АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

УТВЕРЖДАЮ

ДИРЕКТОР АНО ПО «БИТ»

В.В. СЕРГЕЕВ

«31» августа 2020 ГОДА

М.П.

ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК.02.02 «Криптографические средства защиты информации

Калининград 2020

Программа междисциплинарного курса разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1553 и примерной основной образовательной программы СПО, разработанной ФУМО 2017 г.

Организация-разработчик: Автономная некоммерческая организация профессионального образования «Балтийский информационный техникум».

Разработчик: _____ Шафикова А.Л., преподаватель математики

Рассмотрена
на заседании цикловой методической
комиссии №1, протокол № 1
от «31» августа 2020 г.
председатель ЦМК

_____ О.О. Васильева

«31» августа 2020 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МДК 02.02 «Криптографические средства защиты информации»

1.1. Место МДК в структуре основной профессиональной образовательной программы.

Программа МДК.02.02 «Криптографические средства защиты информации» является частью профессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

В результате изучения МДК студент должен освоить основной вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему общие и профессиональные компетенции

1.1.1. Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами**
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.

1.1.3. В результате освоения МДК студент должен:

Иметь практический опыт	– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
Уметь	– применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись
Знать	– основные понятия криптографии и типовых криптографических методов и средств защиты информации

1.2. Количество часов, отводимое на освоение МДК

Всего 170 часов, из них:

на освоение МДК – 146 часов, в том числе

на промежуточную аттестацию по МДК –12 часов,

на лабораторные и практические занятия – 74 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ МДК 02.02 «Криптографические средства защиты информации»

2.1. Объем МДК и виды учебной работы

Индекс	Наименование	Объем образовательной программы в академических часах							
		Всего объем образовательной программы	Работа обучающихся во взаимодействии с преподавателем				Самостоятельная работа	Практики	
			Занятия по дисциплинам и МДК			Теоретическое обучение		Учебная	Производственная
			Всего	в том числе					
				лабораторные и практические занятия	курсовой проект (работа)				
1	2	3	4	5	6	7	8	9	
ПМ.00	**Профессиональный цикл**								
ПМ. 02	**Защита информации в автоматизированных системах программными и программно-аппаратными срелствами**								
МДК.02.01	Программные и программно-аппаратные средства защиты информации								
МДК.02.02	Криптографические средства защиты информации	**170**	**146**	**74**		**72**	**12**		

2.2. Тематический план и содержание МДК

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося	Объем часов	Уровень освоения	Коды профессиональных и общих компетенций
1	2	3	4	5
Раздел 2 модуля. Применение криптографических средств защиты информации		**170**		ПК 2.4 ОК 1-ОК 10
МДК.02.02. Криптографические средства защиты информации		**146**		
Введение	**Содержание**	**4**		ПК 2.4 ОК 1-ОК 10
	Предмет и задачи криптографии. Основные понятия.	2	*1*	
	История криптографии.	2	*2*	
Раздел 1. Математические основы защиты информации		**34**		ПК 2.4 ОК 1-ОК 10
Тема 1.1. Математические основы криптографии	**Содержание**	**18**		
	1. Основные алгебраические структуры, применяемые в криптографии	2	*1*	
	2. Делимость чисел. Алгоритм Евклида нахождения НОД двух чисел.	2	*2*	
	3. Отношения сравнимости. Модулярная арифметика.	2	*2*	
	4. Функция Эйлера. Алгоритм быстрого возведения в степень по модулю.	2	*2*	
	5. Классы вычетов. Таблицы Кэли. Мультипликативная группа Z_n^x.	2	*2*	
	6. Сравнения 1-й степени. Китайская теорема об остатках.	2	*2*	
	7. Проверка чисел на простоту. Алгоритмы генерации простых чисел.	2	*2*	
	8. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2	*2*	
	9. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2	*2*	
	Тематика практических занятий и лабораторных работ	**16**		
	1. Применение теоремы о делении с остатком. Каноническое разложение числа на простые множители.	2		
	2. Применение алгоритма Евклида для нахождения НОД двух чисел.	2		

