Департамент образования и науки Брянской области
Государственное автономное учреждение дополнительного образования
«Центр цифрового образования «АЙТИ-куб» Дятьковского района»

Рассмотрено на заседании
методического совета
Протокол № 1
от «25» августа 2026

Принято решением
педагогического совета
Протокол № 1
от «28» августа 2026

УТВЕРЖДАЮ
Директор ГАУ ДО «Центр цифрового образования «АЙТИ-куб»
Дятьковского района»
Приказ №75 - о/д от «28» августа 2026

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 460BB74F98651B2DFA6103F04894FB75
Владелец: Короткова Елена Николаевна
Действителен: с 17.07.2026 г. 9:01:55 по 10.10.2027 г. 9:01:55

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ (ОБЩЕРАЗВИВАЮЩАЯ) ПРОГРАММА

технической направленности

«Этичный хакинг и реверс-инжиниринг»

возраст обучающихся: 13-15 лет, срок реализации: 1 год

Автор-составитель:
Грязнов Егор Алексеевич,
педагог дополнительного образования

г. Дятьково, 2026

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная (общеразвивающая) программа «Этичный хакинг и реверс-инжиниринг» (далее - Программа), разработана в соответствии с нормативно-правовыми основаниями:

1. Федеральным Законом №273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»;

2. Указом Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»;

3. Концепцией развития дополнительного образования детей до 2030 года (утверждена распоряжением Правительства РФ от 31.03.2022 № 678-р);

4. Постановлением Правительства Российской Федерации от 26.12.2017 № 1642 «Об утверждении государственной программы Российской Федерации «Развитие образования» (с изменениями и дополнениями, действующими в 2026 году);

5. Стратегией развития образования в Российской Федерации до 2036 года с перспективой до 2040 года (утверждена распоряжением Правительства РФ от 18.05.2026 №1106-р);

6. Стратегией развития воспитания в Российской Федерации на период до 2030 года (утверждена распоряжением Правительства Российской Федерации от 29 мая 2015 № 996 р, с изменениями);

7. Приказом Министерства просвещения Российской Федерации от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (с изменениями, внесенными приказом Минпросвещения России от 30.01.2024 №55);

8. Письмом Министерства просвещения Российской Федерации от 19.03.2024 №05-545 «О направлении информации» (с обновленными методическими рекомендациями);

9. Постановлением Главного государственного санитарного врача Российской Федерации от 02.06.2026 № 19 «Об утверждении СП 2.4.2.4283-26 Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

10. Конвенцией ООН о правах ребёнка.

1.1. Направленность

Программа «Этичный хакинг и реверс-инжиниринг» имеет выраженную техническую и исследовательскую направленность. Данная направленность ориентирована на создание условий для вовлечения детей в изучение архитектуры программного обеспечения, принципов работы операционных систем и сетевых протоколов, в приобретение навыков в области информационной безопасности, криптографии, системного программирования, анализа вредоносного кода, поиска уязвимостей, тестирования на проникновение, защиты цифровых активов, а также в освоении низкоуровневых языков программирования и ассемблера. Программа содействует формированию у обучающихся современных знаний, умений и навыков в области защиты информации, алгоритмического мышления и инженерного подхода к решению нестандартных задач и предназначена для использования в системе дополнительного образования детей (старшего школьного возраста).

Сущность программы «Этичный хакинг и реверс-инжиниринг» целенаправлена на обучение детей принципам кибербезопасности с позиции «белой шляпы», формированию навыков выявления и устранения уязвимостей в информационных системах, безопасной разработке программного обеспечения и защите персональных данных на продвинутом уровне. Также ребята освоят инструментарий профессионального пентестера: научатся работать с отладчиками, дизассемблерами, анализаторами трафика и сетевыми сканерами. Особое внимание уделяется реверс-инжинирингу — умению

«читать» чужой код, восстанавливать логику работы программ и протоколов, а также исследовать вредоносное ПО в изолированной среде. Знание этих дисциплин закладывает фундамент для будущей карьеры в ИТ- и ИБ-сфере, позволяя не только защищать цифровую инфраструктуру, но и создавать надежные системы, устойчивые к взлому. Эти навыки пригодятся не только для участия в олимпиадах и CTF-соревнованиях, но и для любой деятельности, связанной с высокими технологиями и программированием.

1.2. Актуальность

В настоящее время выросла потребность общества в технически грамотных специалистах, полностью отвечающих социальному заказу по подготовке квалифицированных кадров в области информационной безопасности и противодействия киберугрозам. Данная Программа строится на концепции подготовки обучающихся к профессии этичного хакера (пентестера) – профессии будущего, выделенной в «Атласе новых профессий» (проект «Агентства стратегических инициатив» по исследованию рынка труда, 2015) и предполагающей проведение контролируемых вторжений в компьютерные системы, выявление уязвимостей, анализ защищённости цифровых инфраструктур, а также восстановление логики работы вредоносного и защищённого кода методами реверс-инжиниринга.

