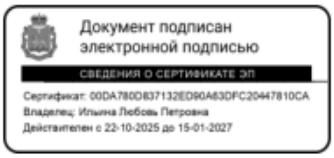
Министерство образования Псковской области

Государственное бюджетное образовательное учреждение дополнительного профессионального образования Псковской области «Центр оценки качества образования»

РАССМОТРЕНО
Научно-методическим советом
протокол № 7
от 31.08.2026 г.

УТВЕРЖДАЮ
Директор ГБОУ ДПО ПО «ЦОКО»



Л.П. Ильина

« 01»_____09_____ 2026 г.

Дополнительная общеразвивающая программа для детей

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Уровень: стартовый

Направленность: техническая

Возраст обучающихся: 12-16 лет

Срок реализации: 1 год

Составитель:
Прокофьев Алексей Валерьевич,
педагог дополнительного образования
центра цифрового образования «IT-куб»

г. Псков, 2026 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

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.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

№ темы	Наименование разделов и тем	Всего (час)	Теория (час)	Практика (час)	Форма аттестации/ контроля
Модуль 1	**Архитектура ПК и развертывание ОС ALT Linux**	**24**	**6**	**18**	
1.1	Вводное занятие. Инструктаж по ТБ. Входное тестирование.	2	1	1	Тестирование (входной контроль)
1.2	Архитектура современного ПК, подбор комплектующих, диагностика.	4	1	3	Опрос, практическая работа
1.3	Философия Open Source. Линейка дистрибутивов ALT Linux.	2	1	1	Контрольное собеседование
1.4	Виртуализация. Настройка сред Oracle VirtualBox под ALT Linux.	4	1	3	Практическая работа
1.5	Чистая установка ОС ALT Linux на ВМ. Разметка дисков.	6	1	5	Лабораторная работа
1.6	Знакомство с GUI (графической средой) и системная настройка.	4	1	3	Экспресс-контроль
Модуль 2	**Командная строка Bash и системное администрирование**	**36**	**10**	**26**	
2.1	Знакомство с CLI (терминалом). Навигация и работа с файлами.	6	2	4	Практическая работа
2.2	Концепция «Всё есть файл». Файловая структура Linux (FHS).	4	1	3	Устный опрос
2.3	Текстовые редакторы в консоли (Nano, Vim). Изменение конфигов.	4	1	3	Практическое задание
2.4	Управление пользователями, группами. Права доступа (chmod/chown).	6	2	4	Лабораторная работа
2.5	Работа с репозиторием «Сизиф» и пакетным менеджером APT-RPM.	6	2	4	Проверка репозиториев

2.6	Процессы, демоны и управление службами через systemctl.	6	1	5	Лабораторная работа
2.7	Автоматизация рутины: основы написания скриптов на Bash.	4	1	3	Защита мини-скрипта
Модуль 3	**Сетевое администрирование в среде ALT Linux**	**28**	**8**	**20**	
3.1	Модель OSI и стек TCP/IP. Физический уровень (обжим витой пары).	4	2	2	Практическая работа
3.2	IP-адресация, маски подсетей, базовая настройка сети в ALT.	6	2	4	Лабораторная работа
3.3	Сетевая диагностика из консоли (ping, traceroute, ip, ss).	4	1	3	Решение ситуационных кейсов
3.4	Протокол SSH. Организация безопасного удаленного доступа.	6	1	5	Лабораторная работа
3.5	Сетевые службы: развертывание базового веб-сервера (Nginx/Apache).	4	1	3	Проверка работоспособности сайта
3.6	Промежуточная аттестация. Практический зачет «Локальная сеть».	4	1	3	Практический зачет
Модуль 4	**Контейнеризация с Docker & Docker Compose**	**28**	**6**	**22**	
4.1	Введение в контейнеризацию. Архитектура Docker. Установка в ALT.	4	2	2	Фронтальный опрос
4.2	Базовые операции с контейнерами (run, ps, stop, rm, logs).	4	1	3	Практическое задание
4.3	Сборка собственных образов. Написание и оптимизация Dockerfile.	6	1	5	Лабораторная работа
4.4	Сети в Docker (bridge, host) и проброс сетевых портов.	4	1	3	Защита сетевой конфигурации
4.5	Постоянное хранение данных: Docker Volumes и Bind Mounts.	4	1	3	Лабораторная работа
4.6	Оркестрация микросервисов:	6	0	6	Защита мультиконтейнерного стека

