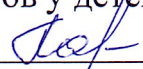


Министерство образования и науки Хабаровского края
Краевое государственное автономное нетиповое образовательное
учреждение «Краевой центр образования»
Региональный центр выявления, поддержки и развития способностей и
талантов у детей и молодёжи

СОГЛАСОВАНО

Руководитель направления «Наука»
Регионального центра выявления, под-
держки и развития способностей и та-
лантов у детей и молодежи «Сириус
27»  / Г.Н. Ко-
пубинская

«22» Августа 2026 г.

УТВЕРЖДАЮ

Генеральный директор
КГАНОУ «Краевой центр образова-
ния»



П.С. Черёмухин

2026 г.

Дополнительная общеобразовательная
общеразвивающая программа по направлению «Информатика»

«Информатика. Информационная безопасность»

Возраст обучающихся: 13–18 лет
Форма обучения: дистанционная

Составитель:
Долгачев Михаил Владимирович

Место реализации:
Хабаровский край, г. Хабаровск
Региональный центр выявления,
поддержки и развития способностей
и талантов у детей и молодежи
КГАНОУ КЦО

Хабаровск
2026

Основания и принятые при составлении допущения

Программа подготовлена в структуре, заданной документом «Общие требования к программе»: пояснительная записка, цель, задачи, формы обучения, объем и режим занятий, сведения о педагогах и партнёрах, учебный план, календарный учебный график, содержание, планируемые результаты, оценочные и методические материалы, материально-техническое обеспечение и список источников. Программа разработана для реализации в КГАНОУ КЦО, г. Хабаровск.

Содержательная часть опирается на методические рекомендации по проведению школьного и муниципального этапов всероссийской олимпиады школьников по информатике на 2026/27 учебный год, в том числе раздел по профилю «Информационная безопасность».

Для расчёта часов использованы параметры из задания заказчика. Программа «Информационная безопасность» рассчитана на 36 учебных недель по 9 академических часов в неделю и два дистанционных учебных блока в неделю (4 и 5 часов с обязательными перерывами внутри блока), всего 324 часа.

Занятия проводятся дистанционно по понедельникам и средам с 18:30 с использованием Яндекс Телемост: в понедельник — 4 академических часа, в среду — 5 академических часов. Конкретные календарные даты заполняются после утверждения расписания.

ПРОГРАММА

«ИНФОРМАТИКА. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1. Пояснительная записка

Программа имеет техническую направленность и ориентирована на системную подготовку школьников к решению учебных и олимпиадных задач по защите информации, криптографии, сетевой безопасности, анализу трафика, Linux/Unix, Web, Forensics, реверс-анализу и средствам защиты информации. Практическая часть строится в виртуальных машинах, локальной сети и учебных CTF-стендах.

Актуальность программы связана с ростом значения безопасной обработки данных и потребностью в практических навыках анализа защищённости. Новизна проекта состоит в объединении базовой теории информатики с задачами олимпиадного типа и учебными CTF-кейсами. Отличительная особенность — приоритет практики и работа только в изолированной, специально разрешённой инфраструктуре.

Тип программы: разноуровневая. Базовый уровень охватывает кодирование, основы криптографии, сети, Linux и цифровую гигиену; углублённый уровень — анализ трафика, Web, Forensics, реверс и комплексные CTF-задачи. Рекомендуемый уровень усвоения — базовый/углублённый в зависимости от входной подготовки обучающегося.

2. Цель программы

Сформировать у обучающихся устойчивые знания и практические навыки безопасной работы с информационными системами и подготовки к олимпиадным заданиям по профилю «Информационная безопасность», включая решение задач в контролируемых учебных лабораториях и формате CTF.

3. Задачи программы

Предметные задачи:

- освоить базовые понятия защиты информации, кодирования, криптографии, сетей и операционных систем;
- научиться анализировать сетевой трафик, системные журналы и цифровые артефакты;
- освоить базовые подходы к безопасной настройке Linux/Unix, web-приложений и средств защиты информации;
- получить опыт решения олимпиадных и CTF-задач в категориях Crypto, Network, Web, Forensics, Linux/Unix, Reverse и СЗИ;
- освоить правила документирования хода практической работы и проверки результата.