Программа актуальна тем, что не имеет аналогов на рынке общеобразовательных услуг и является своего рода уникальным образовательным продуктом в области информационных технологий. Знания, умения и навыки решения актуальных задач, полученные на занятиях, готовят обучающихся к самостоятельной проектно-исследовательской деятельности с применением современных технологий, включая отладку, дизассемблирование, сетевой анализ и криптографические исследования, что позволяет выпускникам не только уверенно ориентироваться в цифровой

среде, но и участвовать в реальных соревнованиях по кибербезопасности (CTF) и разрабатывать собственные инструменты защиты.

1.3. Педагогическая целесообразность

Данная Программа педагогически целесообразна, так как ее реализация органично вписывается в единое образовательное пространство данной образовательной организации. Программа соответствует новым стандартам обучения, которые обладают отличительной особенностью, способствующей личностному росту учащихся, его социализации и адаптации в обществе, формированию ответственного отношения к информационной безопасности и цифровой этике.

Программа «Этичный хакинг и реверс-инжиниринг» является целостной и непрерывной в течение всего процесса обучения. Развивает навыки исследовательской деятельности и системного анализа программного кода, сетевых протоколов и операционных сред, обнаружения скрытых уязвимостей и недокументированных возможностей в цифровых системах.

При изучении данной Программы обучающиеся научатся распознавать уязвимости и слабые места в программном обеспечении, выявлять вредоносный код и недекларированные возможности, анализировать логику работы зашифрованных и обфусцированных приложений, а также противостоять методам социальной инженерии и манипуляции, применяемым злоумышленниками. Полученные знания и умения позволят критически оценивать и классифицировать угрозы информационной безопасности, использовать полученные навыки для создания надёжных защищённых систем и нейтрализовать потенциальные каналы атак, обеспечивая цифровую безопасность как личную, так и корпоративную.

1.4. Новизна или отличительные особенности

Отличительной особенностью программы «Этичный хакинг и реверс-инжиниринг» является её фокус на решение практических задач. Это означает,

что в рамках обучения воспитанники обучаются не только теоретическим знаниям в области информационной безопасности и анализа программного кода, но и получают опыт и навыки по реальным примерам из практики кибербезопасности с использованием современных технологий (отладчики, дизассемблеры, снифферы, эмуляторы, sandbox-среды и фреймворки для тестирования на проникновение). В программе изучается полный спектр инструментов профессионального пентестера и исследователя безопасности для обнаружения уязвимостей, анализа вредоносного ПО и восстановления алгоритмов работы приложений. Освоение программы происходит в основном в процессе практической творческой деятельности, включая решение CTF-задач, участие в учебных киберучениях и разработку собственных скриптов и утилит для автоматизации безопасности.

1.5. Адресат Программы

Возраст обучающихся, участвующих в реализации данной программы - от 13 до 15 лет.

Образовательный процесс осуществляются в группах с обучающимися разного возраста. Программа предоставляет обучающимся возможность освоения учебного содержания занятий с учетом уровня их общего развития, способностей, мотивации. В рамках Программы предполагается реализация параллельных процессов освоения содержания Программы на разных уровнях доступности и степени сложности, с опорой на диагностику стартовых возможностей каждого из воспитанников.

В коллектив могут быть приняты все желающие, не имеющие противопоказаний по здоровью.

Количество обучающихся в одной группе варьируется от 8 до 12 человек.

Срок реализации Программы – 1 год (144 часа).

Формы обучения - сочетание очной и очно-заочной форм образования с применением электронного обучения и дистанционных образовательных технологий (Закон №273-ФЗ, гл.2, ст.17, п.2.).

Реализация Программы предполагает использование здоровьесберегающих технологий.

Занятия проводятся 2 раза в неделю по 2 академических часа. Продолжительность академического часа - 45 минут. После первой половины занятия организовывается перерыв 10 минут для проветривания помещения и отдыха обучающихся.

2. ОБУЧЕНИЕ

2.1. Цель и задачи

Целью Программы является получение навыков практической кибербезопасности и анализа программного кода, развитие творческих способностей у обучающихся к системному исследованию цифровых систем, выявлению уязвимостей и скрытых функций программного обеспечения, формирование культуры безопасной разработки и ответственного использования полученных знаний, а также подготовка обучающихся как компетентных специалистов в области защиты информации, умеющих работать с современными инструментами пентеста и реверс-инжиниринга для решения исследовательских, учебных и профессиональных задач.

Задачи Программы

Обучающие:

- формирование знаний о структуре и архитектуре операционных систем, сетевых протоколов и исполняемых файлов;
- формирование общекультурных навыков работы с технической документацией и исходными кодами;
- ознакомление с методами и средствами статического и динамического анализа программ, поиска уязвимостей и тестирования на проникновение;

- ознакомление обучающихся с основами исследовательской деятельности в области кибербезопасности;
- формирование навыка планирования, проведения и обработки результатов анализа защищённости информационных систем при помощи профессиональных инструментов (дизассемблеры, отладчики, сканеры уязвимостей, снифферы, фреймворки для эксплуатации);
- формирование способности выявлять слабые места в коде, восстанавливать логику работы приложений, обнаруживать вредоносные вставки и недекларированные возможности;
- формирование умения работать с полным пакетом инструментов исследователя безопасности (IDA Pro, Ghidra, OllyDbg, Wireshark, Metasploit, Burp Suite и др.).