	манифесты docker-compose.yml.				
Модуль 5	**Информационная безопасность, аудит и защита проектов**	**28**	**10**	**18**	
5.1	Классификация кибератак. Основы шифрования и SSL/TLS.	4	2	2	Семинар, дискуссия
5.2	Настройка сетевого экрана (файрвола) через UFW / iptables.	4	2	2	Лабораторная работа
5.3	Сканирование сетей на уязвимости с помощью утилиты Nmap.	4	1	3	Практическая работа
5.4	Анализ трафика в Wireshark и журналирование системы (journalctl).	4	1	3	
5.5	Разработка итоговых командных проектов (распределение ролей).	6	2	4	Наблюдение преподавателя
5.6	Итоговая аттестация. Публичная защита проектов (Live Demo).	6	2	4	Публичная защита проекта
	ИТОГО:	**144**	**40**	**104**	

2.2. Учебно-тематический план

Наименование модуля	Всего (ч)	Теория (ч)	Практика (ч)
Модуль 1. Архитектура ПК и развертывание ОС ALT Linux	24	6	18
Модуль 2. Командная строка Bash и администрирование	36	10	26
Модуль 3. Сетевое администрирование в ALT Linux	28	8	20

Модуль 4. Контейнеризация с Docker & Docker Compose	28	6	22
Модуль 5. Информационная безопасность и защита проектов	28	10	18
Итого	144	40	104

2.3. Содержание

Модуль 1. Архитектура ПК и развертывание ОС ALT Linux (24 часа)

Занятие 1-2: Вводный урок. Правила техники безопасности в ИТ-лаборатории. Входное тестирование компьютерной грамотности.
Занятие 3-4: Архитектура современного персонального компьютера. Разбор назначения комплектующих (CPU, RAM, SSD, материнская плата). Модульный ремонт.
Занятие 5-6: Практикум по сборке системного блока. Подбор комплектующих под техническое задание, диагностика неполадок при старте (POST-коды).
Занятие 7-8: История операционных систем UNIX/Linux. Философия Open Source и лицензии GPL. Обзор дистрибутивов «Базальт СПО» (ALT Linux).
Занятие 9-10: Понятие виртуализации. Установка и базовая настройка Oracle VirtualBox. Создание конфигурации под виртуальную машину (ВМ) Linux.
Занятие 11-12: Практическая работа: «Чистая» установка ОС ALT Linux Рабочая станция на виртуальную машину. Этапы начальной загрузки.
Занятие 13-14: Лабораторная работа №1: Разметка дискового пространства в Linux. Создание корневого раздела /, домашнего /home и раздела подкачки swap.
Занятие 15-16: Знакомство с графической оболочкой (GUI) ALT Linux. Настройка региональных параметров, раскладки клавиатуры и монитора.
Занятие 17-18: Архитектура файловой системы Linux. Изучение стандарта FHS (файловая иерархия: /etc, /var, /home, /root, /bin).
Занятие 19-20: Пользователи и суперпользователь root. Понятие административных привилегий. Авторизация и переключение контекста.
Занятие 21-22: Подключение и настройка периферийных устройств (принтеры, накопители). Проверка логов подключения оборудования через GUI.

Занятие 23-24: Обобщающее занятие по Модулю 1. Экспресс-тестирование навыков развертывания и базовой конфигурации операционной системы.

Модуль 2. Командная строка Bash и системное администрирование (36 часов)

Занятие 25-26: Введение в CLI (интерфейс командной строки). Командный интерпретатор Bash. Горячие клавиши терминала, вызов справки (man, --help).

Занятие 27-28: Базовая навигация в терминале. Команды перемещения и просмотра содержимого каталогов (pwd, cd, ls). Абсолютные и относительные пути.

Занятие 29-30: Манипуляция файловой структурой из консоли. Создание, копирование, перемещение и удаление файлов и папок (mkdir, touch, cp, mv, rm).

Занятие 31-32: Философия Linux «Всё есть файл». Понятие стандартных потоков ввода, вывода и ошибок (stdin, stdout, stderr). Перенаправление потоков (>, >>).

Занятие 33-34: Консольные текстовые редакторы. Работа в текстовом редакторе nano. Создание первых конфигурационных файлов.

Занятие 35-36: Продвинутый текстовый редактор vim. Режимы работы (командный, редактирования, визуальный). Базовые команды сохранения и выхода (:w, :q!).

Занятие 37-38: Лабораторная работа №2: Управление учетными записями. Создание пользователей и групп (useradd, groupadd). Работа с файлами /etc/passwd и /etc/group.

Занятие 39-40: Разграничение прав доступа в Linux. Классические права (Read, Write, Execute) для владельца, группы и остальных. Команда chmod.

