Программа «Информационная безопасность и системное администрирование» разработана в соответствии с требованиями нормативных документов:

- Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;
- Распоряжения Правительства РФ от 31.03.2022 № 678-р «Об утверждении Концепции развития дополнительного образования детей до 2030 года и плана мероприятий по ее реализации» (с изменениями и дополнениями);
- Приказа Минпросвещения России от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (Зарегистрировано в Минюсте России 26.09.2022 № 70226);
- Постановления Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» (вместе с «СП 2.4.3648-20. Санитарные правила…») (Зарегистрировано в Минюсте России 18.12.2020 № 61573);
- Постановления Правительства РФ от 26.12.2017 № 1642 (с изменениями и дополнениями) «Об утверждении государственной программы Российской Федерации «Развитие образования
- Распоряжения Правительства РФ от 29.05.2015 № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года».

Направленность программы: техническая.

Уровень освоения программы: стартовый.

Актуальность программы

Актуальность дополнительной общеобразовательной программы «Информационная безопасность и системное администрирование» обусловлена стратегическим вектором Российской Федерации на обеспечение технологического суверенитета, импортозамещение в сфере информационных технологий и защиту критической информационной инфраструктуры.

Современный ИТ-рынок испытывает острый дефицит специалистов, способных администрировать отечественные операционные системы и обеспечивать безопасность данных. Большинство государственных организаций, крупных корпораций и объектов инфраструктуры осуществляют переход на решения на базе ядра Linux, в частности, на экосистему ALT Linux («Базальт СПО»).

Кроме того, современная разработка и администрирование программного обеспечения невозможны без технологий контейнеризации (Docker, Docker Compose). Обучение школьников сквозным технологиям DevOps/DevSecOps и методам защиты сетей со школьной скамьи позволяет сформировать у них инженерное мышление, навыки кибергигиены и заложить прочный фундамент для их ранней профессиональной ориентации в сфере информационной безопасности.

Отличительные особенности программы

- **Полная опора на отечественное ПО (Импортоориентированность):** Обучение строится на базе ОС «AltLinux Образование». Это дает учащимся уникальные и востребованные в РФ компетенции.
- **Фокус на технологии контейнеризации (DevOps/DevSecOps):** В программу интегрирован глубокий блок по работе с Docker и Docker Compose. Подростки учатся разворачивать современные мультиконтейнерные микросервисные архитектуры.
- **Практико-ориентированный подход «Проблема — Решение»:** Более 70% учебного времени отведено под лабораторные и практические работы в изолированных виртуальных средах. Ошибки в конфигурациях поощряются как элемент поиска неисправностей.
- **Сквозная интеграция информационной безопасности:** Киберзащита изучается непрерывно. При развертывании любого сервиса учащиеся настраивают права доступа, брандмауэр UFW/iptables и проводят аудит логов.

Цель и задачи программы

Цель программы: формирование у учащихся комплексных теоретических знаний и практических инженерных компетенций в области системного администрирования отечественных операционных систем (на базе ALT Linux), проектирования защищенных компьютерных сетей и применения технологий контейнеризации (Docker, Docker Compose) для ранней профессиональной ориентации в сфере информационных технологий и кибербезопасности.

Задачи программы:

- **Обучающие (предметные):** Ознакомить с архитектурой ПК; сформировать навыки установки и администрирования ALT Linux через GUI и CLI Bash; научить проектировать сети и настраивать службы (DNS, DHCP, SSH, Docker).
- **Развивающие (метапредметные):** Развивать системное и аналитическое мышление при поиске программных и аппаратных неисправностей; формировать навыки проектной командной деятельности.
- **Воспитательные (личностные):** Воспитывать культуру ответственного поведения в сети Интернет (кибергигиену), бережное отношение к технике и интерес к инженерным ИТ-профессиям.

Категория обучающихся: программа предназначена для учащихся в возрасте от 12 до 16 лет, не требует предварительных знаний и входного тестирования.

Срок реализации программы: программа рассчитана на 1 год, количество учебных часов – 144 (из расчёта 6 учебных часов в неделю).

Формы и режим занятий

Форма обучения: очная, очная с применением дистанционных технологий.

Режим занятий: занятия проводятся в группах до 12 человек, длительность одного занятия составляет 3 академических часа, периодичность занятий – 2 раза в неделю. Продолжительность одного академического часа – 35 минут. После окончания одного академического часа организовывается перерыв длительностью 5 минут для проветривания помещения и отдыха обучающихся.

Планируемые (ожидаемые) результаты программы

После прохождения курса обучающиеся:

должны оперировать следующими понятиями:

- информационная инфраструктура;
- компьютерные комплектующие: центральный процессор, оперативная память, видеоадаптер, жесткий диск, твердотельный накопитель, материнская плата, оптический привод, сетевая карта, блок питания, компьютерный корпус;

- устройства ввода (клавиатура, мышь, сенсорный экран), устройства вывода (монитор/дисплей, принтер):

- контроллер (памяти, периферии), шина данных, шины PCI и PCI Express, слот расширения:

- BIOS, CMOS, UEFI, POST;

- операционная система (Windows, Linux, OS X);

- загрузчик ОС;

- алгоритм, компьютерная программа, исполняемый файл, динамическая библиотека, приложение, API, кросс-платформенность;

- раздел, файловая система, файл, имя файла, расширение, атрибуты файла;

- драйвер;

- лицензионное соглашение;

- пользовательский интерфейс (графический интерфейс, командная строка);

- переменная среды;

- командный (пакетный) файл;

- установка ПО, мастер установки, автоматическая установка;