	3. Решение задач на отношение сравнимости и свойства сравнений.	2		
	4. Вычисление значений функции Эйлера.	2		
	5. Нахождение обратного элемента в кольце классов вычетов.	2		
	6. Решение сравнений 1-й степени.	2		
	7. Проверка чисел на простоту.	2		
	8. Программная реализация базовых алгоритмов, применяемых в криптографии.	2		
Раздел 2. Классическая криптография		**32**		
Тема 2.1. Методы криптографической защиты информации	**Содержание**	**6**		
	Шифры замены.	2	*2*	
	Шифры перестановки.	2	*2*	
	Гаммирование.	2	*2*	
	Тематика практических занятий и лабораторных работ	**10**		
	Применение классических шифров простой замены.	2		
	Применение простейших блочных шифров.	2		
	Применение классических шифров перестановки.	2		
	Применение шифров маршрутной перестановки.	2		
	Применение метода гаммирования.	2		
Тема 2.2. Криптоанализ	**Содержание**	**4**		ПК 2.4 ОК 1-ОК 10
	Основные методы криптоанализа. Принципы Киркхоффса	2	*1*	
	Перспективные направления криптоанализа.	2	*1*	
	Тематика практических занятий и лабораторных работ	**6**		
	Криптоанализ шифра простой замены методом частотного анализа.	2		
	Криптоанализ классических шифров методом полного перебора ключей.	2		
	Криптоанализ шифра Виженера.	2		
Тема 2.3. Поточные шифры и генераторы	**Содержание учебного материала**	**4**		
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.	2	*1*	
	Методы получения псевдослучайных последовательностей: ЛКГ, метод	2	*2*	

псевдослучайных чисел	Фибоначчи, метод BBS.			
	Тематика практических занятий и лабораторных работ	**2**		
	Применение методов генерации ПСЧ	2		
Раздел 3. Современная криптография		**74**		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**4**		
	Кодирование информации. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	2	*1*	
	Компьютеризация шифрования. Аппаратное и программное шифрование. Стандартизация программно-аппаратных криптографических систем и средств.	2	*1*	
	Тематика практических занятий и лабораторных работ	**6**		
	Кодирование информации	2		
	Программная реализация классических шифров замены	2		
	Программная реализация классических шифров перестановки	2		
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**8**		ПК 2.4 ОК 1-ОК 10
	Принципы построения блочных шифров. Сеть Фейстеля.	2	*1*	
	Американские стандарты шифрования данных DES, AES. Российский стандарт ГОСТ 28147-89.	2	*1*	
	Отечественные алгоритмы Магма и Кузнечик. Стандарты ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.	2	*1*	
	Режимы использования блочных шифров	2	*3*	
	Тематика практических занятий и лабораторных работ	**4**		
	Изучение программной реализации современных симметричных шифров	2		
	Изучение программной реализации современных симметричных шифров	2		
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**4**		
	Криптосистемы с открытым ключом. Понятие односторонней функции. Шифрсистема RSA.	2	*2*	
	Шифры Шамира и Эль-Гамаля.	2	*2*	

	Тематика практических занятий и лабораторных работ	**10**		
	Реализация шифра Шамира.	2		
	Реализация шифра Эль-Гамаля.	2		
	Реализация алгоритма RSA	2		
	Применение метода «Шаг младенца-шаг великана» для решения проблемы дискретного логарифма	2		
	Программная реализация метода взлома шифров «Шаг младенца-шаг великана»	2		
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**6**		
	Аутентификация данных. Электронная подпись. Хэш-функции.	2	*1*	
	Электронная подпись RSA. Электронная подпись на базе шифра Эль-Гамаля	2	*2*	
	Стандарты на электронную подпись	2	*2*	
	Тематика практических занятий и лабораторных работ	**10**		
	Применение различных функций хеширования, анализ особенностей хешей	2		
	Применение криптографических атак на хеш-функции.	2		
	Генерация и проверка ЭП RSA.	2		
	Генерация и проверка ЭП Эль-Гамаля.	2		
	Применение стандартов на электронную подпись	2		
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**2**		
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Алгоритм Диффи-Хеллмана для обмена ключами шифрования.	2	*2*	
	Тематика практических занятий и лабораторных работ	**2**		
	Применение алгоритма Диффи-Хеллмана для обмена ключами шифрования.	2		
Тема 3.6. Криптозащита информации в сетях передачи	**Содержание учебного материала**	**4**		
	Абонентское, пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр.	2	*2*	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с	2	*2*	