Развивающие:

- создание условий для развития поисковой активности, исследовательского подхода к решению нестандартных задач;
- развитие самостоятельности и творческого подхода к анализу сложных систем;
- развитие логического, системного и алгоритмического мышления;
- способствование формированию умения практического применения полученных знаний для защиты цифровых активов;
- формирование у обучающихся способностей к самообучению и постоянному профессиональному росту в быстро меняющейся сфере ИБ;
- создание мотивации к участию в CTF-соревнованиях и конкурсах по кибербезопасности.

Воспитательные:

- развитие коммуникативной культуры обучающихся, как внутри проектных групп, так и в коллективе в целом, включая навыки командной работы при проведении пентестов;
- создание творческой атмосферы, обеспечивающей развитие личности, социализацию и эмоциональное благополучие каждого воспитанника;

• формирование информационной культуры и этического мышления, осознания личной ответственности за использование полученных знаний только в законных целях;

• воспитание ценностного отношения к безопасности своей и чужой цифровой среды, уважения к интеллектуальной собственности и приватности.

2.2. Учебный план

Таблица 1

№ п/п	Название раздела, темы	Общее кол-во часов	В том числе		Формы аттестации/ контроля
			Теория	Практика	
Введение		**2**	**1**	**1**	
1	Вводный инструктаж по ТБ. Знакомство с предметом	2	1	1	Опрос
Раздел 1. Основы этичного хакинга и информационной безопасности		**24**	**6**	**18**	
2	Понятие этичного хакинга, виды хакеров, правовые аспекты	6	1	5	Опрос, практическая работа
3	Основы информационной безопасности: угрозы, уязвимости, риски	6	2	4	
4	Методология тестирования на проникновение (OSSTMM, PTES)	6	2	4	
5	Сбор информации (OSINT) и разведка	6	1	5	
Раздел 2. Сетевые технологии и атаки		**24**	**8**	**16**	
6	Основы сетей OSI, TCP/IP, протоколы	6	2	4	Опрос, практическая работа
7	Сканирование сети и анализ трафика (Nmap, Wireshark)	6	2	4	
8	Атаки на сетевом уровне (ARP-spoofing, DoS)	8	2	6	
9	Беспроводные сети и их безопасность (Wi-Fi атаки)	4	2	2	
Раздел 3. Основы программирования для задач безопасности		**16**	**4**	**12**	
10	Основы Python для	4	2	2	Опрос,

№ п/п	Название раздела, темы	Общее кол-во часов	В том числе		Формы аттестации/ контроля
			Теория	Практика	
	пентеста: синтаксис, библиотеки				практическая работа
11	Написание скриптов для автоматизации сканирования и атак	6	1	5	
12	Безопасное программирование, общие уязвимости в коде	6	1	5	
Раздел 4. Реверс-инжиниринг и анализ вредоносного ПО		**14**	**4**	**10**	
13	Статический анализ: дизассемблеры (IDA Pro, Ghidra)	6	2	4	Опрос, практическая работа
14	Анализ вредоносных программ, распаковка, обход антиотладки. Исследование памяти и файловых систем	8	2	6	
Раздел 5. Инструменты пентеста и эксплуатация		**32**	**8**	**24**	
15	Фреймворк Metasploit: основы и использование	6	2	4	Опрос, практическая работа
16	Эксплуатация уязвимостей (buffer overflow, RCE)	8	2	6	
17	Постэксплуатация и закрепление в системе	10	2	8	
18	Социальная инженерия и методы обхода защиты	8	2	6	
Раздел 6. Веб-безопасность и криптография		**18**	**4**	**14**	
19	Основы веб-технологий (HTTP, Cookies, Sessions)	6	2	4	Опрос, практическая работа
20	Атаки на веб-приложения: SQL-инъекции, XSS, CSRF. Защита веб-приложений (WAF, шифрование)	12	2	10	
Проектная деятельность		**14**	**2**	**12**	
21	Обобщение материала, разработка проектов (CTF-задания, исследование уязвимостей,	14	2	12	Проектная работа

№ п/п	Название раздела, темы	Общее кол-во часов	В том числе		Формы аттестации/ контроля
			Теория	Практика	
	написание программ для автоматизации пентеста, реверс инжиниринга)				
Итого:		**144**	**37**	**107**	

2.3. Содержание учебного плана

Введение

Теория

Знакомство с работой творческого объединения, проведение инструкций по охране труда и техники безопасности. Входной контроль.

Раздел 1. Основы этичного хакинга и информационной безопасности

Теория

Понятие этичного хакинга, виды хакеров (белые, серые, чёрные), различия между пентестом и аудитом безопасности. Основные угрозы, уязвимости и риски. Классификация атак (активные, пассивные, внутренние, внешние). Методологии тестирования на проникновение (OSSTMM, PTES, OWASP). Знакомство с жизненным циклом атаки (разведка, сканирование, эксплуатация, постэксплуатация). Сбор информации из открытых источников (OSINT): поиск данных о доменах, IP-адресах, сотрудниках компаний.

