Комитет образования, науки и молодежной политики Волгоградской области
Государственное бюджетное профессиональное образовательное учреждение
«Волжский политехнический техникум»

УТВЕРЖДЕНО
на заседании Методического
совета техникума
Протокол № 7 от «09» января 2023 г.
Председатель Методического совета
Зам. директора по учебно-методической
работе
_____ А.М.Коротеева

Рабочая программа профессионального обучения по профессии

27618 Шифровальщик

2023

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение «Волжский политехнический техникум» (ГБ ПОУ «ВПТ»).

Разработчики:
Дмитриев Алексей Андреевич – преподаватель ГБ ПОУ «ВПТ»

СОДЕРЖАНИЕ

1. Пояснительная записка

Программа профессионального обучения по профессии 27618 «Шифровальщик» (далее Рабочая программа) рассчитана на 180 ч.

Образовательная область: информатика и ИКТ, информационные технологии в профессиональной деятельности.

Рабочая программа направлена на развитие практических навыков в области расшифровки входящих данных, шифровка важных документов, пресечение попыток взлома, использование криптографических средств. В рамках обучения используются программно-аппаратные криптографические средства защиты информации.

Рабочая программа предназначена для изучения основ терминологии современной криптографии, обучение первоначальным навыкам защиты информации, максимально учитывая технические возможности компьютерной техники мастерской по компетенции
«Разработка компьютерных игр и мультимедийных приложений» и направлена на развитие творческого потенциала слушателей.

Рабочая программа предусматривает очное, очно-заочное и с элементами дистанционного обучения.
После завершения обучения по рабочей программе предусмотрен квалификационный экзамен (8 часов).

2. Формы организации занятий

Основа рабочей программы – теоретическая и практическая направленность занятий. Освоение знаний и способов криптографических средств, элементы шифрования и дешифрования. Осознание и присвоение слушателями достигаемых результатов происходят с помощью рефлексивных заданий. Такой подход гарантирует повышенную мотивацию и результативность обучения. Знания, умения и способы организации программных проектов являются элементами информационной компетенции.

3. Планируемые результаты

Рабочая программа направлена на достижение следующих целей:

- овладение навыками основ криптографической защиты информации

- овладение навыками современных стандартов шифрования

- овладение навыками криптографических методов обеспечения безопасности

сетевых технологий

- овладение навыками интернет вещей

В рамках рабочей программы реализуются следующие задачи:

-познакомить слушателей с алгоритмами шифрования

-познакомить слушателей с основами криптографической защиты информации

-познакомить слушателей с электронной цифровой подписью (ЭЦП)

Минимально необходимый уровень знаний и умений слушателя перед прохождением обучения по рабочей программе:

- уверенный пользователь персонального компьютера;

- лица, имеющие среднее профессиональное и (или) высшее образование;

- лица, получающие среднее профессиональное и (или) высшее образование.

4. Тематический план и содержание рабочей программы «Шифровальщик

N n/n	Тема занятия
	Основы криптографических методов защиты информации
1/1-2	Свойства информационной безопасности
2/3-4	Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности.
3/5-6	Криптографические методы
4/7-8	Шифрование. Кодирование. Стеганография. Сжатие.
5/9-10	Математика криптографии.
6 /11-12	Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение.
7 /13-14	Традиционные шифры перестановки.
8 /15-16	Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования.
9/17-18	Традиционные шифры замены.
10/19-20	Шифры замены. Шифры многоалфавитной замены. Частотность символов.
11/21-22	Криптоанализ.
12/23-24	Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста.
13/25-26	Компьютерное шифрование
14/27-28	Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.
	Практическая часть
15/29-30	Стенографические методы скрытия информации
16/31-32	Бинарная арифметика. Модульная арифметика
17/33-34	Применение методов шифрования перестановкой
18/35-36	Применение методов шифрования заменой
19/37-38	Применение методов шифрования многоалфавитной замены
20/39-40	Криптоанализ методов перестановки
21/41-42	Криптоанализ методов замены
22/43-44	Компьютерное шифрование
	Современные стандарты шифрования
23/45-46	Симметричное шифрование
24/47-48	Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES
25/49-50	Усовершенствованный стандарт шифрования AES
26/51-52	Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES
27/53-54	Российские стандарты симметричного шифрования
28/55-56	Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015
29/57-58	Проблема распределения ключей симметричного шифрования
30/59-60	Алгоритм Диффи-Хелмана. Управление ключами. Kerberos
31/61-62	Асимметричное шифрование
32/63-64	Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках
33/65-66	Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля
	Криптосистемы на основе метода эллиптических кривых. ЭЦП