Занятие 41-42: Смена владельцев файлов. Использование команды chown. Понятие утилиты безопасного делегирования прав sudo и конфигурация /etc/sudoers.

Занятие 43-44: Экосистема пакетов ALT Linux. Понятие репозитория и независимой базы «Сизиф». Инструменты работы с ПО: пакетный менеджер APT-RPM.

Занятие 45-46: Практика администрирования ПО. Поиск, установка, обновление и удаление программ через команды apt-get update, apt-get install, apt-get remove.**Занятие 47-48:** Управление процессами в Linux. Понятие PID (идентификатора процесса) и родительских процессов. Мониторинг ресурсов через консольные утилиты ps, top, htop.

Занятие 49-50: Жизненный цикл процессов. Принудительное завершение зависших задач (kill, killall). Перевод процессов в фоновый режим.

Занятие 51-52: Менеджер системных служб Systemd. Понятие юнитов и демонов. Управление фоновыми службами с помощью команды systemctl (start, stop, restart, status, enable).

Занятие 53-54: Лабораторная работа №3: Настройка автоматического запуска служб при старте ALT Linux. Анализ времени загрузки хоста.

Занятие 55-56: Введение в автоматизацию. Понятие автоматических сценариев (скриптов) на языке Bash. Переменные, циклы и условия.
Занятие 57-58: Практика создания Bash-скриптов для системных нужд. Реализация простейшего автоматического резервного копирования файлов.
Занятие 59-60: Защита практических мини-скриптов. Подведение итогов Модуля 2. Анализ частых ошибок администрирования.

Модуль 3. Сетевое администрирование в среде ALT Linux (28 часов)

Занятие 61-62: Теория компьютерных сетей. Сетевые модели OSI и TCP/IP. Физический уровень: типы кабелей, стандарты обжима витой пары.
Занятие 63-64: Практикум: Ручной обжим патч-корда (прямой и перекрестный кабели). Тестирование кабеля на обрыв жил прибором-тестером.
Занятие 65-66: Логическая структура сети. IPv4-адресация, классы адресов, маски подсетей. Понятие шлюза по умолчанию (Default Gateway).
Занятие 67-68: Лабораторная работа №4: Настройка сетевых интерфейсов в ALT Linux через консоль. Назначение статических IP-адресов. Конфигурация файла /etc/net/ifaces/.
Занятие 69-70: Инструменты сетевой диагностики. Проверка доступности узлов и трассировка маршрутов из терминала Linux (ping, traceroute).
Занятие 71-72: Мониторинг сетевых соединений. Изучение утилит ip address, ip route, ss и netstat. Просмотр открытых портов хоста.
Занятие 73-74: Разрешение сетевых имен. Принципы работы службы DNS. Конфигурация файла /etc/resolv.conf. Диагностика DNS-запросов утилитами nslookup и dig.
Занятие 75-76: Принципы работы динамической конфигурации сетей. Изучение протокола DHCP. Настройка получения IP-адреса ВМ в автоматическом режиме.
Занятие 77-78: Безопасный удаленный доступ. Протокол SSH. Установка и запуск службы sshd на сервере под управлением ALT Linux. Подключение через PuTTY/Терминал.
Занятие 79-80: Лабораторная работа №5: Повышение безопасности SSH. Отключение root-авторизации по паролю, переход на защищенный доступ по SSH-ключам.
Занятие 81-82: Введение в сетевые веб-службы. Архитектура клиент-серверных веб-приложений. Развертывание и базовая настройка веб-сервера Nginx в ALT Linux.
Занятие 83-84: Практикум: Конфигурирование виртуальных хостов в Nginx. Размещение простой статической HTML-страницы и проверка ее доступности с хост-машины.
Занятие 85-86: Промежуточная аттестация по курсу. Практический комплексный зачет «Локальная сеть»: объединение 3 виртуальных машин в сеть с веб-сервером.

Занятие 87-88: Разбор зачетных работ. Подведение итогов промежуточной аттестации. Анализ типичных сетевых сбоев.