Практика

Отработка методов OSINT с использованием поисковых систем, сервисов Whois, DNS-запросов, инструментов (theHarvester, Maltego). Сканирование сети с помощью Nmap: определение открытых портов, служб, ОС. Анализ полученных результатов. Составление отчёта о поверхности атаки для гипотетической организации.

Раздел 2. Сетевые технологии и атаки

Теория

Модель OSI и стек TCP/IP. Базовые протоколы: IP, ICMP, ARP, TCP, UDP, HTTP, DNS. Принципы маршрутизации и коммутации. Уязвимости сетевого уровня: ARP-spoofing, MAC-flooding, ICMP-атаки. Атаки на уровне L7 (веб-сценарии). Основы безопасности беспроводных сетей Wi-Fi: типы шифрования (WEP, WPA/WPA2), методы взлома (перехват рукопожатия, атаки на WPS).

Практика

Захват и анализ сетевого трафика в Wireshark: фильтрация, выделение подозрительных пакетов, восстановление сессий. Проведение ARP-отравления в локальной сети с целью перехвата данных. Подбор пароля к Wi-Fi сети с использованием aircrack-ng (на лабораторном стенде). Настройка фаервола и обнаружение вторжений (Snort/Suricata). Разработка скрипта для автоматического сканирования портов.

Раздел 3. Анализ мнений интернет-пользователей

Теория

Обзор языков, используемых в пентесте (Python, Bash, PowerShell). Основы синтаксиса Python: переменные, циклы, условия, функции, работа со строками и файлами. Библиотеки для сетевого взаимодействия (socket, requests, scapy). Принципы написания безопасного кода: проверка входных данных, избегание переполнения буфера, правильная работа с памятью. Типичные уязвимости в приложениях (инъекции, переполнение, небезопасная десериализация).

Практика

Написание простого портового сканера на Python. Создание сниффера для перехвата HTTP-заголовков. Разработка скрипта для брутфорса форм авторизации (с использованием библиотек requests и BeautifulSoup). Анализ собственного кода на наличие уязвимостей с помощью статических анализаторов (Bandit, Pylint). Решение CTF-задач по обратному инжинирингу простых программ на C и Python.

Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве

Теория

Архитектура процессоров x86/x64: регистры, система команд, стек, сегментация памяти. Основы ассемблера и машинных кодов. Форматы исполняемых файлов (PE, ELF, Mach-O). Различие статического и динамического анализа. Инструменты дизассемблирования (IDA Pro, Ghidra, Radare2) и отладки (OllyDbg, x64dbg, GDB). Методы обфускации и упаковки кода, распаковка UPX и других упаковщиков. Признаки вредоносного ПО: шифровальщики, бэкдоры, кейлоггеры.

Практика

Работа с дизассемблером: загрузка исполняемого файла, навигация по графу потока управления, распознавание основных конструкций. Динамическая отладка: установка точек останова, отслеживание изменения регистров и памяти, анализ вызовов API. Распаковка простого образца вредоносной программы (в изолированной среде). Составление алгоритма работы зашифрованного алгоритма. Создание отчёта по результатам реверс-инжиниринга с указанием потенциально опасных функций.

Раздел 5. Безопасность устройств и информации на них

Теория

Обзор фреймворков для автоматизации атак: Metasploit, Empire, Cobalt Strike. Структура эксплойта: шеллкод, обход DEP/ASLR, поиск гаджетов ROP. Уязвимости типа переполнение буфера и переполнение целочисленных значений. Веб-инструменты: Burp Suite, OWASP ZAP — перехват и модификация запросов. Методы постэксплуатации: сбор учётных данных, повышение привилегий, удалённое управление. Социальная инженерия: фишинг, претекстинг, подделка электронных писем.

Практика

Использование Metasploit для эксплуатации уязвимости в тестовой ОС (например, EternalBlue). Написание собственного модуля для Metasploit на

Ruby. Работа с Burp Suite: перехват и изменение GET/POST-запросов, подмена заголовков, репитер для ручного тестирования. Разработка фишинговой страницы (в целях обучения) для демонстрации рисков. Построение отчёта с рекомендациями по устранению найденных уязвимостей.

Раздел 6. Порядок действий ликвидации последствий сбоев системы

Теория

Архитектура веб-приложений: клиент-сервер, сессии, куки, REST API. Наиболее распространённые уязвимости OWASP Top 10: SQL-инъекции, XSS (межсайтовый скриптинг), CSRF, небезопасная аутентификация. Способы защиты: параметризованные запросы, валидация ввода, шифрование сессий, Content Security Policy. Основы криптографии: симметричные и асимметричные алгоритмы (AES, RSA), хеш-функции (MD5, SHA), цифровые подписи и сертификаты. Применение криптографии в блокчейне и безопасных протоколах (TLS/SSL).

