Кировское областное государственное автономное образовательное учреждение
дополнительного образования
«ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ОДАРЕННЫХ ШКОЛЬНИКОВ»

Принято на заседании
Экспертного совета
Регионального центра
«15» мая 2026 г.

Принято на заседании
методического совета
КОГАОУ ДО ЦДООШ
«19» мая 2026 г.

УТВЕРЖДАЮ
_____
директор
КОГАОУ ДО ЦДООШ
Е. Н. Перминова
«19» мая 2026 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направленность программы — естественно-научная
Срок реализации — 14 дней

АВТОР-СОСТАВИТЕЛЬ:
Алдущенков Николай Сергеевич,
учитель МОАУ ЛИнТех №28 города Кирова

РУКОВОДИТЕЛЬ ПРОГРАММЫ:
Алдущенков Николай Сергеевич

Киров
2026

I ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Направленность

Направленность программы — естественно-научная.

1.2 Актуальность, новизна, педагогическая целесообразность

Дополнительная общеобразовательная программа «Информационная безопасность» реализуется в рамках третьей смены ДОЛ «Вишкиль» и предназначена для учащихся 7–10 классов общеобразовательных школ города Кирова и Кировской области, показавших хорошие результаты на олимпиадах регионального уровня или успешно прошедших конкурсный отбор.

Программа ориентирована на подготовку учащихся к участию в соревнованиях по информационной безопасности в формате CTF (Capture The Flag). Данный формат является современным и эффективным способом обучения, объединяющим теорию и практику в условиях, приближенных к реальным задачам специалистов по кибербезопасности. Программа построена по принципу «от простого к сложному»: закладывает фундаментальные основы и знакомит с основными категориями задач, углубляет знания и нацелена на отработку навыков для успешного выступления на серьезных соревнованиях.

1.3 Цели и задачи дополнительной общеобразовательной программы

Цель – удовлетворение индивидуальных потребностей обучающихся в интеллектуальном развитии, формировании компетенций в области информационной безопасности и подготовке к участию в соревнованиях по кибербезопасности в формате CTF (Capture The Flag) через освоение современных инструментов и технологий защиты информации.

Задачи:

– образовательные: сформировать системные знания по ключевым категориям CTF – криптография, стеганография, веб-безопасность, форензика, администрирование, обратная инженерия. Обучить работе со специализированным программным обеспечением и инструментарием (Kali Linux, Wireshark, Burp Suite, Ghidra и др.);

– воспитательные: сформировать навыки работы в команде, тайм-менеджмента и эффективной коммуникации в условиях стресса и ограниченного времени, развить аналитическое, алгоритмическое и креативное мышление для решения нестандартных задач;

– развивающие: развитие познавательного интереса к технике и программированию, логического и алгоритмического мышления, пространственного воображения, самостоятельности и творческих способностей учащихся.

1.4 Отличительные особенности данной общеобразовательной программы от уже существующих образовательных программ

Дополнительная общеобразовательная программа «Информационная безопасность» рассчитана на учащихся школ г. Кирова и Кировской области, обучающихся в 2025–2026 учебном году в 7–10 классах, проявляющих интерес и способности к информатике, программированию и информационной безопасности, показавших хорошие результаты на олимпиадах регионального уровня или успешно прошедших конкурсный отбор.

Учебный материал основан на авторских разработках, подготовленных специально для занятий по данной программе.

1.5 Формы и режим занятий

Все занятия проводятся в рамках третьей смены ДОЛ «Вишкиль».

Формы организации занятий: беседа, дискуссия, решение и обсуждение задач, разборы задач, консультации, личные и командные соревнования.

Режим занятий: 4–6 академических часов в день, включая перерывы. На занятиях применяются индивидуальные, групповые и коллективные формы работы.

1.6 Правила и критерии отбора обучающихся

Правила и критерии отбора на программу публикуются на официальном сайте ЦДООШ на странице https://cdoosh.ru/information-security/ не позднее чем за 75 дней до начала смены.