- пользователь, учетная запись, группа, права пользователя, профиль пользователя;

- панель управления, консоль управления компьютером, оснастка, диспетчер (устройств, задач), планировщик заданий, автозагрузка, ассоциации файлов;

- компьютерная сеть, топология сети, хост;

- витая пара;

- повторитель, концентратор, коммутатор, сетевой мост, маршрутизатор;

- кадр, пакет, заголовок, протокол, стек протоколов;

- TCP/IP, Ethernet, IP-адрес, маска подсети, DHCP, ICMP, TCP, UDP, порт;

- DNS, доменное имя, HTTP, FTP, URL, URI, URN, прокси-сервер, NAT, ICS:

- веб-сервер, WWW;

- Wi-Fi, идентификатор сети (SSID), WPA, AES, ключ сети (PSK);

- VPN, PPTP, L2TP, PPPoE, IPSec, SSTP;

- рабочая группа, сетевой путь, общий сетевой ресурс, сетевой диск;

- компьютерный вирус, троянская программа, сетевой червь, блокировщик, фишинг, DoS (DDoS);

- антивирус, межсетевой экран (брандмауэр, файерволл), система обнаружения вторжений;

- резервное копирование, образ системы.

Должны *уметь:*

- собирать компьютер из комплектующих;

- устанавливать операционную систему Linux (Ubuntu);

- устанавливать драйверы оборудования;

- управлять учетными записями пользователей (создавать, удалять, назначать права);

- персонализировать внешний вид и рабочую среду Linux;

- пользоваться командной строкой и создавать командные файлы;

- обжимать и тестировать витую пару;

- настраивать параметры протокола IPv4: IP-адрес, маску подсети, основной шлюз, адреса DNS-серверов;

- настраивать маршрутизацию на компьютере с Linux;

- настраивать параметры общего доступа к сетевым ресурсам;

- настраивать Wi-Fi-маршрутизатор;

- организовать защиту от вредоносных программ и потери данных: установить и настроить антивирус, межсетевой экран, организовать резервное копирование;

- диагностировать и устранять неисправности аппаратного обеспечения ПК;

- диагностировать и устранять неисправности сети;

- диагностировать и устранять неисправности ПО.

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Программа реализуется при наборе группы в течение учебного года. В очной форме проводится на базе Центра цифрового образования «IT-куб» ГБОУ ДПО ПО «Центр оценки качества образования».

СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

Официальная документация и базы знаний разработчика (Базальт СПО)

1. Портал официальной документации BaseALT — https://docs.altlinux.org — полные обновляемые руководства системного администратора по линейке дистрибутивов ALT Linux (Рабочая станция, Сервер, Образование). [1]
2. Вики-документация сообщества ALT Linux Wiki — https://www.altlinux.org — крупнейшая открытая база прикладных инструкций, разборов системных логов и решений по настройке периферийного оборудования [1.3].
3. Образовательный портал «Альт Академия» — https://kurs.basealt.ru — методические материалы, дистанционные курсы и учебные программы для преподавателей ИТ-дисциплин [1.3].
4. Форум поддержки пользователей ALT Linux — https://forum.altlinux.org — площадка для консультаций, разбора баг-репортов и обмена опытом администрирования.

Основная учебная литература и методические пособия

1. Губина Т. С., Костромин В. А. Администрирование ОС «Альт». Часть 1. Учебное пособие. — М.: ООО «Базальт СПО», 2024. (Базовые концепции, пользователи, права доступа)
2. Губина Т. С., Костромин В. А. Администрирование ОС «Альт». Часть 2. Учебное пособие. — М.: ООО «Базальт СПО», 2024. (Загрузка системы, мониторинг, логирование, Systemd).
3. Коллектив авторов AU_TEAM совместно с «Базальт СПО». Настольная книга будущего сисадмина — ALT Linux. Практикум для подготовки к демонстрационным экзаменам по стандартам СПО по сетевому и системному администрированию. — М., 2025.
4. Поляков В. О. Контейнеризация приложений в Docker и Docker Compose для начинающих инженеров. — М.: ДМК Пресс, 2025. (Пошаговое написание Dockerfile и yaml-манифестов)
5. Киренберг А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: Учебное пособие. — Кемерово: КузГТУ им. Т.Ф. Горбачева, 2022. — 119 с. (Теория сетевой безопасности и межсетевых экранов).

Дополнительная техническая литература (Справочники)

1. Немет Э., Снайдер Г., Хейн Т. Unix и Linux: руководство системного администратора. 5-е изд. — Пер. с англ. — СПб.: Альфа-книга, 2021. — 1168 с. (Мировая классика системного администрирования).
2. Таненбаум Э., Бос Х. Современные операционные системы. 5-е изд. — СПб.: Питер, 2023. — 1120 с. (Архитектура ядер, процессов и управления памятью) [1.3].
3. Лукас М. Изучаем Bash. Скрипты и автоматизация задач в Linux. — Пер. с англ. — М.: Символ-Плюс, 2022.

Профильные интернет-ресурсы по DevOps и кибербезопасности

1. Официальный портал документации Docker (англ.) — docker.com — справочник по инструкциям сборки образов и синтаксису утилиты Docker Compose
2. Информационный ресурс «Хабр» (Хабрахабр) — https://habr.com — статьи, практические кейсы, разборы уязвимостей и ИТ-инфраструктур в хабах «Linux», «Docker», «Информационная безопасность»
3. Проект информационной безопасности «Codeby» — https://codeby.net — профильный форум и статьи по поиску уязвимостей, тестированию на проникновение и сетевому аудиту.