Практика

Выполнение SQL-инъекции на учебном сайте (DVWA или подобном) с извлечением данных из БД. Создание XSS-скрипта для кражи cookie. Настройка HTTPS-сервера с самоподписанным сертификатом. Криптоанализ: подбор хешей с помощью словаря, расшифровка простого шифра методом частотного анализа. Разработка простого шифровальщика и дешифровщика на Python для понимания принципов.

Проектная деятельность

Теория

Самостоятельный выбор учащимися тем проектов в области этичного хакинга и реверс-инжиниринга. Обсуждение возможных направлений: разработка инструмента для автоматизации пентеста, исследование уязвимости конкретного ПО, создание стенда для CTF-задач, написание учебного руководства по безопасному программированию. Постановка целей, определение этапов работы, формирование проектных групп.

Практика

Реализация выбранного проекта: поиск и изучение литературы, патентный обзор (при необходимости), программирование, тестирование, оформление результатов. Подготовка презентации и защита проекта на итоговом мероприятии (например, в рамках школьной конференции или CTF-соревнования). Участие в реальных онлайн-олимпиадах и конкурсах по кибербезопасности для проверки полученных навыков в условиях, приближенных к профессиональным.

2.4. Планируемые результаты

Предметные результаты

Обучающийся будет:

- владеть основными приёмами работы в специализированных программах для тестирования на проникновение и анализа кода (дизассемблеры, отладчики, сканеры уязвимостей, фреймворки эксплуатации, анализаторы трафика);
- иметь представление об архитектуре операционных систем, сетевых протоколов и форматах исполняемых файлов (PE, ELF), а также о принципах работы низкоуровневого программного обеспечения;
- понимать методы и средства статического и динамического анализа программ, поиска уязвимостей и восстановления алгоритмов работы приложений;
- применять навыки планирования, проведения и обработки результатов исследования защищённости информационных систем при помощи профессиональных инструментов (Nmap, Wireshark, Burp Suite, Metasploit, IDA Pro, Ghidra, OllyDbg);
- уметь выявлять и критически оценивать слабые места в программном коде, конфигурациях сетевых служб и веб-приложениях, определять их потенциальную опасность;

- уметь определять признаки вредоносного поведения программ, обнаруживать скрытые функции, недекларированные возможности и закладки на основе анализа кода и сетевого трафика;
- уметь распознавать методы социальной инженерии, фишинговые атаки и способы обхода средств защиты, а также разрабатывать контрмеры для нейтрализации подобных угроз.

Личностные результаты

У обучающегося будут сформированы:

- устойчивый интерес к соблюдению этических норм и правовых ограничений в области информационной безопасности, осознание личной ответственности за применение полученных знаний исключительно в законных целях;
- умения проявлять в самостоятельной деятельности логическую культуру, системное мышление и компетентность при решении нестандартных задач;
- аналитическое, критическое и алгоритмическое мышление, способность к декомпозиции сложных систем;
- самостоятельность и самоорганизация, умение ставить цели и достигать их в условиях ограниченного времени (например, при участии в CTF соревнованиях);
- умение работать в команде, распределять роли и эффективно взаимодействовать при проведении коллективных пентестов и расследований;
- умение вести себя сдержанно и спокойно в стрессовых ситуациях, связанных с обнаружением критических уязвимостей или инцидентов безопасности.

Метапредметные результаты

Обучающийся научится:

- самостоятельно планировать последовательность своих действий для достижения поставленных целей (например, составление плана тестирования на проникновение или анализа вредоносного образца), а также грамотно

распределять свое время и ресурсы для получения максимально эффективного результата;

- организовать учебное сотрудничество и совместную деятельность с педагогом и сверстниками, в том числе при работе над групповыми проектами и в ходе совместного решения CTF-задач;
- продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты, особенно при обсуждении спорных технических решений;
- принимать решения в условиях неполной информации, а также умение формулировать, аргументировать и отстаивать своё мнение при защите результатов исследований и проектов перед аудиторией.

2.5. Контроль и оценка результатов обучения

Система отслеживания результатов обучающихся выстроена следующим образом:

- **входной контроль** (определение начального уровня знаний, умений и навыков);
- **промежуточный контроль** (промежуточная аттестация);
- **итоговый контроль** (итоговая аттестация).

Входной контроль по программе «Этичный хакинг и реверс-инжиниринг» проводится с целью выявления у обучающихся начальных представлений в области информатики, программирования, компьютерных сетей и основ информационной безопасности, а также оценки их мотивации и готовности к освоению материала повышенной сложности. Осуществляется по следующим параметрам:

- **техника безопасности** — знание правил работы с компьютерной техникой, понимание инструкций по технике безопасности при работе в изолированных виртуальных средах и с потенциально опасным кодом;

- **мотивированность** — интерес к теме этичного хакинга, реверс-инжиниринга и кибербезопасности, готовность к самостоятельной исследовательской деятельности;
- **базовая зрелость** — наличие базовых знаний о структуре компьютера, операционных системах, принципах работы сетей и интернета; умение выстраивать взаимодействие со сверстниками при обсуждении технических вопросов;
- **умелость** — начальные навыки работы с персональным компьютером, файловой системой, командной строкой, установка и настройка простого программного обеспечения, базовые навыки программирования (желательно, но не обязательно);
- **владение терминологией** — понимание основных понятий в области информационной безопасности (уязвимость, атака, защита, шифрование, вредоносное ПО, брандмауэр) и умение оперировать ими.

