МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ХАБАРОВСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ХАБАРОВСКИЙ ТЕХНИКУМ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.21 Основы информационной безопасности

Форма обучения
очная

очная, заочная, очно-заочная

09.02.06 Сетевое и системное администрирование

Хабаровск

2024 г.

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) **на базе основного общего образования** по специальности среднего профессионального образования (далее СПО 09.02.06 «Сетевое и системное администрирование».

Организация-разработчик: КГБ ПОУ «Хабаровский техникум техносферной безопасности и промышленных технологий»

Разработчики:

Иващенко Л.В. –преподаватель спецдисциплин

Методист Лазукова С. А.

Рассмотрено и одобрено на заседании ПЦК «Информатика и вычислительная техника»

Протокол №__от « __»_____20_____г.

Председатель ПЦК_____(_____).

Согласовано на заседании методического совета

Протокол № _____ от «____»_____202 г.

Председатель МС _____ (_____).

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ Основы информационной безопасности

1.1. Область применения примерной программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности **09.02.06 Сетевое и системное администрирование.**

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина входит в профессиональный цикл как общепрофессиональная дисциплина.

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

Цель рабочей программы учебной дисциплины:

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

- Формулировать тему, проблему, ставить цель и задачи, обосновывать актуальность проблемы, определять гипотезу, доказывать или опровергать ее.
- Изготовлять продукт исследовательской деятельности.
- Составлять содержание работы и план своих действий на каждом этапе.
- Составлять структуру своего исследования.
- Проводить исследование и делать вывод по его результатам.
- Работать с различными источниками информации, используя разные формы защиты информации.
- Выявлять вирусы.
- Использовать современные средства защиты информации.

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

- Современные методы защиты информации;
- Основные виды угроз;
- Виды продуктов вирусов;
- Формы защиты информации в сети ЭВМ;
- Требования к защите информации, критерии оценки угроз.

В результате освоения дисциплины формируются компоненты следующих *профессиональных компетенций* обучающегося*:*

ПК 3.3. осуществлять защиту информации в сети с использованием программно-аппаратных средств.

В результате освоения учебной дисциплины студент, должен обладать следующими общими компетенциями

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.

В результате процессе изучения дисциплин достигаются следующие личностные результаты

Личностные результаты реализации программы воспитания *(дескрипторы)*	Код личностных результатов
Осознающий себя гражданином и защитником великой страны	**ЛР 1**
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России	**ЛР 2**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России	**ЛР 3**
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания	**ЛР 4**
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля	**ЛР 5**
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение	**ЛР 6**
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость	**ЛР 7**
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности	**ЛР 8**
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности»	**ЛР 9**
Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый	**ЛР 10**

оказать поддержку нуждающимся	
Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением	**ЛР 11**
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих	**ЛР 12**

1.4. Количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 66 часов,

в том числе: обязательной аудиторной учебной нагрузки обучающегося 64 часа;

практических занятий 30 часов;

Самостоятельная работа – 2 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Объем образовательной нагрузки	**66**
Всего учебных занятий	**64**
в том числе:	
Лекции, уроки	32
практические занятия	30
самостоятельная работа	2
Промежуточная аттестация в форме: дифференцированный зачёт	**3 семестр**

2.1. Тематический план и содержание учебной дисциплины: Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лекции и практические занятия, самостоятельная работа обучающихся.	Объем часов	Уровень освоения	ОК, ПК, ЛР
1	2	3	4	
Раздел 1.	**Общие вопросы информационный безопасности.**			
Тема 1.1. Международные стандарты информационного обмена	**Содержание учебного материала**	**2**	**1**	
	1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. 2. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная.			ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	Практические занятия: Защита документооборота в вычислительных системах	2	**2**	
Тема 1.2 Понятия и угрозы.	**Содержание учебного материала**	**2**	**1**	
	1. Основные понятия. Механизмы безопасности. Классы безопасности. 2. Основные определения и критерии классификации угроз			ОК01, 02, 05, 09
	Практическая работа Криптографические методы защиты	2	**2**	ПК 3.3 ЛР 1-12
Раздел 2.	**Государственная система информационной безопасности**			
Тема 2.1	**Содержание учебного материала**	**4**	**1**	
Информационная безопасность в условиях функционирования в России глобальных сетей.	1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.			ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	Практические занятия: Шифрование методом IDEA	**2**	**2**	