Модуль 4. Контейнеризация с Docker & Docker Compose (28 часов)

Занятие 89-90: Эволюция ИТ-архитектур. Понятие контейнеризации. Сравнительный анализ: почему контейнер Docker легче и быстрее классической виртуальной машины.
Занятие 91-92: Архитектура экосистемы Docker. Роли демона (dockerd), клиента (docker CLI) и облачного хранилища образов Docker Hub. Установка Docker в ОС ALT Linux.
Занятие 93-94: Первые шаги в Docker. Базовые команды CLI. Запуск тестовых контейнеров, просмотр логов и статуса работы (docker run, docker ps, docker logs).
Занятие 95-96: Жизненный цикл контейнера. Остановка, перезапуск, удаление контейнеров и очистка дискового пространства от кэша (docker stop, docker rm, docker system prune).
Занятие 97-98: Понятие образов (Images). Слоистая структура файловой системы образов UFS. Скачивание, тегирование и удаление образов из локального хранилища.
Занятие 99-100: Концепция "Infrastructure as Code" (Инфраструктура как код). Знакомство с манифестом Dockerfile. Разбор ключевых инструкций: FROM, RUN, ENV.
Занятие 101-102: Лабораторная работа №6: Написание кастомного Dockerfile для сборки собственного веб-приложения на базе Python или Node.js. Сборка командой docker build.
Занятие 103-104: Сетевое взаимодействие контейнеров Docker. Драйверы сетей: изолированный bridge, сквозной host, отключенный none. Создание кастомных сетей.
Занятие 105-106: Проброс портов контейнера на реальный хост (-p). Обеспечение сетевой доступности приложений, развернутых внутри изолированного Docker-контейнера.
Занятие 107-108: Проблема эфемерности данных в контейнерах. Архитектура постоянного хранения данных. Понятие постоянных томов Docker Volumes и привязок папок Bind Mounts.
Занятие 109-110: Лабораторная работа №7: Настройка сохранения данных. Подключение Docker Volume к контейнеру базы данных (СУБД) для защиты информации от удаления.
Занятие 111-112: Введение в оркестрацию микросервисов. Зачем нужен Docker Compose. Синтаксис и структура декларативных конфигурационных файлов docker-compose.yml.
Занятие 113-114: Написание многоконтейнерного проекта в Docker Compose. Описание связей, переменных окружения (.env) и порядка запуска сервисов через depends_on.

Занятие 115-116: Практикум: Запуск комплексной веб-инфраструктуры (Связка: Веб-сервер Nginx + База данных PostgreSQL) одной консольной командой docker compose up -d.

Модуль 5. Информационная безопасность, аудит и защита проектов (28 часов)

Занятие 117-118: Введение в кибербезопасность. Классификация угроз. Понятие уязвимостей систем. Виды сетевых атак (Brute-force, MITM, DDoS). Концепция SecOps.

Занятие 119-120: Основы криптографии и защиты данных. Симметричное и асимметричное шифрование. Архитектура открытых ключей (PKI) и протокол SSL/TLS (HTTPS).

Занятие 121-122: Защита сетевого периметра хоста ALT Linux. Понятие межсетевого экрана (файрвола). Изучение базового инструмента фильтрации трафика Netfilter/iptables.

Занятие 123-124: Лабораторная работа №8: Конфигурирование простого файрвола UFW (Uncomplicated Firewall). Настройка правил блокировки портов и запрета сторонних IP.

Занятие 125-126: Сетевой аудит инфраструктуры. Сканер сети Nmap. Изучение методов обнаружения активных хостов, сканирования открытых портов и определения версий ОС.

Занятие 127-128: Практическая работа по киберзащите: Проверка собственного сервера утилитой Nmap со стороны. Нахождение «забытых» открытых портов и их устранение.

Занятие 129-130: Анализ сетевого трафика. Консольный сниффер tcpdump. Перехват пакетов данных. Понимание того, как хакеры видят незашифрованные пароли (HTTP/FTP).

Занятие 131-132: Графический анализатор пакетов Wireshark. Фильтрация трафика по протоколам (TCP, UDP, ICMP, DNS), чтение структуры заголовков сетевых пакетов.

Занятие 133-134: Системное журналирование как основа аудита безопасности. Изучение логов ALT Linux в каталоге /var/log/ (файлы messages, auth.log).

Занятие 135-136: Утилита journalctl для чтения логов Systemd. Поиск следов несанкционированного доступа (неудачные попытки ввода паролей по SSH, ошибки служб).

Занятие 137-138: Запуск итоговых проектов. Объединение учащихся в команды (по 2-3 человека), распределение ролей: *Системный администратор, DevOps, Специалист по ИБ*.

Занятие 139-140: Практикум по разработке выпускных работ. Консультации преподавателя, настройка конфигурационных файлов и проверка отказоустойчивости систем.

Занятие 141-142: Финальное тестирование итоговых стендов. Написание презентации проекта по структурированному шаблону центра «IT-куб». Подготовка к докладу.