Метапредметные задачи:

- развивать алгоритмическое и системное мышление, способность декомпозировать задачу;
- формировать навыки анализа данных из нескольких источников и аргументированного вывода;
- развивать самостоятельность, самоконтроль, работу с документацией и тестирующими системами.

Личностные задачи:

- формировать ответственное и этическое отношение к технологиям информационной безопасности;
- закрепить принцип работы только с собственными, учебными или явно разрешёнными системами;
- развивать аккуратность, академическую честность и уважение к конфиденциальности данных.

4–9. Организационно-педагогические условия

Форма обучения	Дистанционная; синхронные занятия в Яндекс Телемост, демонстрации, самостоятельная работа и виртуальные лаборатории.
Возраст и категория	13–18 лет, 7–11 классы; мотивированные обучающиеся с базовыми навыками работы на ПК.
Объём программы	324 академических часа.
Срок освоения	9 учебных месяцев, 36 учебных недель; конкретные календарные даты утверждаются образовательной организацией.
Режим занятий	Понедельник и среда, начало в 18:30. Понедельник — 4 академических часа, среда — 5 академических часов; суммарно 9 часов в неделю. Внутри длительных блоков предусматриваются обязательные технологические и санитарные перерывы.
Руководитель программы	Долгачев Михаил Владимирович, педагог дополнительного образования КГА-НОУ КЦО.
Педагогические работники	Реализацию программы осуществляет один педагог: Долгачев Михаил Владимирович, педагог дополнительного образования КГАНОУ КЦО. Общий объём преподавательской нагрузки — 324 ч.
Партнёры	Не предусмотрены.

10. Учебный план (Приложение № 1)

№	Название раздела, блока, модуля	Количество часов			Формы промежуточного контроля
		всего	теория	практика	
1	Введение в информационную безопасность и безопасная учебная среда	18	6	12	Стартовая диагностика, чек-лист безопасной работы
2	Представление информации, кодирование и основы криптографии	36	12	24	Мини-тест, практикум по кодированию и шифрам
3	Безопасность операционных систем Linux/Unix и виртуализация	54	14	40	Лабораторные работы, мини-CTF
4	Компьютерные сети, сетевые протоколы и анализ трафика	54	14	40	Анализ рсар/трафика, практическая работа
5	Безопасность web-приложений в изолированных учебных стендах	54	12	42	Практические задания и CTF-флаги
6	Forensics: поиск следов инцидентов и анализ цифровых артефактов	45	10	35	Кейс расследования, отчёт по артефактам
7	Реверс-анализ и безопасное программирование	36	10	26	Практикум по анализу кода, мини-CTF
8	Средства защиты информации и комплексная защита систем	18	4	14	Защита конфигурации, оценочный лист
9	Итоговый практический тур в формате учебного CTF	9	0	9	Итоговый CTF и рефлексия
	Итого за год	324	82	242	Итоговая диагностика / итоговый практический тур

11. Календарный учебный график (Приложение № 2)

Примечание: занятия проводятся по понедельникам и средам с 18:30. Конкретные календарные даты вносятся образовательной организацией после утверждения расписания. Недельный объём — 9 академических часов.

Месяц	Дата / неделя	Тема занятия	Форма проведения	Кол-во часов	Форма контроля	Примечания
Сентябрь	Пн, нед. 1, 18:30	Вводное занятие. Цели программы, правила дистанционной работы, стартовая диагностика	Дистанционно: Яндекс Телемост + интерактивный практикум	4	Мини-тест / устный разбор	Модуль 1
Сентябрь	Ср, нед. 1, 18:30	Модель угроз, конфиденциальность, целостность, доступность. Цифровая гигиена	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 1
Сентябрь	Пн, нед. 2, 18:30	Информация, данные и способы их представления	Дистанционно: Яндекс Телемост + интерактивный практикум	4	Мини-тест / устный разбор	Модуль 1