Входной контроль осуществляется самим педагогом в сентябре месяце на первых занятиях в свободной форме (собеседование, короткий тест или выполнение простого практического задания, например, навигация в командной строке Linux).

Промежуточная аттестация проводится в конце первого полугодия в декабре месяце. На усмотрение педагога промежуточный контроль может осуществляться в любой форме, например:

- в форме **презентации результатов исследования** (обучающийся демонстрирует выполненный анализ уязвимости, разбор вредоносного образца или созданный инструмент для пентеста);
- в виде **практического кейса** — решение на время задачи по сканированию сети, эксплуатации уязвимости или дизассемблированию простой программы с последующим устным объяснением действий;
- в форме **интерактивного тестирования** (например, викторина с вопросами по теории и практическими мини-заданиями, где учитывается правильность и скорость ответов);

- в виде **командного CTF-состязания**, где участники в командах решают задания по категориям (криптография, стеганография, взлом веб-приложений, реверс-инжиниринг, форензика).

Выбор формы остаётся за педагогом с учётом уровня подготовки группы и технических возможностей.

Итоговая аттестация проводится во втором полугодии (в конце каждого года обучения) — обязательно, в любой выбранной педагогом и обучающимся форме (прописанной в образовательной программе Центра). Как правило, итоговый контроль проходит в виде **защиты индивидуальных или групповых проектов**, которые могут включать:

- разработку собственного скрипта или утилиты для автоматизации пентеста;
- исследование реальной уязвимости (CVE) с демонстрацией эксплуатации в лабораторной среде и выработкой мер защиты;
- анализ вредоносной программы с использованием статического и динамического анализа (подготовка отчёта);
- создание CTF-задания для младших групп;
- подготовку учебного материала (видеоурок, статья, методическое пособие) по одной из тем программы.

Проект защищается перед комиссией (педагог, возможно, приглашённые эксперты). Оценивается не только техническая правильность, но и качество презентации, аргументация выводов, соответствие этическим и правовым нормам.

Критерии оценивания результативности определяются самим педагогом таким образом, чтобы можно было определить отнесенность обучающегося к одному из трёх уровней результативности: **высокий, средний, низкий**.

Согласно Положению «О форме, порядке и периодичности промежуточной и итоговой аттестации обучающихся в ГАУ ДО «Центр

цифрового образования «АЙТИ-куб» Дятьковского района», критерии оценки не должны противоречить следующим показателям:

- **высокий уровень** – успешное освоение обучающимися более 70% содержания Программы, подлежащей аттестации (обучающийся уверенно применяет инструментарий, способен самостоятельно решать задачи средней и высокой сложности, может объяснить логику своих действий);
- **средний уровень** – успешное освоение обучающимися от 50% до 70% содержания Программы, подлежащей аттестации (обучающийся владеет базовыми навыками, выполняет типовые задания, но испытывает трудности при решении нестандартных или комплексных задач);
- **низкий уровень** – успешное освоение обучающимися менее 50% содержания Программы, подлежащей аттестации (обучающийся демонстрирует фрагментарные знания, не может самостоятельно выполнить практические задания без помощи педагога).

Все результаты промежуточной и итоговой аттестации фиксируются в протоколах результатов аттестации обучающихся.

3. ВОСПИТАНИЕ

3.1. Цель, задачи, целевые ориентиры воспитания

В соответствии с законодательством Российской Федерации общей **целью воспитания** является развитие личности, самоопределение и социализация обучающихся на основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению; взаимного уважения; бережного отношения к культурному наследию и традициям многонационального народа

Российской Федерации, природе и окружающей среде (Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», ст. 2, п. 2).

Задачами воспитания по Программе являются:

- усвоение обучающимися знаний норм, духовно-нравственных ценностей, традиций, которые выработало Российское общество;
- формирование интереса к техническому творчеству;
- приобретение обучающимися опыта поведения, общения, межличностных и социальных отношений в составе учебной группы;
- создание, поддержка и развитие среды воспитания воспитанников, условий физической безопасности, комфорта, активностей и обстоятельств общения, социализации, признания, самореализации, творчества при освоении предметного и метапредметного содержания Программы.

