

Муниципальное бюджетное общеобразовательное учреждение «Гимназия №8» г.
Шумерля Чувашской Республики

«СОГЛАСОВАНО»
Заместитель директора по ВР
_____/ Митина О.А.

«УТВЕРЖДАЮ»
Директор школы:
_____/Сасакина И.В.
Приказ № 90 от 30 августа 2025 г.

Подписан цифровой подписью:
Ирина Владимировна Сасакина
Основание: Я являюсь автором
этого документа

**ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА ТЕХНИЧЕСКОЙ
НАПРАВЛЕННОСТИ**

«КИБЕРБЕЗОПАСНОСТЬ»

Курс проекта «Код будущего» от Финансового университета

Возраст обучающихся: 14-15 лет

Автор – составитель: педагог дополнительного образования Димитриев А.В.

Срок реализации: 1 год

Содержание

1. Пояснительная записка
2. Содержание курса
3. Учебно-тематическое планирование
4. Планируемые результаты
5. Условия реализации
6. Методическое обеспечение

1. Пояснительная записка

Практико-ориентированный курс для учеников 8–9 классов по кибербезопасности, анализу угроз и выявлении уязвимости цифровых сервисов и информационных систем.

Обучение строится от простого к сложному: от основ кибергигиены и шифрования до хеширования, стеганографии и анализа сетевого трафика.

Курс помогает осознанно сформировать профессиональный интерес к информационной безопасности, дает базовое представление о карьере в ИБ и развивает системное мышление, навыки анализа кода и работы с реальными данными.

Программа имеет техническую направленность.

Цель: формирование у обучающихся практических навыков защиты информации и программирования на Python.

Обучающиеся научатся шифровать данные, выявлять уязвимости в коде и веб-приложениях, анализировать сетевые угрозы и разрабатывать собственные инструменты безопасности.

Обучение построено на реальных кейсах ИТ-компаний, интерактивных тренажёрах с автоматической проверкой и проектной работе.

Полученные навыки открывают путь к ИТ-профессиям и участию в олимпиадах.

Целевая аудитория

Программа рассчитана на учащихся 8-9 классов

2. Содержание курса

Модуль 1. Основы кибербезопасности и программирование

Тема 1.1 Знакомство с образовательной платформой, инструментами обучения и триадой информационной безопасности: конфиденциальность, целостность, доступность

Тема 1.2 Ответственное использование ИТ: персональные данные, безопасность, цифровой след и этика ИИ

Тема 1.3 Безопасная среда разработки и работа со строками

Текущий контроль по 1 модулю

Тема 1.4 Логика защиты: валидаторы

Тема 1.5 Циклы в безопасности

Тема 1.6 Случайные числа. Кейс-задача

Промежуточная аттестация по 1 модулю

Модуль 2. Шифрование и защита данных

Тема 2.1 Кодирование и шифрование

Тема 2.2 Операция XOR как основа шифрования

Тема 2.3 Цифровые отпечатки: введение в хеширование

Текущий контроль по 2 модулю

Тема 2.4 Стеганография: искусство скрывать

Тема 2.5 Шифрование файлов. Кейс-задача

Промежуточная аттестация по 2 модулю

Модуль 3: Безопасность в сетях и веб-среде

Тема 3.1 Как компьютеры общаются: IP-адреса, порты и сокеты

Тема 3.2 "Веб-запросы, библиотеки, искусственный интеллект как инструмент в ИБ"

Тема 3.3 Табличные данные цифрового двойника: работа с CSV

Текущий контроль по 3 модулю

Тема 3.4 Межсайтовый скриптинг (XSS): как вредоносный код попадает на сайт. Проверка уязвимостей с применением ИИ

Тема 3.5 Фишинг и проверка URL-адресов

Тема 3.6 Безопасное хранение данных: введение в базы данных и SQL-инъекции. Кейс-задача

Промежуточная аттестация по 3 модулю

Модуль 4: Итоговый проект

Тема 4.1 Доктрина информационной безопасности. Белые, серые, черные хакеры. Этика и закон.

Тема 4.2 Аудит кода: ищем уязвимости в чужих и своих программах

Тема 4.3 Проектирование итогового проекта

Текущий контроль по 4 модулю

Тема 4.4 Разработка и отладка проекта

Тема 4.5 Оформление проекта и подготовка к защите

Промежуточная аттестация по 4 модулю

Итоговая аттестация

4. Учебно-тематическое планирование

Модуль 1. Основы кибербезопасности и программирование

№ темы	Название темы	Трудоемкость (ак. час)
Тема 1.1	Знакомство с образовательной платформой, инструментами обучения и триадой информационной безопасности: конфиденциальность, целостность, доступность	2
Тема 1.2	Ответственное использование ИТ: персональные данные, безопасность, цифровой след и этика ИИ	3
Тема 1.3	Безопасная среда разработки и работа со строками	5
	<i>Текущий контроль по 1 модулю</i>	1
Тема 1.4	Логика защиты: валидаторы	5
Тема 1.5	Циклы в безопасности	10
Тема 1.6	Случайные числа. Кейс-задача	9
	<i>Промежуточная аттестация по 1 модулю</i>	1