Занятие 143-144: Итоговая аттестация. Публичная защита командных проектов (Live Demo в терминале, стресс-тесты преподавателя). Подведение итогов, вручение сертификатов.

3. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Контроль знаний, умений и навыков учащихся носит комплексный характер и осуществляется на протяжении всего учебного года. Система оценивания направлена на выявление уровня сформированности предметных компетенций (владение ALT Linux, Docker, сетевыми технологиями и инструментами ИБ) и метапредметных результатов (командная работа, системное мышление)

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Для успешной реализации программы и достижения учащимися заявленных результатов в центре цифрового образования «IT-куб» создается комплекс условий, включающий материально-техническое, программное, информационно-методическое и кадровое обеспечение.

Требования к оборудованию учебного класса (на группу из 12 человек):

Персональные компьютеры учащихся (минимально 12 шт. + 1 ПК преподавателя):
Процессор (CPU): 4–6 ядерный, с тактовой частотой не менее 3.0 ГГц (уровня Intel Core i5 / AMD Ryzen 5). В BIOS/UEFI обязательно должны быть активированы технологии аппаратной виртуализации (**Intel VT-x** или **AMD-V**).
Оперативная память (RAM): не менее **16 ГБ DDR4/DDR5**. Данный объем критически важен, так как на ПК одновременно разворачивается хостовая система, графическая среда, среда виртуализации и мультиконтейнерные стеки Docker.
Накопитель (Диск): **SSD (NVMe)** объемом от 240–500 ГБ. Скорость дисковой подсистемы напрямую влияет на время развертывания образов Docker и виртуальных машин.
Монитор: Диагональ не менее 21.5" с разрешением Full HD (1920x1080) для комфортной одновременной работы с терминалом и методическими материалами.
Сетевое оборудование учебной лаборатории:
Управляемый коммутатор (Switch) на 16–24 порта (скорость до 1 Гбит/с) для построения изолированных физических подсетей во время лабораторных работ.
Маршрутизатор (Роутер) с поддержкой Wi-Fi и возможностью гибкой настройки таблиц маршрутизации, DHCP-сервера и проброса портов.

Стабильный выделенный канал доступа в Интернет со скоростью не менее 100 Мбит/с на учебный класс (необходим для первоначального обновления пакетов из репозитория «Сизиф» и скачивания базовых образов с Docker Hub).

Дополнительное и демонстрационное оборудование:

Интерактивная панель или мультимедийный проектор с экраном для демонстрации преподавателем консольных команд и архитектурных схем.

Стендовое сетевое оборудование: бухта кабеля «витая пара» (UTP Cat 5e), коннекторы RJ-45, обжимной инструмент (кримперы), стрипперы для снятия изоляции и кабельный тестер (2–3 комплекта на класс для практической работы по обжиму).

Маркерная доска для проектирования сетевых топологий и разбора структуры YAML-файлов.

Программное обеспечение (ПО):

В соответствии с целями импортозамещения и технологического суверенитета, все программное обеспечение, используемое в рамках курса, является либо отечественным, либо распространяется по свободным лицензиям (Open Source):

1. **Хостовая операционная система:** Дистрибутив линейки **ALT Linux** (например, «Альт Рабочая станция» или «Альт Образование» от компании «Базальт СПО»).
2. **Среда виртуализации:** Свободно распространяемый гипервизор второго типа **Oracle VirtualBox** (версии 7.x и выше) с пакетом Extension Pack.
3. **Инструменты контейнеризации и оркестрации:** Среда выполнения контейнеров **Docker Engine** и утилита управления мультиконтейнерными приложениями **Docker Compose**, установленные из официального репозитория ALT Linux.
4. **Программы для работы с текстом и кодом:** Встроенные текстовые консольные редакторы nano и vim, графический редактор кода (например, VSCodium или Geany) для редактирования сложных манифестов YAML и Dockerfile.
5. **Специализированный софт для сетевого аудита и ИБ:** Сканер сети nmap, консольный перехватчик пакетов tcpdump, графический сетевой анализатор Wireshark, межсетевой экран ufw.

Информационно-методическое обеспечение

Информационная среда курса поддерживается локальными и сетевыми ресурсами:

- Печатные или электронные методические указания к лабораторным работам, разработанные педагогом (инструкционные карты, чек-листы самопроверки).
- Доступ к локальному зеркалу репозитория репозитория «Сизиф» (при необходимости экономии внешнего интернет-трафика).
- Постоянный доступ учащихся к базе знаний ALT Linux Wiki и официальной технической документации продуктов «Базальт СПО» для развития навыков самостоятельного поиска инженерных решений.

5. 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».

6. 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.