

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»



УТВЕРЖДАЮ
Проректор по УиНР

А.В. Лейфа
2020 год.

РАБОЧАЯ ПРОГРАММА
по дисциплине
ОП.04. Основы информационной безопасности

Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
Квалификация выпускника – техник по защите информации
Год набора 2020
Курс 2 Семестр 3
Экзамен 3 семестр
Практические занятия 18 (час.)
Лекции 26 (час.)
Самостоятельная работа 6 (час.)
Промежуточная аттестация 6 (час.)
Общая трудоемкость дисциплины 56 (час.)

Составитель: Черенцова Д.А.

2020 г

Рабочая программа составлена на основании Федерального государственного образовательного стандарта среднего профессионального образования по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом министерства образования и науки Российской Федерации от 09.12.2016 N 1551.

Рабочая программа обсуждена на заседании ЦМК дисциплин технического профиля

«12» 05 _____ 2020 г. протокол № 9

Председатель ЦМК Лобань Новомлинцева Н.А.

СОГЛАСОВАНО
Зам. декана по учебной работе
А.А. Санова
«27» 05 2020 г.

СОГЛАСОВАНО
с научной библиотекой
И.В. Петрова
«28» 05 2020 г.

1. Область применения программы

Рабочая программа учебной дисциплины является частью ППССЗ по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

2. Место учебной дисциплины в структуре образовательной программы:

учебная дисциплина ОП.04. Основы информационной безопасности относится к группе общепрофессиональных дисциплин профессиональной подготовки, читается в 3 семестре в объеме 56 часов.

3. Показатели освоения учебной дисциплины:

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

Код	Наименование результата обучения
Общие компетенции	
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
Профессиональные компетенции	
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.
ПК 1.4.	Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей.
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.

ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.
ПК 3.3	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

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

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

- 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;

- 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.

4. Тематический план и содержание учебной дисциплины ОП.04. Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание учебного материала		2
	1	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		2, 3
	1	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.	
	Практические занятия		
	1	Определение объектов защиты на типовом объекте информатизации.	2
	2	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2
	Самостоятельная работа		
	Доклад на тему: «Понятие Политики безопасности»		1
Тема 1.3. Угрозы безопасности защищаемой информации.	Содержание учебного материала		2, 3
	1	Понятие угрозы безопасности информации Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации	

	Уязвимости. Методы оценки уязвимости информации		
	Практическое занятие		
	1 Определение угроз объекта информатизации и их классификация	4	2, 3
	Самостоятельная работа		
	Доклад по теме: «Методы оценки уязвимости информации»	1	
Раздел 2. Методология защиты информации			
Тема 2.1. Методологические подходы к защите информации	Содержание учебного материала		2, 3
	1 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.	2	
	Самостоятельная работа		
	Доклад по теме: «Виды мер и основные принципы защиты информации»	1	
Тема 2.2. Нормативно правовое регулирование защиты информации	Содержание учебного материала		2, 3
	1 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	2	
		2	
		2	
	Практическое занятие		
	1 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	4	2, 3
	Самостоятельная работа		
	1 Доклад по теме: «Законодательные акты в области защиты информации»	1	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала		2, 3
	1 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	2	
		2	
		2	

	Практическое занятие			
1	Выбор мер защиты информации для автоматизированного рабочего места		4	2, 3
	Самостоятельная работа			
1	Реферат по теме: «Инженерная защита и техническая охрана объектов информатизации»		1	
2	Подготовка к экзамену		1	
Промежуточная аттестация			6	
Итого			56	

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)

5. Образовательные технологии

Результаты освоения дисциплины достигаются за счет использования в процессе обучения современных инструментальных средств: лекции с применением мультимедийных технологий.

При проведении занятий используются активные и интерактивные формы. В таблице приведен перечень образовательных технологий и методов, используемых в данной дисциплине.

Тип занятия	Практическая работа
Методы/формы	
Разбор конкретной ситуации	Определение угроз объекта информатизации и их классификация

6. Требования к минимальному материально-техническому обеспечению:

Занятия проводятся в компьютерном классе

Оснащение: Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, доска, мультимедиа-проектор, проекционный экран, ПК.

7. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основные источники:

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-07979-1. — Режим доступа : www.biblio-online.ru/book/1997F695-44FF-4570-BF5D-882F5286AE77.

2. Бубнов А. А. Основы информационной безопасности : учебник для СПО / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин – 1-е изд. - М.: Академия, 2018. - 256 с. - Режим доступа: <http://www.academia-moscow.ru/reader/?id=302888>

Дополнительные источники:

1. Белов Е.Б. , Пржегорлинский В. Н. Организационно-правовое обеспечение информационной безопасности: учебник для СПО. - М.: Академия, 2017. - 336 с. - Режим доступа: <http://www.academia-moscow.ru/reader/?id=293834>

2. Основы информационной безопасности: сб. учеб.- метод. материалов для специальности: 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем. / АмГУ, ФСПО; сост. С.А. Панов. – Благовещенск: Изд-во Амур.гос. ун-та, 2018. - 15с. Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10133.pdf

Перечень программного обеспечения

Операционная система WindowsServer 2008 - DreamSparkPremiumElectronicSoftwareDelivery (3 years) Renewal по договору - Сублицензионный договор № Tr000074357/КНВ 17 от 01 марта 2016 года, Операционная система MS Windows XP SP3 - DreamSparkPremiumElectronicSoftwareDelivery (3 years) Renewal по договору - Сублицензионный договор № Tr000074357/КНВ 17 от 01 марта 2016 года

8. Контроль и оценка результатов освоения учебной дисциплины

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения теоретических, практических и лабораторных занятий, а также выполнения обучающимися различных индивидуальных заданий.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
Освоенные умения:	
- классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации;	Устный опрос, реферат, практическая работа,

	самостоятельная работа
Усвоенные знания:	
<ul style="list-style-type: none"> - 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; 	Устный опрос, реферат, практическая работа, самостоятельная работа
Промежуточная аттестация: экзамен	Экзамен – 3 семестр

ОП.04 Основы информационной безопасности изучается на протяжении 3 семестра. Итоговой оценкой по ОП.04 Основы информационной безопасности считать оценку за 3-ий семестр

Вопросы к экзамену 3 семестр

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

18. Российские и международные стандарты, определяющие требования к защите информации.
19. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации
20. Основные механизмы защиты информации. Система защиты информации.
21. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
22. Программные и программно-аппаратные средства защиты информации
23. Инженерная защита и техническая охрана объектов информатизации
24. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим.
25. Принципы построения организационно-распорядительной системы