1.7 Ожидаемые результаты и способы определения их результативности

Результатами занятий являются повышение уровня знаний и умений учащихся в области информационной безопасности, развитие мыслительных процессов.

Основным средством диагностики является проверка решений задач самостоятельной работы и результаты заключительной олимпиады.

II СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебно-тематический план

Тема	Кол-во часов
1. Введение в ИБ и CTF. Этические нормы	4
2. Безопасная среда. Kali Linux. Командная строка	8
3. Криптография (Classic, XOR, Base64)	10
4. Стеганография (файлы, изображения)	4
5. Веб-технологии. Протокол HTTP/S. Инструменты	2
6. Уязвимости: SQLi, XSS	10
7. Компьютерная форензика (Basic Forensics)	8
8. Введение в Python для автоматизации в ИБ	8
9. Подготовка и участие в Internal CTF	6
Итого	**60**

2.2 Учебная программа

2.2.1 Введение в ИБ и CTF. Этические нормы

Теория (2 часа): Основные понятия информационной безопасности. История и философия CTF. Форматы соревнований (Jeopardy, Attack-Defense). Правовые основы и этический кодекс специалиста по кибербезопасности (ethical hacking).

Практика (2 часа): Регистрация на платформах CTFtime.org, HackTheBox. Разбор регламента типичных соревнований. Решение простейших задач на логику и общую эрудицию (trivia) в формате CTF.

2.2.2 Безопасная среда. Kali Linux. Командная строка

Теория (2 часа): Обзор дистрибутивов для пентеста. Архитектура и базовые принципы ОС Linux. Структура файловой системы. Основы управления процессами и правами доступа.

Практика (6 часов): Установка и настройка Kali Linux в виртуальной среде. Освоение командной строки (Bash): навигация, работа с файлами (cat, grep, find, strings), архивация, управление процессами (ps, kill). Сетевая диагностика (ping, netstat, nc). Написание простых bash-скриптов для автоматизации рутинных операций.

2.2.3 Криптография (Classic, XOR, Base64)

Теория (2 часа): Основные понятия криптографии: шифрование, дешифрование, ключ. Классические шифры (Цезарь, Атбаш, Виженер) и методы их взлома (частотный анализ). Математические основы XOR-шифрования. Принципы кодирования (Base64, Hex, URL-encoding).

Практика (8 часов): Решение задач на взлом классических шифров с по-

мощью скриптов и онлайн-инструментов (CyberChef). Написание программ на Python для реализации и взлома шифров. Анализ и декодирование данных в различных представлениях. Решение CTF-задач категории Crypto начального уровня.

2.2.4 Стеганография (файлы, изображения)

Теория (1 час): Понятие стеганографии. Обзор методов сокрытия информации: в файлах (метод конца файла), в изображениях (LSB-анализ), в аудиофайлах.

Практика (3 часа): Использование инструментов (binwalk, strings, hexedit, steghide, zsteg) для поиска скрытых данных. Извлечение флагов из файлов различных форматов. Анализ метаданных (exiftool). Решение CTF-задач категории Stego.

2.2.5 Веб-технологии. Протокол HTTP/S. Инструменты

Теория (1 час): Основы веб-технологий (HTTP-запросы/ответы, методы, cookies, сессии, заголовки). Принципы работы браузера и веб-сервера. Обзор инструментов для тестирования (Burp Suite, браузерные разработчики).

Практика (1 час): Перехват и анализ HTTP-трафика через Burp Proxy. Модификация запросов. Анализ исходного кода страниц.

2.2.6 Уязвимости: SQLi, XSS

Теория (2 часа): Природа уязвимостей. SQL-инъекции (SQLi): виды, принципы exploitation. Межсайтовый скриптинг (XSS): отраженный, хранимый, DOM-based.

Практика (8 часов): Поиск и эксплуатация SQLi (ручной и с помощью sqlmap). Обход базовых фильтров. Эксплуатация XSS: похищение cookies, выполнение произвольного JavaScript. Работа с учебными стендами (например, OWASP WebGoat, bWAPP). Решение CTF-задач категории Web.