Основные целевые ориентиры воспитания на основе российских базовых (конституционных) ценностей направлены на воспитание, формирование:

- понятия о своей российской гражданской принадлежности (идентичности), сознания единства с народом России и Российским государством в его тысячелетней истории и в современности, в настоящем, прошлом и будущем;
- российского национального исторического сознания на основе исторического просвещения, знания истории России, сохранения памяти предков;
- готовности к защите Отечества, способности отстаивать суверенитет и достоинство народа России и Российского государства, сохранять и защищать историческую правду;
- уважения прав, свобод и обязанностей гражданина России, неприятия любой дискриминации людей по социальным, национальным, расовым, религиозным признакам, проявлений экстремизма, терроризма, коррупции, антигосударственной деятельности;

- этнической, национальной принадлежности, знания и уважения истории и культуры своего народа;
- принадлежности к многонациональному народу Российской Федерации, Российскому Отечеству, российской культурной идентичности;
- сознания ценности жизни, здоровья и безопасности, значения личных усилий в сохранении и укреплении здоровья (своего и других людей), соблюдения правил личной и общественной безопасности, в том числе в информационной среде;
- ориентации на осознанный выбор сферы профессиональных интересов, профессиональной деятельности в российском обществе с учётом личных жизненных планов, потребностей семьи, общества;
- познавательных интересов в разных областях знания, представлений о современной научной картине мира, достижениях российской и мировой науки и техники;
- понимания значения науки и техники в жизни российского общества, гуманитарном и социально-экономическом развитии России, обеспечении безопасности народа России и Российского государства;
- навыков наблюдений, накопления и систематизации фактов, осмысления опыта в разных областях познания, в исследовательской деятельности;
- навыков критического мышления, определения достоверной научной информации и обоснованной критики антинаучных представлений.

Основные целевые ориентиры воспитания в Программе определяются также в соответствии с предметными направленностями разрабатываемых программ и приоритетами, заданными «Концепцией развития дополнительного образования детей до 2030 года»; они направлены на воспитание, формирование:

- интереса к технической деятельности, истории техники в России и мире, к достижениям Российской и мировой технической мысли;
- понимания значения техники в жизни Российского общества;

- интереса к личностям конструкторов, организаторов производства;
- ценностей авторства и участия в техническом творчестве;
- навыков определения достоверности и этики технических идей;
- отношения к влиянию технических процессов на природу;
- ценностей технической безопасности и контроля;
- отношения к угрозам технического прогресса, к проблемам связей технологического развития России и своего региона;
- уважения к достижениям в технике своих земляков;
- воли, упорства, дисциплинированности в реализации проектов;
- опыта участия в технических проектах и их оценки.

3.2. Формы и методы воспитания

Программа имеет практико-ориентированный характер и ориентирована на такие виды и формы воспитательной деятельности, которые способствуют формированию и развитию у обучающихся индивидуальных способностей и способов деятельности, объективных представлений о мире, окружающей действительности, внутренней мотивации к творческой деятельности, познанию, нравственному поведению.

Основной формой воспитания и обучения воспитанников по Программе является учебное занятие.

В ходе учебных занятий в соответствии с предметным и метапредметным содержанием Программы обучающиеся:

- усваивают информацию, имеющую воспитательное значение;
- получают опыт деятельности, в которой формируются, проявляются и утверждаются ценностные, нравственные ориентации;
- осознают себя способными к нравственному выбору;
- участвуют в освоении и формировании среды своего личностного развития, творческой самореализации.

Получение информации об открытиях, изобретениях, достижениях, связанных с информационными технологиями; изучение биографий деятелей Российской и мировой науки, героев и защитников Отечества и т. д. — это источник формирования у обучающихся сферы интересов, этических установок, личностных позиций и норм поведения. Важно, чтобы воспитанники не только получали эти сведения от педагога, но и сами осуществляли работу с информацией: поиск, сбор, обработку, обмен и т. д.

В ходе изучения Программы на практических занятиях у воспитанников усваиваются и применяются правила поведения и коммуникации, формируются позитивные и конструктивные отношения к событиям, в которых они участвуют.

Участвуя в различных проектах, у воспитанников формируется умение в области целеполагания, планирования и рефлексии, укрепляется внутренняя дисциплина, приобретается опыт долгосрочной системной деятельности.

В коллективных играх проявляются и развиваются личностные качества: эмоциональность, активность, нацеленность на успех, готовность к командной деятельности и взаимопомощи.

Итоговые мероприятия: конкурсы, соревнования, презентации проектов — способствуют закреплению ситуации успеха, развивают рефлексивные и коммуникативные умения, ответственность, благоприятно воздействуют на эмоциональную сферу обучающихся.

Воспитательное значение активностей обучающихся при реализации Программы наиболее наглядно проявляется в социальных проектах, благотворительных и волонтёрских акциях, в экологической, патриотической, трудовой, профориентационной деятельности.

Также в воспитательной деятельности с обучающимися по Программе используются такие методы воспитания как:

- метод формирования сознания личности – беседа, диспут, внушение, инструктаж, контроль, объяснение, пример, разъяснение, рассказ, самоконтроль, совет, убеждение и др.;

- метод организации деятельности и формирования опыта поведения – задание, общественное мнение, педагогическое требование, поручение, приучение, создание воспитывающих ситуаций, тренинг, упражнение и др.;
- метод мотивации деятельности и поведения - одобрение, поощрение социальной активности, порицание, создание ситуаций успеха, создание ситуаций для эмоционально- нравственных переживаний, соревнование и др.