данных	использованием протоколов WPA, WEP.			
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	**4**		
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	2	*1*	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2	*2*	
	Тематика практических занятий и лабораторных работ	**4**		
	Применение аутентификации по одноразовым паролям.	2		
	Реализация алгоритмов создания одноразовых паролей.	2		
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**4**		
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	2	*1*	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.	2	*2*	
	Тематика практических занятий и лабораторных работ	**4**		
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	2		
	Реализация простейших стеганографических алгоритмов	2		
Примерная тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Криптография в России 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Методы механизации шифрования 5. Цифровое представление различных форм информации 6. Анализ современных симметричных криптоалгоритмов 7. Сравнительный анализ функций хеширования 8. Криптосистемы на эллиптических кривых 9. Законодательство в области криптографической защиты информации 10. Перспективные направления криптографии				ПК 2.4 ОК 1-ОК 10

Промежуточная аттестация по МДК.02.02	**12**		ПК 2.4 ОК 1-ОК 10
Примерные виды самостоятельной работы при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	**12**		ПК 2.4 ОК 1-ОК 10
Всего:	**170**		

Для характеристики уровня усвоения 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).

6. Рябко Б. Я., Фионов Ф. Н. Криптографические методы защиты информации (учебное пособие). – М., 2005.

3.2.4. Электронные издания (электронные ресурсы):

1. Сикорская, Г. А. Алгебра и теория чисел: учебное пособие для СПО / Г. А. Сикорская. — Саратов: Профобразование, 2020. — 303 с. — ISBN 978-5-4488-0612-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/91847.html
2. Белаш, В. Ю. Основы теории информации: учебно-методическое пособие для СПО / В. Ю. Белаш. — Саратов: Профобразование, 2019. — 45 с. — ISBN 978-5-4488-0284-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/84442.html
3. Гультяева, Т. А. Основы теории информации и: конспект лекций / Т. А. Гультяева. — Новосибирск: Новосибирский государственный технический университет, 2010. — 88 с. — ISBN 978-5-7782-1425-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/44987.html
4. https://www.studmed.ru/science/informatics/informacionnaya-bezopasnost/kriptologiya-i-kriptografiya/history
5. https://www.studmed.ru/science/informatics/informacionnaya-bezopasnost/kriptologiya-i-kriptografiya/methods
6. https://www.studmed.ru/science/informatics/informacionnaya-bezopasnost/kriptologiya-i-kriptografiya/kriptologiya

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МДК 02.02 «Криптографические средства защиты информации»

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

Лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- комплект обучающего материала (комплект презентаций).

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- рабочее место преподавателя;
- учебно-методическое обеспечение МДК;
- комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

3.2. Информационное обеспечение реализации программы

Библиотечный фонд в виде печатных изданий и доступа к электронно-библиотечной системе **ipr.books**, кроме того, в процессе освоения программы профессионального модуля студенты имеют возможность доступа к электронным учебным материалам, имеющимся в свободном доступе в сети Интернет.

3.2.1 Печатные издания:

1. Ерохин В.В. Информационная безопасность для СПО. Учебник. - СПб.: ООО «Диалектика», 2018.
2. Масачков А.С. Особенности киберпреступлений в России. - СПб.: ООО «Альфа – книга», 2018.
3. Нестеров, С.А. Информационная безопасность: учебник и практикум для СПО. - М.: Издательство «ЮРАЙТ», 2019. – 350 с.
4. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности
5. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учебное пособие. – М.: Горячая линия – Телеком, 2007.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК 02.02 «Криптографические средства защиты информации»

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде,	- взаимодействие с обучающимися,	

эффективно взаимодействовать с коллегами, руководством, клиентами.	преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной	- эффективность использования информационно-коммуникационных	

деятельности.	технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	