Месяц	Дата / неделя	Тема занятия	Форма проведения	Кол-во часов	Форма контроля	Примечания
Сентябрь	Ср, нед. 2, 18:30	Кодирование текстовой, числовой и двоичной информации: практикум	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 1
Сентябрь	Пн, нед. 3, 18:30	Системы счисления и преобразования как основа кодирования	Дистанционно: Яндекс Телемост + интерактивный практикум	4	Мини-тест / устный разбор	Модуль 2
Сентябрь	Ср, нед. 3, 18:30	Коды, форматы и контроль целостности данных	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 2
Сентябрь	Пн, нед. 4, 18:30	Исторические шифры и принципы криптографии	Дистанционно: Яндекс Телемост + интерактивный практикум	4	Мини-тест / устный разбор	Модуль 2
Сентябрь	Ср, нед. 4, 18:30	Практикум по классическим шифрам и частотному анализу	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 2
Октябрь	Пн, нед. 5, 18:30	Современная криптография: симметричные и асимметричные подходы	Дистанционно: Яндекс Телемост + интерактивный практикум	4	Мини-тест / устный разбор	Модуль 2
Октябрь	Ср, нед. 5, 18:30	Хэширование: свойства, контроль целостности, учебные задачи	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 2
Октябрь	Пн, нед. 6, 18:30	Электронная подпись и доверие к данным	Дистанционно: Яндекс Телемост + интерактивный практикум	4	Мини-тест / устный разбор	Модуль 2
Октябрь	Ср, нед. 6, 18:30	Модульный практикум: кодирование, шифрование, хэширование	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 2
Октябрь	Пн, нед. 7, 18:30	Виртуальные машины и изолированная учебная лаборатория	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 3
Октябрь	Ср, нед. 7, 18:30	Linux/Unix: файловая система и навигация	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 3
Октябрь	Пн, нед. 8, 18:30	Пользователи, группы и права доступа	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 3
Октябрь	Ср, нед. 8, 18:30	Практикум по правам доступа и безопасной настройке файлов	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 3
Ноябрь	Пн, нед. 9, 18:30	Процессы, службы и управление ресурсами	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 3
Ноябрь	Ср, нед. 9, 18:30	Диагностика процессов и служб в учебной VM	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 3
Ноябрь	Пн, нед. 10, 18:30	Журналы событий и системные логи	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 3
Ноябрь	Ср, нед. 10, 18:30	Поиск событий безопасности по логам	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 3
Ноябрь	Пн, нед. 11, 18:30	Командная строка и простые сценарии автоматизации	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 3
Ноябрь	Ср, нед. 11, 18:30	Практикум: команды, конвейеры, обработка файлов	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 3
Ноябрь	Пн, нед. 12, 18:30	Безопасная настройка Linux/Unix: обновления, минимизация привилегий	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	CTF-флаги / автоматическая проверка	Модуль 3
Ноябрь	Ср, нед. 12, 18:30	Мини-CTF по Linux/Unix в изолированной среде	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	CTF-флаги / автоматическая проверка	Модуль 3
Декабрь	Пн, нед. 13, 18:30	Основы компьютерных сетей и модель TCP/IP	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 4
Декабрь	Ср, нед. 13, 18:30	IP-адресация и подсети: расчетные задачи	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 4
Декабрь	Пн, нед. 14, 18:30	Канальный и сетевой уровни. ARP, IP, ICMP	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 4
Декабрь	Ср, нед. 14, 18:30	Практикум: наблюдение сетевого обмена	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 4
Декабрь	Пн, нед. 15, 18:30	Транспортный уровень: TCP/UDP, порты и соединения	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 4
Декабрь	Ср, нед. 15, 18:30	Анализ соединений и сетевых состояний	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 4
Декабрь	Пн, нед. 16, 18:30	Прикладные протоколы: DNS, HTTP(S), DHCP	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 4
Декабрь	Ср, нед. 16, 18:30	Разбор сетевого трафика по протоколам	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 4