2.2.7 Компьютерная форензика (Basic Forensics)

Теория (2 часа): Введение в компьютерную форензику. Типы цифровых артефактов. Основы анализа файловых систем и сетевого трафика.

Практика (6 часов): Анализ дампов сетевого трафика (Wireshark): поиск переданных файлов, паролей, ключей. Исследование образов дисков и файловых систем (autopsy, binwalk, strings). Извлечение скрытых данных из файлов различных форматов. Анализ метаданных. Решение CTF-задач категории Forensics.

2.2.8 Введение в Python для автоматизации в ИБ

Теория (2 часа): Базовый синтаксис Python. Обзор полезных библиотек для ИБ (requests, sockets, pwntools).

Практика (6 часа): Написание скриптов для автоматизации: HTTP-запросы к веб-приложениям, взаимодействие с сетевыми портами, декодирование данных, простой брутфорс.

2.2.9 Подготовка и участие в Internal CTF

Практика (6 часов): Командное участие в полноценном внутреннем CTF-соревновании формата Jeopardy, включающем задачи всех пройденных категорий. Закрепление навыков, применение изученного инструментария, отработка стратегии решения задач и тайм-менеджмента.

III ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Вид аттестации	Формы контроля	Виды оценочных материалов
Входящая	Участие во вступительном тестировании	Результаты тестирования
Текущая	Выполнение практических заданий	Протоколы выполнения заданий
Итоговая	Участие в итоговых соревнованиях	Результаты соревнований

IV ОРГАНИЗАЦИОННО–ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1 Учебно-методическое и информационное обеспечение программы

1. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва: ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.

2. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.

3. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие / Р. Н. Гилязова. — Санкт-Петербург : Лань, 2020. — 44 с. — ISBN 978-5-8114-4294-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130179 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография - М.: Солон-Пресс, 2017. — 262 с. — ISBN 978-5-91359-173-9.

5. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 13.07.2021).

— Режим доступа: для авториз. пользователей.

6. Журавлев, А. Е. Инфокоммуникационные системы: протоколы, интерфейсы и сети. Практикум : учебное пособие для спо / А. Е. Журавлев. — Санкт-Петербург : Лань, 2020. — 192 с. — ISBN 978-5-8114-5633-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152624 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

7. Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

8. Кибербезопасность: что нужно знать о новом виде защиты? - https://stepik.org/course/69690/syllabus

9. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114- 5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

10. Лившиц И.И. Нормативно-методическое обеспечение информационной безопасности - Учебно-методическое пособие. – СПб: Университет ИТМО, 2021. – 68 с.

11. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

12. Математика в кибербезопасности - https://stepik.org/course/62247/syllabus

13. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

14. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-7906-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167185 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

15. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации)

[Электронный ресурс] : учебное пособие / В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 176 с. — Режим доступа: https://e.lanbook.com/book/111084. — Загл. с экрана.

16. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/175506 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

17. Федосеев В.А. Цифровые водяные знаки и стеганография - 2-е изд., испр. и дополн. — Самара: Самарский университет, 2019. — 144 с. — ISBN 978-5-7883-1370-2 40. Хасанов Р.И. Основы стеганографии - Оренбург: Оренбургский государственный университет, 2017. — 102 с.

18. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

4.2 Материально-технические условия реализации программы

Перечень необходимого оборудования, материалов и программного обеспечения для реализации программы

Для педагога:

- компьютер, подключенный к сети Интернет;
- проектор;
- принтер;
- установленная виртуальная машина с образом Linux и сервером для выдачи тасков;
- пакет офисных программ, включающий редактор презентаций, текстовый редактор, табличный редактор;
- средство для просмотра документов в формате PDF.

Предполагается использование раздаточного материала в бумажном или электронном виде с содержанием лекционного материала, заданиями и условиями задач.

Для учащегося:

- компьютер, подключенный к сети Интернет;
- установленная виртуальная машина с образом Linux;
- средство для просмотра документов в формате PDF.