МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова

УТВЕРЖДАЮ
Первый проректор
_____ И.Г. Гайрабеков
«_25_» _____01_____ 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 «Основы информационной безопасности»

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация

техник по защите информации

Грозный – 2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП 01 Основы информационной безопасности»

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.01 Основы информационной безопасности является обязательной частью общепрофессионального цикла ОПОП в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Особое значение дисциплина имеет при формировании и развитии ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.2, ПК 2.4

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ПК 1.3 ПК 1.4 ПК 2.1 ПК 2.2 ПК 2.4	настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; применять программные и программно-аппаратные средства для защиты информации в базах	порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

	данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись	типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
ОК 02, ОК 09	определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; **п**рименять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение.	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы учебной дисциплины	122
в т.ч. в форме практической подготовки	
в т. ч.:	
теоретическое обучение	48
лабораторные работы	-
практические занятия	48
курсовая работа (проект)	-
Самостоятельная работа	16
Промежуточная аттестация	**10**

2.2. Тематический план и содержание учебной дисциплины

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		**56/24**	
Тема 1.1. Основные понятия и задачи информационной безопасности	**Теоретические занятия**	**8**	
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	4	ОК 02, ОК 09, ПК 2.1
	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 не информированности в области информационной безопасности.	4	ОК 02, ОК 09, ПК 1.3
	Практические занятия	**8**	
	1. Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты	4	ОК 02, ОК 09, ПК 1.3, ПК 1.4
	2. Реализация политик информационной безопасности. Дискреционная модель политики безопасности	2	ОК 02, ОК 09, ПК 1.3, ПК 1.4
	3. Реализация и исследование политик информационной безопасности. Мандатная модель политики безопасности	2	ОК 02, ОК 09, ПК 1.3, ПК 1.4
	Самостоятельная работа обучающихся	**8**	
	1. Контроль целостности информации. Электронно-цифровая подпись 2. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей 3. Правовое обеспечение информационной безопасности 4. Классификация политик безопасности	*8*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.2, ПК 2.4
	Теоретические занятия	**8**	

Тема 1.2. Основы защиты информации	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	*4*	ОК 02, ОК 09, ПК 2.1, ПК 2.4
	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.	*2*	ОК 02, ОК 09, ПК 2.1, ПК 2.4
	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	*2*	ОК 02, ОК 09, ПК 2.1, ПК 2.4
	Практические занятия	**8**	
	1. Определение объектов защиты на типовом объекте информатизации.	*4*	ОК 02, ОК 09, ПК 2.4
	2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	*4*	ОК 02, ОК 09, ПК 2.4
	Самостоятельная работа обучающихся	-	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Теоретические занятия**	**8**	
	Понятие угрозы безопасности информации	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Системная классификация угроз безопасности информации.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Каналы и методы несанкционированного доступа к информации	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Уязвимости. Методы оценки уязвимости информации	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Практическое занятие	**8**	
	1. Определение угроз объекта информатизации и их классификация	*4*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	2. Реализация и исследование политик информационной безопасности	*4*	ОК 02, ОК 09,

			ПК 1.3, ПК 1.4, ПК 2.1
	Самостоятельная работа обучающихся	-	
Раздел 2. Методология защиты информации		**56/24**	
Тема 2.1. Методологические подходы к защите информации	**Теоретические занятия**	**8**	
	Анализ существующих методик определения требований к защите информации.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Виды мер и основные принципы защиты информации.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.2
	Практическое занятие	**12**	
	1. Методы криптографической защиты информации. Традиционные симметричные криптосистемы	*6*	ОК 02, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.2
	2. Элементы криптоанализа. Оценка частотности символов в тексте	*6*	ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.2
	Самостоятельная работа обучающихся	-	
Тема 2.2. Нормативно правовое регулирование защиты информации	**Теоретические занятия**	**8**	
	Организационная структура системы защиты информации	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1
	Законодательные акты в области защиты информации.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.4
	Российские и международные стандарты, определяющие требования к защите информации.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.4

	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.4
	Практическое занятие	**8**	
	1. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	*4*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.4
	2. Симметричные и асимметричные криптосистемы. Электронно-цифровая подпись	*4*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.4
	Самостоятельная работа обучающихся	**-**	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Теоретические занятия**	**8**	
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 2.1, ПК 2.2, ПК 2.4
	Программные и программно-аппаратные средства защиты информации	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.2, ПК 2.4
	Инженерная защита и техническая охрана объектов информатизации	*2*	ОК 09, ПК 1.3, ПК 1.4, ПК 2.1, ПК 2.4
	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	*2*	ОК 02, ОК 09, ПК 1.3, ПК 1.4, ПК 2.4
	Практическое занятие	**4**	
	Выбор мер защиты информации для автоматизированного рабочего места	*4*	ОК 02, ОК 09, ПК 1.3, ПК 1.4
	Самостоятельная работа обучающихся	**8**	
	1. Идентификация и аутентификация субъектов 2. Базовые механизмы безопасности коммутаторов 3. Безопасность на основе сегментации трафика	*8*	ОК 02, ОК 09, ПК 1.3, ПК 1.4,

	4. Компьютерные средства реализации защиты в информационных системах		ПК 2.1, ПК 2.2, ПК 2.4
Промежуточная аттестация по учебной дисциплине		***10***	
Всего		***122***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Кабинет «Нормативного правового обеспечения информационной безопасности», оснащенный в соответствии с п. 6.1.2.1 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет электронные образовательные и информационные ресурсы для использования в образовательном процессе.

3.2.1. Основные электронные издания

1. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 236 с. — ISBN 978-5-4497-0535-8. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/95150.

2. Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1 : учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 171 с. — ISBN 978-5-9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/107943.

3. Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : Новосибирский государственный технический университет, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/91329.

4. Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/118458.

3.2.2. Дополнительные источники

1. Бахаров, Л. Е. Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л. Е. Бахаров. — Москва : Издательский Дом МИСиС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/98171.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	*Критерии оценки*	*Формы и методы оценки*
– 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.	**Критерии оценивания рубежной аттестации:** **Аттестован** - выставляется обучающемуся, ответившему правильно на 6-20 вопросов. **Не аттестован** - выставляется обучающемуся, который ответил менее 5 вопроса. **Критерии оценивания зачета/экзамена:** **Зачтено** - выставляется обучающемуся, ответившему правильно на 11 вопросов. **Не зачтено** - выставляется обучающемуся, который ответил 10 и менее вопроса. **Отлично** - выставляется обучающемуся, ответившему на 31-40 вопросов. **Хорошо** - выставляется обучающемуся, ответившему на 21-30 вопросов. **Удовлетворительно** - выставляется обучающемуся, ответившему на 11 и более вопросов.	Рубежная аттестация Экзамен
– классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации;		

Разработчик:

Преподаватель ФСПО _____ / Н.В.Асламбекова /
(подпись)

Согласовано:

Председатель ПЦК «Информационные технологии»

_____ / И.М.Дубаев/
(подпись)

Зам. декана по МР ФСПО _____ / И.В.Сулейманова/
(подпись)

Директор ДУМР _____ / М.А. Магомаева/
(подпись)