Месяц	Дата / неделя	Тема занятия	Форма проведения	Кол-во часов	Форма контроля	Примечания
Январь	Пн, нед. 17, 18:30	Введение в анализ трафика. Формат рсар	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 4
Январь	Ср, нед. 17, 18:30	Фильтрация и поиск событий в сетевой трассе	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 4
Январь	Пн, нед. 18, 18:30	Известные сетевые атаки: признаки и защитные меры	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 4
Январь	Ср, нед. 18, 18:30	Практикум: выявление аномалий по учебному трафику	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 4
Январь	Пн, нед. 19, 18:30	Архитектура web-приложений и HTTP	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 5
Январь	Ср, нед. 19, 18:30	Запросы, ответы, заголовки, cookies и сессии	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 5
Январь	Пн, нед. 20, 18:30	Аутентификация и авторизация web-приложений	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 5
Январь	Ср, нед. 20, 18:30	Практикум на учебном локальном web-стенде	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 5
Февраль	Пн, нед. 21, 18:30	Ввод данных и валидация. Класс инъекционных ошибок	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 5
Февраль	Ср, нед. 21, 18:30	Лаборатория: поиск и исправление уязвимой логики на учебном стенде	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 5
Февраль	Пн, нед. 22, 18:30	Клиентская безопасность и межсайтовые сценарии: обзор	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 5
Февраль	Ср, нед. 22, 18:30	Практикум: безопасная обработка пользовательского ввода	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 5
Февраль	Пн, нед. 23, 18:30	Защита сессий, разграничение доступа, безопасные настройки	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 5
Февраль	Ср, нед. 23, 18:30	Проверка конфигурации учебного web-приложения	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 5
Февраль	Пн, нед. 24, 18:30	Комплексный разбор web-задач олимпиадного типа	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	CTF-флаги / автоматическая проверка	Модуль 5
Февраль	Ср, нед. 24, 18:30	Мини-CTF по Web в разрешённой лаборатории	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	CTF-флаги / автоматическая проверка	Модуль 5
Март	Пн, нед. 25, 18:30	Forensics: цели, этапы и сохранность цифровых следов	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 6
Март	Ср, нед. 25, 18:30	Хэши и идентификация файлов: практикум	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 6
Март	Пн, нед. 26, 18:30	Метаданные файлов и временные метки	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 6
Март	Ср, нед. 26, 18:30	Построение временной шкалы событий по учебному кейсу	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 6
Март	Пн, нед. 27, 18:30	Анализ системных и прикладных журналов	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 6
Март	Ср, нед. 27, 18:30	Корреляция событий из нескольких источников	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 6
Март	Пн, нед. 28, 18:30	Forensics сетевого инцидента: связка логов и трафика	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 6
Март	Ср, нед. 28, 18:30	Практикум по поиску индикаторов в рсар и логах	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 6
Апрель	Пн, нед. 29, 18:30	Комплексный кейс расследования инцидента	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 6
Апрель	Ср, нед. 29, 18:30	Оформление краткого технического отчёта и защита выводов	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 6
Апрель	Пн, нед. 30, 18:30	Реверс-анализ: назначение и безопасная методика	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 7
Апрель	Ср, нед. 30, 18:30	Анализ исходного кода и поиск логики проверки	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 7
Апрель	Пн, нед. 31, 18:30	Строки, форматы файлов и простые артефакты бинарных программ	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 7

Месяц	Дата / неделя	Тема занятия	Форма проведения	Кол-во часов	Форма контроля	Примечания
Апрель	Ср, нед. 31, 18:30	Практикум по поиску значимых строк и структур	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 7
Апрель	Пн, нед. 32, 18:30	Отладка и трассировка на учебных примерах	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 7
Апрель	Ср, нед. 32, 18:30	Реверс-задачи базового уровня в виртуальной среде	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 7
Май	Пн, нед. 33, 18:30	Безопасное программирование: валидация, ошибки, секреты	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	CTF-флаги / автоматическая проверка	Модуль 7
Май	Ср, нед. 33, 18:30	Мини-CTF: анализ кода и безопасное исправление	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	CTF-флаги / автоматическая проверка	Модуль 7
Май	Пн, нед. 34, 18:30	Средства защиты информации: классы и назначение	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 8
Май	Ср, нед. 34, 18:30	Практикум: межсетевой экран, резервирование, контроль доступа	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 8
Май	Пн, нед. 35, 18:30	Комплексная защита: принцип эшелонирования и настройка	Дистанционно: Яндекс Телемост + виртуальная лаборатория	4	Мини-тест / устный разбор	Модуль 8
Май	Ср, нед. 35, 18:30	Защита конфигурации учебной системы по чек-листу	Дистанционно: Яндекс Телемост + виртуальная лаборатория	5	Практическая работа / артефакт	Модуль 8
Май	Пн, нед. 36, 18:30	Итоговый учебный CTF: сетевые, web, Linux, forensics и crypto-задачи	Дистанционно: Яндекс Телемост + учебный CTF на изолированной платформе	4	Итоговая диагностика / CTF	Модуль 9
Май	Ср, нед. 36, 18:30	Завершение CTF, разбор решений, итоговая диагностика и рефлексия	Дистанционно: Яндекс Телемост + учебный CTF на изолированной платформе	5	Итоговая диагностика / CTF	Модуль 9