Раздел 3.	**Угрозы безопасности**			
Тема 3.1 Угрозы безопасности.	**Содержание учебного материала**	**2**		ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	1. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения 2. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации		**1**	
	Практические занятия: Шифрование методом RC6	**2**	**2**	
Раздел 4.	**Теоретические основы методов защиты информационных систем**			
Тема 4.1 Теоретические основы методов защиты информационных систем	**Содержание учебного материала**	**4**		ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	1. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности 2. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла- ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей		**1**	
	Практические занятия: Шифрование методом SAFER K-64	**2**	**2**	
Раздел 5.	**Методы защиты средств вычислительной техники**			
Тема 5.1 Методы защиты средств вычислительной техники	**Содержание учебного материала**	**2**	**1**	ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	1. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. 2. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.			
	Практические занятия: Криптосистема Эль-Гамаля	**4**	**2**	

Раздел 6.	**Основы криптографии**			
Тема 6.1	**Содержание учебного материала**	**4**	**1**	
Основы криптографии	1. Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. 2. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы.			ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	Практические занятия Шифрование методом Вернам	**4**	**2**	
Раздел 7.	**Архитектура защитных экономических систем**			
Тема 7.1 Архитектура защитных экономических систем	**Содержание учебного материала**			
	1. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. 2. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.	**4**	**1**	ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	Практические занятия Шифрование методом аналитических преобразований	**4**	**2**	
Раздел 8.	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**			
Тема 8.1 Алгоритмы и привязки программного обеспечения к аппаратному окружению	**Содержание учебного материала**	**4**	**1**	
	1. Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. 2. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода			ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	Практические занятия Сокрытие информации методом стеганографии	**4**	**2**	
	Самостоятельная работа обучающегося: 1. Презентация на тему «Технология spyware» 2. Составить алгоритм программного обеспечения	**2**	**3**	

Раздел 9.	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**			
Тема 9.1 Алгоритмы безопасности в компьютерных сетях	**Содержание учебного материала**	**2**	**1**	
	1. Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. 2. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.			ОК01, 02, 05, 09 ПК 3.3 ЛР 1-12
	Практические занятия Сокрытие информации методом стеганографии	**4**	**2**	
ИТОГО		**64**		
САМОСТОЯТЕЛЬНАЯ РАБОТА		**2**		
ВСЕГО		**66**		

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 учебного кабинета.

Оборудование учебного кабинета:
- сетевой компьютерный класс с выходом в Интернет;
- комплекты «столы-стулья» (2 к 1) в количестве не менее 15 шт.;
- шкафы для методической литературы;
- огнетушитель;
- информационные стенды

Технические средства обучения:
- интерактивная доска;
- проектор;
- компьютерное рабочее место для преподавателя;
- принтер;
- сканер.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, интернет ресурсов, дополнительной литературы

Основные источники:

1) Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; под редакцией С. М. Молявко ; перевод с английского В. Д. Хорева. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 482 с. — ISBN 978-5-00101-700-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151552 (дата обращения: 24.06.2024). — Режим доступа: для авториз. пользователей.

2) Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие / В. И. Васильев. — 3-е изд., стереотип. — Москва : Машиностроение, 2021. — 172 с. — ISBN 978-5-907104-99-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/192986 (дата обращения: 24.06.2024). — Режим доступа: для авториз. пользователей.

Дополнительные источники:

1) Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2012.

2) Соколов А. В., Степанюк О. М. Защита от компьютерного терроризма. Справочное пособие. - СПб.: БХВ - Петербург, Арлит, 2012.- 496с.:ил.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения
Программа составлена в соответствии с требованиями ФГОС СПО для специальностей технического профиля

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
уметь: • Формулировать тему, проблему, ставить цель и задачи, обосновывать актуальность проблемы, определять гипотезу, доказывать или опровергать ее. • Изготовлять продукт исследовательской деятельности. • Составлять содержание работы и план своих действий на каждом этапе. • Составлять структуру своего исследования. • Проводить исследование и делать вывод по его результатам. • Работать с различными источниками информации, используя разные формы защиты информации. • Выявлять вирусы. • Использовать современные средства защиты информации.	Выполнение и защита заданий по практическим работам. Экспертное оценивание выполнения практических работ и самостоятельной работы
знать: • Современные методы защиты информации; • Основные виды угроз; • Виды продуктов вирусов; • Формы защиты информации в сети ЭВМ; Требования к защите информации, критерии оценки угроз	