФ и ПООП СПО для специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» (утверждён приказом Министерства образования и науки от 9 декабря 2016 №1551).

Организация разработчик: Политехнический колледж ЛГАУ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.04 Основы информационной безопасности

1.1. Область применения программы учебной дисциплины

Рабочая программа учебной дисциплины (далее – рабочая программа) является частью освоения программ подготовки специалистов среднего звена (далее ППССЗ) в соответствии с ФГОС СПО РФ и ПООП СПО для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

(указать профессию, специальность, укрупненную группу (группы) профессий или направление (направления) подготовки)

Рабочая программа учебной дисциплины ОП.04 Основы информационной безопасности по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем может быть использована на базе среднего (полного общего) образования, в профессиональном обучении и дополнительном профессиональном образовании.

1.2. Цели и задачи учебной дисциплины, требования к результатам освоения учебной дисциплины

Учебная дисциплина ОП.04 Основы информационной безопасности относится к общепрофессиональному циклу.

Целью реализации основной образовательной программы среднего общего образования по предмету ОП.04 Основы информационной безопасности является освоение содержания предмета Основы информационной безопасности и достижение обучающимися результатов изучения в соответствии с требованиями, установленными ФГОС СПО РФ и ПООП СПО.

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания.

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

-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 об- работке 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;

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

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

- классифицировать основные угрозы безопасности информации;

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4	- 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 об- работке 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;

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Тематический план учебной дисциплины

ОП.04 Основы информационной безопасности

Вид учебной работы	**Количество часов**
1	2
Максимальная учебная нагрузка (всего)	69
Обязательная аудиторная учебная нагрузка (всего)	69
в т. ч.:	
теоретическое обучение	17
практические занятия	29
Самостоятельная работа обучающегося	21
Промежуточная аттестация: дифференцированный зачет	2
ИТОГО	69

3.2. Содержание обучения по учебной дисциплине ОП.04 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
Раздел 1. Электронные приборы		**34**	
Тема 1.1 Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**11**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	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».	3	
	Практическое занятие. Инструктаж по ТБ Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации.	5	
	Самостоятельная работа обучающихся Защита человека от опасной информации и от не информированности в области информационной безопасности	3	
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**11**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	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.	2	
	Практическое занятие. Инструктаж по ТБ Определение объектов защиты на типовом объекте информатизации	5	
	Самостоятельная работа обучающихся Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	4	
Тема 1.3 Угрозы безопасности защищаемой информации.	**Содержание учебного материала**	**12**	ОК 03, ОК 06, ОК 09, ОК 10,
	Понятие угрозы безопасности информации Системная классификация угроз безопасности информации. Каналы и методы несанкционированного **доступа к информации Уязвимости.**	3	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	Практическое занятие. Инструктаж по ТБ Определение угроз объекта информатизации и их классификация	5	ПК 2.4
	Самостоятельная работа обучающихся Методы оценки уязвимости информации	4	
Раздел 2 Методология защиты информации		**33**	
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**	**10**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	3	
	Практическое занятие. Инструктаж по ТБ Виды мер защиты информации.	4	
	Самостоятельная работа обучающихся . Основные принципы защиты информации.	3	
Тема 2.2. **Нормативно правовое регулирование защиты информации**	**Содержание учебного материала**	**12**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	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.	3	
	Практическое занятие. Инструктаж по ТБ Работа в справочно-правовой системе с нормативными и правовыми документами по ин формационной безопасности	5	
	Самостоятельная работа обучающихся . Основные правила и документы системы сертификации РФ в области защиты информации	4	
Тема 2.3. **Защита информации в авто-матизированных (информационных) системах**	**Содержание учебного материала**	**11**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	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 внутри объектовый режим.	3	
	Практическое занятие. Инструктаж по ТБ	5	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	Выбор мер защиты информации для автоматизированного рабочего места		
	Самостоятельная работа обучающихся . Принципы построения организационно-распорядительной системы.	3	
	Всего: **из них практических занятий** **лекций** **самостоятельная работа** **зачет** **экзамен**	186 78 50 56 2 -	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Требования к материально-техническому обеспечению

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

Эффективность преподавания курса Основы информационной безопасности зависит от наличия соответствующего материально-технического оснащения. Это объясняется особенностями курса, в первую очередь его многопрофильностью и практической направленностью.

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.

(*Приводится перечень средств обучения, включая тренажеры, модели, макеты, оборудование, технические средства, в т. ч. аудиовизуальные, компьютерные и телекоммуникационные и т. п. (количество не указывается)*

Требования к квалификации педагогических кадров, осуществляющих реализацию ППССЗ по специальности, должны обеспечиваться педагогическими кадрами, имеющими среднее профессиональное, высшее образование, соответствующее профилю преподаваемой учебной дисциплины. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла.

Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже одного раза в 5 лет.

4.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

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. Исто- рия защиты информации в России. – М.: Издательство КДУ.

2.Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.

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.

6. Белов Е.Б. Пржегорлинский В.Н. Организационно-правовое обеспечение ин- формационной 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 безо- пасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

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

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК Рос- сии) 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 темати- ке 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 об- разовании» htpp\\:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем при проведении лабораторных работ, практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований, практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
1	2
Умения	
- классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации;	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;	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

ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СПЕДСТВА

учебной дисциплины

ОП.04 Основы информационной безопасности

(наименование учебной дисциплины)

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

(код, наименование профессии/специальности)

2024

Вопросы к дифференцированному зачету 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».
5. Понятие «риска информационной безопасности».
6. Примеры преступлений в сфере информации и информационных технологий.
7. Сущность функционирования системы защиты информации.
8. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
9. Целостность, доступность и конфиденциальность информации.
10. Классификация информации по видам тайны и степеням конфиденциальности.
11. Понятия государственной тайны и конфиденциальной информации.
12. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
13. Цели и задачи защиты информации. Основные понятия в области защиты информации.
14. Элементы процесса менеджмента ИБ.
15. Модель интеграции информационной безопасности в основную деятельность организации.
16. Понятие Политики безопасности.
17. Работа с документами в области информационной безопасности РФ по определению объектив защиты и классификации тайн
18. Определение объектов защиты на типовом объекте информатизации
19. Классификация защищаемой информации по видам тайны и степеням конфиденциальности
20. Понятие угрозы безопасности информации.
21. Системная классификация угроз безопасности информации.
22. Каналы и методы несанкционированного доступа к информации.
23. Уязвимости. Методы оценки уязвимости информации
24. Анализ существующих методик определения требований к защите информации.
25. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
26. Виды мер и основные принципы защиты информации.
27. Организационная структура системы защиты информации.
28. Законодательные акты в области защиты информации.
29. Российские и международные стандарты, определяющие требования к защите информации.
30. Система сертификации РФ в области защиты информации.
31. Основные правила и документы системы сертификации РФ в области защиты информации

32. Основные механизмы защиты информации.

33. Система защиты информации.

34. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.

35. Программные и программно-аппаратные средства защиты информации

36. Инженерная защита и техническая охрана объектов информатизации

37. Организационно-распорядительная защита информации.

38. Работа с кадрами и внутриобъектовый режим.

39. Принципы построения организационно-распорядительной системы.