12. Содержание программы

Модуль 1. Введение в информационную безопасность и безопасная учебная среда

Понятия информационной безопасности и модели угроз; конфиденциальность, целостность и доступность; цифровая гигиена; учётные записи; правила дистанционной работы. Настройка безопасной учебной среды. Практика проводится только на собственных виртуальных машинах, локальных стендах и CTF-платформах, предоставленных преподавателем.

Модуль 2. Представление информации, кодирование и основы криптографии

Технологии получения, обработки и использования информации; кодирование; системычисления; классические шифры; принципы симметричного и асимметричного шифрования; хэширование; электронная подпись. Практика: задачи с коротким ответом, программирование и анализ результатов.

Модуль 3. Linux/Unix и виртуализация

Файловая система, пользователи и группы, права доступа, процессы, службы, журналы событий, командная строка, базовая автоматизация и безопасная настройка. Практика в виртуальной машине.

Модуль 4. Сети и анализ трафика

Основы TCP/IP, IP-адресация, TCP/UDP, DNS, HTTP(S), сетевые состояния, рсар, фильтрация и интерпретация сетевого трафика. Известные атаки рассматриваются с точки зрения признаков, последствий и мер защиты.

Модуль 5. Web-безопасность

Архитектура web-приложений, HTTP, сессии, аутентификация, авторизация, валидация данных, типовые классы уязвимостей и безопасные способы обработки данных. Все упражнения выполняются на локальном или специально предназначенном учебном стенде.

Модуль 6. Forensics

Поиск следов инцидентов информационной безопасности, работа с хэшами, метаданными, временными метками, логами и учебными сетевыми трассами. Формирование временной шкалы и технического отчёта.

Модуль 7. Реверс-анализ и безопасное программирование

Анализ исходных текстов и логики программ, строки и форматы, базовые приёмы отладки и трассировки, поиск ошибок в коде, безопасная обработка ввода и секретов.

Модуль 8. Средства защиты информации

Назначение и классы СЗИ, контроль доступа, межсетевые экраны, резервирование, обновления, принцип эшелонированной защиты. Практика — защита учебной конфигурации по чек-листу.

Модуль 9. Итоговый CTF

Комплексный учебный практический тур: Crypto, Linux/Unix, Network, Web, Forensics, Reverse, СЗИ. Автоматическая проверка части заданий по флагам; итоговый разбор и индивидуальные рекомендации.

Образовательные технологии: проблемное обучение, демонстрация с последующим воспроизведением, виртуальная лаборатория, кейс-метод, мини-CTF, автоматическая проверка, разбор типичных ошибок, индивидуальная траектория по результатам диагностик.

13. Планируемые результаты освоения

По итогам программы обучающийся должен демонстрировать следующие диагностируемые результаты:

- объясняет назначение базовых механизмов защиты информации и корректно использует основную терминологию не менее чем в 70% заданий итогового теста;
- решает задачи на кодирование, шифрование и хэширование базового/среднего уровня;
- работает в Linux/Unix VM: навигация, права доступа, процессы, журналы, безопасная конфигурация;
- читает учебные сетевые трассы и выделяет существенные признаки событий по заданному сценарию;
- находит и описывает ошибки безопасности в специально подготовленных web-стендах и предлагает безопасный способ исправления;
- проводит базовый Forensics-анализ учебного кейса и оформляет краткий отчёт с подтверждающими артефактами;
- решает не менее 60% заданий базового набора итогового CTF либо показывает сопоставимый прирост относительно стартовой диагностики;
- соблюдает границы разрешённой лаборатории и правила ответственного использования инструментов.

