

Дополнительная общеобразовательная программа

Кибербезопасность. 10-11 класс (базовый уровень)



Кибербезопасность. 10-11 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 10-11 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 ЕГЭ

Особенности программы

Программа имеет техническую направленность. Цель: формирование у обучающихся системных знаний и практических навыков в области информационной безопасности и программирования на Python для защиты информации и разработки безопасных приложений.

Обучающиеся научатся шифровать данные, устранять уязвимости, анализировать сетевые угрозы и создавать защищённые программные продукты.

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

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



СТРУКТУРА ПРОГРАММЫ

Модуль 1. Python как инструмент для кибербезопасности

№ темы	Название темы	Трудоемкость (ак. час)
Тема 1.1	Знакомство с образовательной платформой, инструментами обучения и введение в кибербезопасность	2
Тема 1.2	Ответственное использование ИТ: государственная политика ИБ, персональные данные, правовая ответственность и этика ИИ	3
Тема 1.3	Безопасная среда разработки	5
	<i>Текущий контроль по 1 модулю</i>	1
Тема 1.4	Структуры данных и модули	5
Тема 1.5	Объектно-ориентированная логика защиты: классы и инкапсуляция	10
Тема 1.6	Криптографически стойкая случайность и работа с байтами. Кейс-задача	9
	<i>Промежуточная аттестация по 1 модулю</i>	1

СТРУКТУРА ПРОГРАММЫ

Модуль 2. Прикладная криптография: от математики к защищённому коду

№ темы	Название темы	Трудоемкость (ак. час)
Тема 2.1	Математика криптографии: модульная арифметика и простые числа	10
Тема 2.2	RSA с нуля: реализация асимметричного шифрования	5
Тема 2.3	AES и современное симметричное шифрование	5
	<i>Текущий контроль по 2 модулю</i>	1
Тема 2.4	HMAC и целостность данных: защита от подделки	5
Тема 2.5	Взлом слабой криптографии: словарные атаки и радужные таблицы	5
Тема 2.6	PKI и цифровые подписи. Кейс-задача	4
	<i>Промежуточная аттестация по 2 модулю</i>	1

СТРУКТУРА ПРОГРАММЫ

Модуль 3. Сетевая безопасность и веб-уязвимости: инструменты атаки и защиты

№ темы	Название темы	Трудоемкость (ак. час)
Тема 3.1	Сокеты и сетевое программирование: клиент-сервер с шифрованием	10
Тема 3.2	Сканер портов и сетевая разведка. ИИ как инструмент в ИБ	5
Тема 3.3	Анализ логов и обнаружение аномалий	4
	<i>Текущий контроль по 3 модулю</i>	1
Тема 3.4	Веб-уязвимости: XSS и CSRF. Проверка уязвимостей с применением ИИ	5
Тема 3.5	Path Traversal: небезопасная работа с файловой системой	5
Тема 3.6	Безопасная работа с файлами и сериализация данных. Кейс-задача	5
	<i>Промежуточная аттестация по 3 модулю</i>	1

СТРУКТУРА ПРОГРАММЫ

Модуль 4. Итоговый проект: от идеи к готовому продукту

№ темы	Название темы	Трудоемкость (ак. час)
Тема 4.1	Этика, закон и профессия: белые, серые и чёрные хакеры	5
Тема 4.2	Аудит кода: статический анализ и поиск уязвимостей	10
Тема 4.3	Проектирование итогового проекта: модель угроз (threat model) и архитектура	6
	<i>Текущий контроль по 4 модулю</i>	1
Тема 4.4	Разработка, отладка и статический анализ проекта	8
Тема 4.5	Оформление проекта	5
	<i>Промежуточная аттестация по 4 модулю</i>	1

Планируемые результаты обучения

По окончании обучения по программе обучающиеся будут:

иметь представление:

- о триаде информационной безопасности
- об этике и правовых нормах
- о принципах работы веб-уязвимостей

знать:

- основы синтаксиса Python
- ООП
- базовые криптографические алгоритмы
- типы сетевых и веб-угроз
- принципы безопасной среды разработки



Планируемые результаты обучения

По окончании обучения по программе обучающиеся будут:

уметь:

- писать скрипты для шифрования и хеширования
- реализовывать простейшие сетевые инструменты
- распознавать базовые веб-угрозы и применять методы их нейтрализации
- проводить статический анализ кода

владеть:

- инструментами криптографической библиотеки cryptography
- методами построения модели угроз
- навыками безопасной работы с файловой системой и данными



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).