Модуль 2. Шифрование и защита данных

№ темы	Название темы	Трудоемкость (ак. час)
Тема 2.1	Кодирование и шифрование	10
Тема 2.2	Операция XOR как основа шифрования	5
Тема 2.3	Цифровые отпечатки: введение в хеширование	4
	<i>Текущий контроль по 2 модулю</i>	1
Тема 2.4	Стеганография: искусство скрывать	5
Тема 2.5	Шифрование файлов. Кейс-задача	10
	<i>Промежуточная аттестация по 2 модулю</i>	1

Модуль 3. Безопасность в сетях и веб-среде

№ темы	Название темы	Трудоемкость (ак. час)
Тема 3.1	Как компьютеры общаются: IP-адреса, порты и сокет	10
Тема 3.2	Веб-запросы, библиотеки, искусственный интеллект как инструмент в ИБ	5
Тема 3.3	Табличные данные цифрового двойника: работа с CSV	4
	<i>Текущий контроль по 3 модулю</i>	1
Тема 3.4	Межсайтовый скриптинг (XSS): как вредоносный код попадает на сайт. Проверка уязвимостей с применением ИИ	5
Тема 3.5	Фишинг и проверка URL-адресов	5
Тема 3.6	Безопасное хранение данных: введение в базы данных и SQL-инъекции. Кейс-задача	5
	<i>Промежуточная аттестация по 3 модулю</i>	1

Модуль 4. Итоговый проект

№ темы	Название темы	Трудоемкость (ак. час)
Тема 4.1	Доктрина информационной безопасности. Белые, серые, черные хакеры. Этика и закон.	5
Тема 4.2	Аудит кода: ищем уязвимости в чужих и своих программах	10
Тема 4.3	Проектирование итогового проекта	6
	<i>Текущий контроль по 4 модулю</i>	1
Тема 4.4	Разработка и отладка проекта	8
Тема 4.5	Оформление проекта и подготовка к защите	5
	<i>Промежуточная аттестация по 4 модулю</i>	1

5. Планируемые результаты

- Писать программы на Python с использованием ветвлений, циклов и функций для решения задач информационной безопасности: проверки данных и генерации паролей.
- Понимать разницу между кодированием и шифрованием, реализовывать алгоритмы: шифр Цезаря, XOR и др.
- Распознавать фишинг и понимать принципы триады информационной безопасности: конфиденциальность, целостность, доступность.

По окончании обучения по программе обучающиеся будут:

иметь представление:

- о роли специалиста по ИБ и форматах профессионального развития в ИТ

знать:

- базовые конструкции языка Python
- принципы информационной безопасности (конфиденциальность, целостность, доступность)
- основные виды шифрования (симметричное, асимметричное), хеширование и их применение
- типичные веб-уязвимости
- правовые и этические нормы в сфере ИБ

понимать:

- разницу между кодированием, шифрованием и хешированием и уместность применения каждого из методов
- роль ИИ-инструментов в современном процессе разработки и аудита кода, а также риски, связанные с некритическим использованием сгенерированного кода.

уметь:

- писать программы на Python для шифрования/дешифрования данных, проверки паролей, анализа URL-адресов
- использовать библиотеки hashlib, secrets, socket для решения задач ИБ
- анализировать логи и выявлять подозрительную активность

владеть:

- навыками работы со стандартными библиотеками Python для задач ИБ
- навыками чтения, написания и комментирования кода на Python в соответствии с базовыми принципами читаемости
- навыками поиска и исправления уязвимостей в учебном коде
- навыками защиты итогового проекта
- культура цифровой гигиены и ответственного поведения в сети
- понимание правовой ответственности и этических границ деятельности специалиста по ИБ
- критическое мышление при работе с ИИ-инструментами
- навыки командной работы
- мотивация к дальнейшему изучению ИТ и информационной безопасности, в том числе к участию в олимпиадах и соревнованиях

5. Условия реализации

Методы обучения

Модульный, проблемный и контекстный подходы.

Формы занятий

Лекции с демонстрацией мультимедийных материалов, практические работы, самостоятельная работа.

Технологии

Традиционные (объяснительно-иллюстративные) и интерактивные (групповые обсуждения, решение кейсов).

7. Методическое обеспечение

1. Личный кабинет курса «Кибербезопасность» финансового университета.
2. Презентации, предоставленные ФУ.