14. Оценочные материалы

Стартовая диагностика: 20 заданий (10 вопросов по базовой информатике и безопасности, 5 задач на кодирование/логику, 5 практических микрзадач). Результат используется для распределения по уровню сложности и не входит в итоговую отметку.

Текущий контроль: мини-тесты; практические работы в VM; задания с автоматической проверкой; CTF-флаги; отчёты с кратким описанием действий и результата; контрольные чек-листы безопасной конфигурации.

Итоговая диагностика: учебный CTF и короткий теоретический тест. В CTF включаются задачи нескольких категорий, соответствующих содержанию программы. Для заданий СЗИ допускается оценка по предоставленным файлам/скриншотам/конфигурациям.

15. Критерии оценивания выполненных заданий

Рекомендуемая 100-балльная система: текущие практические работы — 40 баллов; модульные контрольные и мини-CTF — 30 баллов; итоговый CTF и итоговый тест — 30 баллов. Для практических задач учитываются: корректность результата (до 60% баллов задания), воспроизводимость/подтверждающий артефакт (до 20%), объяснение решения и соблюдение формата (до 20%).

Интерпретация результата: 85–100 баллов — высокий уровень; 70–84 — достаточный; 50–69 — базовый; менее 50 — требуется повторная отработка ключевых тем. При оценивании олимпиадных задач могут использоваться автоматические статусы «полное/частичное решение» и частичные баллы.

16. Методические материалы и электронные ресурсы

- Перед каждой практикой преподаватель выдаёт рабочий лист: цель, безопасная область эксперимента, критерии результата, формат сдачи.
- Для обучающихся начального уровня применяются пошаговые чек-листы и задачи с подсказками; для продвинутых — задания с минимальным количеством подсказок и дополнительными CTF-челленджами.
- Разбор проводится после фиксации результатов; обучающиеся сравнивают несколько корректных способов решения и формируют краткий конспект.
- При дистанционной работе демонстрация экрана используется для объяснения, а сдача результатов выполняется через LMS/тестирующую систему. Запрещается выполнять практические действия в отношении внешних систем без явного разрешения.

17. Материально-технические средства

- Персональный компьютер/ноутбук с устойчивым доступом в Интернет для Яндекс Телемост и LMS; для лабораторий — не менее 8 ГБ ОЗУ рекомендуется, поддержка виртуализации.
- Гипервизор VirtualBox или эквивалент; заранее подготовленные виртуальные машины участника и преподавателя.
- Браузер, Python 3 и среда разработки/редактор; локальная тестирующая система или CTFd/аналог.
- Средства анализа трафика и системных артефактов, установленные в учебной VM; точный перечень утверждается преподавателем до начала модуля.
- Для итогового практического тура — изолированная инфраструктура без необходимости доступа к внешним целям; доступ к платформе с заданиями и индивидуальные учётные записи.

18. Список источников

Для педагогов

- Методические рекомендации по проведению школьного и муниципального этапов всероссийской олимпиады школьников по информатике в 2026/27 учебном году. Раздел «Информационная безопасность».
- Материалы и разборы прошлых лет: <https://vsosh.miem.hse.ru/>
- Онлайн-тренинг по web-безопасности: <https://portswigger.net/web-security>
- Учебные материалы CTF: <https://spb.ctf.su/> и <https://overthewire.org/wargames/>

Для обучающихся

- CTF для начинающих: <https://vk.com/@spbctf-ctf-for-beginners>
- Учебная платформа SPB CTF: <https://spb.ctf.su/>
- Hack The Box (учебная платформа): <https://www.hackthebox.com/>
- Hackerdom SQL training: <https://sql.training.hackerdom.ru/1.php>
- OverTheWire Wargames: <https://overthewire.org/wargames/>