

Дополнительная общеобразовательная программа

Кибербезопасность. 8-9 класс (базовый уровень)



Кибербезопасность. 8-9 класс (базовый уровень)

Программа сочетает глубокую техническую подготовку с развитием командных навыков и правовой грамотности.

Содержание программы разработано с учётом возрастных особенностей целевой аудитории (школьники 8-9 классов) и обеспечивает последовательное усвоение информации от базового синтаксиса Python до разработки проекта.



Краткая характеристика программы

Направление обучения: Современные языки программирования (в том числе для обеспечения информационной безопасности)

Уровень

Базовый

Сроки

1 учебный год (01.10.2026 – 28.05.2027)

Формат

Онлайн и офлайн

Объём

145 ак. часов

Аттестация

- Промежуточная (по модулям): 11 вариантов — тесты и практико-ориентированные задачи в тренажере
- Итоговая: 7 вариантов комплексных заданий — тест и защита проекта с презентацией

Учебно-методический комплект

- Презентации (теория + практика)
- Описания практических заданий и кейс-задач
- Задания для самоконтроля и самостоятельной работы
- Методические материалы для преподавателей
- Оценочные материалы всех уровней контроля

Практическая составляющая

- Практические задания различного уровня сложности
- 3 кейс-задачи (включая задачу от аккредитованной ИТ-организации)
- Проектная работа
- Вариативные, парные и групповые задания
- Задания на проверку и исправление ИИ-кода

Дополнительная ценность: учет элементов содержания ОГЭ

Особенности программы

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.



СТРУКТУРА ПРОГРАММЫ

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
	Текущий контроль по 1 модулю	1
Тема 1.4	Логика защиты: валидаторы	5
Тема 1.5	Циклы в безопасности	10
Тема 1.6	Случайные числа. Кейс-задача	9
	Промежуточная аттестация по 1 модулю	1

СТРУКТУРА ПРОГРАММЫ

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

СТРУКТУРА ПРОГРАММЫ

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

СТРУКТУРА ПРОГРАММЫ

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

Планируемые результаты обучения

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



Планируемые результаты обучения

По окончании обучения по программе обучающиеся будут:

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



Планируемые результаты обучения

По окончании обучения по программе у обучающегося будут сформированы:

- 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



Методы, формы и технологии, применяемые при реализации программы



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).