34/67-68	Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2014 . Безопасность асимметричных алгоритмов.
35/69-70	Классические криптосистемы
36/71-72	Криптосистема AES
37/73-74	Криптосистема RSA
38/75-76	Выполнение задач по сжатию данных
39/77-78	Решение задач с применением метода Хаффмена
40/79-80	Выполнение заданий по арифметическому методу сжатия данных
	Практические занятия
41/81-82	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа
42/83-84	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители
	Криптографические методы обеспечения безопасности сетевых технологий
43/85-86	Целостность сообщения.
44/87-88	Случайная модель Orac1e. Установление подлинности сообщения.
45/89-90	Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94.
46/91-92	ГОСТ Р 34.11 -2014 Анализ безопасности хэш-функций. Атаки на хэш-функции.
47/93-94	Электронная цифровая подпись.
48/95-96	Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП
49/97-98	Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой.
50/99-100	Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2014 .
51/101-102	Установление подлинности объекта.
52/103-104	Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены.
53/105-106	Проблемы распределения открытого ключа асимметричного шифрования
54/107-108	Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI.
55/109-110	Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне.
56/111-112	Электронная почта. Архитектура e-mail. PGP. S/M1ME .
57 /113-114	Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне.
58 /115-116	Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec.
59/117-118	Организация VPN-сети
60/119-120	Защита информации в сетях организованных по технологии беспроводного доступа.
61/121-122	IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16.
62/123-124	Защита информации в сетях сотовой связи.
63/125-126	A3. A8.A5/3. Атаки на алгоритмы.
64/127-128	Перспективы развития беспроводной мобильной связи.
65/129-130	Криптовалюты.
66/131-132	Биткоин. Блокчейн-системы Ethereum
67/133-134	Перспективы развития криптографии.
68/135-136	Квантовая криптография. Проблемы ограничения скорости шифрования.
69/137-138	Проблемы теории асимметричных алгоритмов.
	Практическая часть
70/139-140	Разработка хэш-функции
71/141-142	Разработка схемы простого пароля

72/143-144	Разработка схемы динамического пароля
73/145-146	Сертификаты открытого ключа
74/147-148	Настройка и администрирование токена
75/149-150	Настройка сервисов Рутокен-PinPad
76/151-152	Настройка сервисов Рутокен-ЭЦП
77/153-154	Настройка сервисов Рутокен–Bluetooth
78/155-156	Настройка сервисов Рутокен–S
79/157-158	Разработка алгоритма PGP
80/159-160	Изучение протоколов SSL, TLS, IPSec
81/161-162	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2
	Future Skills IoT (Интернет вещей)
82/163-164	Введение. Что такое IoT (Интернет вещей) и зачем он нужен. История IoT (Интернет вещей). IoT (Интернет вещей) сегодня: сценарии применения. IoT (Интернет вещей) завтра: куда движется IoT.
83/165-166	Обзор IoT (Интернет вещей) проектов и их эффективности
84/167-168	Архитектура IoT (Интернет вещей). Обзор "аппаратной" составляющей IoT (Интернет вещей). Обзор облачной составляющей IoT (Интернет вещей).
85/169-170	**Практическая часть**
86/171-172	Обзор "домашних" решений для IoT (Интернет вещей). IoT (Интернет вещей) Технологии Microsoft. IoT (Интернет вещей) Технологии IBM
	Квалификационный экзамен
87/173-174	Квалификационный экзамен
88/175-176	Квалификационный экзамен
89/177-178	Квалификационный экзамен
90/179-180	Квалификационный экзамен

5. Требования к материально техническому обеспечению мастерской «Разработка компьютерных игр и мультимедийных приложений»

- Компьютер (процессор не ниже i5, видеокарта не ниже 2GB, оперативная память не ниже 4 ГБ, клавиатура+мышь) Монитор 14 шт
- Монитор 24” 12 шт
- Ноутбук HP 250 G7 Corei3 с предустановленной ОС 2шт
- Информационные киоски(Терминалы) 3шт
- МФУ BROTHER MFC 1912WR 1шт
- Проектор VIEWSONIC PA503S 1шт
- Магнитно-маркерная доска 200 х 100 см 1шт
- Кронштейн для проектора Cactus 1шт
- Колонки SVEN 2шт
- кабель VGA 1шт
- Экран Cactus 244x183 настенно-потолочный, белый 1шт
- Шкаф закрытый, тумба 1шт
- КабельHDMI 14шт
- Столы офисные с подставкой 12шт
- LCD панель видеостены LEVEL IX5504+ кронштейны+ коммутационные провода 2шт
- Системы охлаждения 1шт
- МФУ KYOCERA V3145 dn 1шт
- Принтер Xerox AltaLink_ 3T 1шт
- Стол письменный "Бюджет" 1200x600x740 орех онтарио 15шт
- Обрезчик углов Warrior 21144/AD-1 1шт
- Буклетмейкер UCIDA U-Booklet 1шт
- Ламинатор А3 So Good 330S реверс 1шт
- Кресло VB БЮРОКРАТ CH-330M кожзам синий ,хром 13шт
- Операционная система (Windows 10 Pro) 12шт
- Программное обеспечение офисный пакет приложений (MS Office 2019) 16 шт
- Операционная система (Windows 10 Pro) для терминалов 3шт

6. Кадровое обеспечение

Требования к квалификации педагогических кадров, обеспечивающих обучение по рабочей программе:
высшее образование, соответствующее профилю профессионального модуля;
опыт деятельности в организациях соответствующей профессиональной сферы - прохождение стажировки в профильных организациях не реже 1 раза в 3 года.

7. Информационное обеспечение обучения:

Основные источники (печатные издания):

1. *Васильева, И. Н.* Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6.
2. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8.
3. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3.
4. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6.