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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

уровень образования *основное общее образование*

Форма обучения *очная*

09.02.07 Информационные системы и программирование

Хабаровск 2020

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности **09.02.07 Информационные системы и программирование на базе основного общего образования**

Организация-разработчик: КГБ ПОУ «Хабаровский техникум техносферной безопасности и промышленных технологий»
Разработчики:
Иващенко Л.В. –преподаватель спец.дисциплин высшей категории

Рассмотрено и одобрено на заседании ПЦК «Информатика и Вычислительная техника»
Протокол № _____ от «____»_____20_____г.

Председатель ПЦК _____ (_____).

Согласовано на заседании методического совета
Протокол № _____ от «____» _____20_____г.
Председатель МС _____ (_____).

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ Основы информационной безопасности

1.1 Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности Информационные системы и программирование.

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:

Код ПК, ОК	Умения	Знания
ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10,	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 каждомэтапе. Составлять структуру своегоисследования. 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	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

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.

- 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 оказать поддержку нуждающимся	ЛР 10
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
Способный в цифровой среде использовать различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	ЛР 13
Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и	ЛР 16

чужое деструктивное поведение в сетевом пространстве .	
Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению	ЛР 17
Осознающий значимость системного познания мира, критического осмысления накопленного опыта	ЛР 18
Развивающий творческие способности, способный креативно мыслить	ЛР 19
Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации	ЛР 20
Готовый к профессиональной конкуренции и конструктивной реакции на критику	ЛР 21
Самостоятельный и ответственный в принятии решений во всех сферах своей дея-тельности, готовый к исполнению разнообразных социальных ролей, востребован-ных бизнесом, обществом и государством	ЛР 23
Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики	ЛР 34

1.4. Количество часов на освоение программы дисциплины:
максимальная учебная нагрузка обучающегося 72 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 64 часов;

самостоятельной работы обучающегося 2часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Объем образовательной нагрузки	**72**
Всего учебных занятий	**64**
в том числе:	
лекции	32
практические занятия	30
консультации	2
экзамен	6
самостоятельная работа	2
Промежуточная аттестация в форме: экзамена	**4 семестр**

2.1. Тематический план и содержание учебной дисциплины: Информационная безопасность и защита информации

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	5
Раздел 1.	**Общие вопросы информационный безопасности.**			ОК 1-6 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
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 автораи 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.			
	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			
	Практическая работа Криптографические методы защиты	2	**2**	
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 2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензированиеи сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.			ОК 1-6 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23

	Практические занятия: Шифрование методом IDEA	2	2	
Раздел 3.	**Угрозы безопасности**			ОК 1-6 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
Тема 3.1 Угрозы безопасности.	**Содержание учебного материала**	**2**	**1**	
	1. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основныенарушения 2. Характер происхождения угроз (умышленные и естественные факторы).Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного полученияинформации			
	Практические занятия: Шифрование методом RC6	2	2	
Раздел 4.	**Теоретические основы методов защиты информационных систем**			ОК 1-6 ОК 9, 10 ЛР 1-12 ЛР 13, 16-23
Тема 4.1 Теоретические основы методов защиты информационных систем	**Содержание учебного материала**	**4**	**1**	
	1. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные моделибезопасности 2. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрицадоступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла- ЛаПадулы. Ролевая политика безопасности. Ограничения на областиприменения формальных моделей			
	Практические занятия: Шифрование методом SAFER K-64	2	2	
Раздел 5.	**Методы защиты средств вычислительной техники**			ОК 1-6 ОК 9, 10 ЛР 1-12 ЛР 13, 16-23
Тема 5.1 Методызащиты средств вычислительной техники	**Содержание учебного материала**	**2**	**1**	
	1. Использование защищенных компьютерных систем. Аппаратные ипрограммные средства для защиты компьютерных систем отНСД. 2. Средства операционной системы. Средства резервирования данных.Проверка целостности. Способы и средства восстановленияработоспособности.			
	Практические занятия: Криптосистема Эль-Гамаля	4	2	

Раздел 6.	**Основы криптографии**			ОК 1-6 ОК 9, 10 ЛР 1-12 ЛР 13, 16-23
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.			
	Практические занятия Шифрование методом Вернам	4	**2**	
Раздел 7.	**Архитектура защитных экономических систем**			ОК 1-6 ОК 9, 10 ЛР 1-12 ЛР 13, 16-23
Тема 7.1 Архитектура защитных экономических систем	**Содержание учебного материала**	**4**	**1**	
	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.			
	Практические занятия Шифрование методом аналитических преобразований	4	**2**	
Раздел 8.	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**			ОК 1-6 ОК 9, 10 ЛР 1-12 ЛР 13, 16-23
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 (trialversion). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода			
	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**			ОК 1-6 ОК 9, 10 ЛР 1-12 ЛР 13, 16-23
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.			
	Практические занятия Сокрытие информации методом стеганографии	**4**	**2**	
ИТОГО		**64**		
САМОСТОЯТЕЛЬНАЯ РАБОТА		**2**		
ЭКЗАМЕН		**6**		
ВСЕГО		**72**		

Для характеристики уровня освоения учебного материала используются следующие обозначения: 1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или подруководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемныхзадач)

2 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙДИСЦИПЛИНЫ

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 15шт.;
- шкафы для методической литературы;
- огнетушитель;
- информационны естенды

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) Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. : БИНОМ, 2017. - (Программисту). - http://www.studentlibrary.ru/book/ISBN9785996329526.html

Электронное издание на основе: Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ.-3-е изд. (эл.).-Электрон. текстовые дан. (1 файл pdf : 482 с.).- М. : БИНОМ. Лаборатория знаний, 2015.- (Программисту).-Систем. требования: AdobeReader XI ; экран 10". - ISBN 978-5-9963-2952-6.

2) Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. -М.:

Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html

Электронное издание на основе: Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN978-5-94275-667-3.

3) Информатика 2015 [Электронный ресурс] : учебное пособие / Алексеев А.П. - М. : СОЛОН-ПРЕСС, 2015. - http://www.studentlibrary.ru/book/ISBN9785913591586.html

Электронное издание на основе: Информатика 2015: учебное пособие/ Алексеев А.П.- 2015. - 400 с., илл. - ISBN 978-5-91359-158-6.

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.

3. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины: 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	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Примеры форм и методов контроля и оценки • Компьютерное тестирование на знание терминологии по теме; • Тестирование…. • Контрольная работа …. • Самостоятельная работа. • Защита реферата…. • Семинар • Выполнение проекта; • Наблюдение за выполнением практического задания. (деятельностью студента) • Оценка выполнения практического задания(работы) • Подготовка и выступление с докладом, сообщением, презентацией… • Решение ситуационной задачи….
Перечень умений, осваиваемых в рамках дисциплины: 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. Выявлятьвирусы. Использовать современные средства защитыинформации		