3.3. Условия воспитания, анализ результатов

Воспитательный процесс осуществляется в условиях организации деятельности учебной группы в соответствии с нормами и правилами работы Центра, а также на площадках других организаций с учётом установленных правил и норм деятельности на этих площадках.

Анализ результатов воспитания проводится в процессе педагогического наблюдения за поведением обучающихся, их общением, отношениями друг с другом, в коллективе, их отношением к педагогам, к выполнению своих заданий по Программе.

Косвенная оценка результатов воспитания, достижения целевых ориентиров воспитания по Программе проводится путём опросов родителей в процессе реализации Программы (отзывы родителей, интервью с ними) и после её завершения (итоговые исследования результатов реализации программы за учебный период, учебный год).

Анализ результатов воспитания по Программе не предусматривает определение персонифицированного уровня воспитанности, развития качеств личности конкретного обучающегося, а предполагает получение общего представления о воспитательных результатах реализации Программы, продвижения в достижении определённых целевых ориентиров воспитания, влияния реализации Программы на коллектив обучающихся: что удалось достичь, а что является предметом воспитательной работы в будущем.

Результаты, полученные в ходе оценочных процедур — опросов, интервью — используются только в виде агрегированных усреднённых и анонимных данных.

3.4. Календарный план воспитательной работы на 2026-2027 учебный год

Таблица 2

№ п/п	Мероприятие	Сроки проведения	Приоритетные направления воспитательной работы	Цель мероприятия
1	**День знаний** – вводное занятие «Этичный хакер: миссия и ответственность»	Сентябрь 2026	Умственное, нравственное и гражданское воспитание	Формирование у обучающихся представления о значении знаний в области кибербезопасности, осознания личной ответственности за применение навыков
2	**Мероприятия, посвящённые «Дню отца»:** – мастер-класс по созданию интерактивной открытки-поздравления с использованием HTML/CSS и JavaScript; – цифровая фотовыставка «Мой папа и я – большие друзья» (обработка фото в графических редакторах); – викторина «Кибербезопасность в семье»	Октябрь 2026	Нравственное воспитание. Творческая деятельность	Поддержание традиций уважительного отношения к мужчине через цифровое творчество и формирование навыков безопасного общения в семье
3	**День учителя** – разработка интерактивной поздравительной презентации или веб-страницы с использованием анимации и скриптов	Октябрь 2026	Нравственное воспитание. Творческая деятельность	Формирование у обучающихся представления о значении знаний, уважения к педагогам через техническое творчество

4	**Мероприятия, посвящённые Дню народного единства:** – квест-игра «Единство в цифровом мире» (командное решение CTF-задач на тему истории России); – познавательная лекция-беседа «Кибербезопасность – общая ответственность»	Ноябрь 2026	Гражданско-патриотическое воспитание	Формирование интереса и уважения к истории страны, осознания важности коллективных действий в защите национальных интересов в цифровой среде
5	**Мероприятия, посвящённые Дню матери:** – мастер-класс «Создание интерактивной открытки-приложения на Python (Tkinter)»; – конкурс цифровых рисунков «Портрет мамы» (с использованием графических редакторов и нейросетей)	Ноябрь 2026	Нравственное воспитание. Творческая деятельность	Поддержание традиций бережного отношения к женщине через цифровое искусство и программирование
6	**«С историей не спорят, с историей живут»** – тематическое занятие, посвящённое Дню Конституции РФ. Обсуждение правовых и этических аспектов деятельности в области кибербезопасности, анализ статей об информационной безопасности	Декабрь 2026	Гражданское воспитание. Патриотическое воспитание	Формирование у обучающихся таких качеств, как долг, ответственность, честь, через призму законодательства и профессиональной этики
7	**День полного освобождения Ленинграда от фашистской блокады** – занятие «Криптография и защита связи в годы войны» (изучение исторических шифров, создание простого шифратора/дешифратора)	Январь 2027	Гражданское воспитание. Патриотическое воспитание	Формирование у обучающихся таких качеств, как долг, ответственность, честь, через связь истории и современных технологий защиты информации

8	**Мероприятия, посвящённые «Дню защитника Отечества»:** – викторина «Защита цифрового отечества» (вопросы по истории кибервойн, известным хакерским атакам и методам защиты); – соревнование по взлому учебного стенда (в изолированной среде) с последующим составлением отчёта об уязвимостях	Февраль 2027	Гражданское воспитание. Патриотическое воспитание	Формирование у обучающихся таких качеств, как долг, ответственность, честь, готовность защищать информационные рубежи страны
9	**Мероприятия, посвящённые «Международному женскому дню»:** – оформление цифровых портретов «Моя любимая мама» (графические редакторы); – создание интерактивных открыток с анимацией на языке программирования (Scratch/Python) или в среде веб-разработки	Март 2027	Нравственное и эстетическое воспитание. Творческая деятельность	Поддержание традиций бережного отношения к женщине через цифровое творчество и программирование
10	**День воссоединения Крыма с Россией** – тематический хакатон «Кибербезопасность и суверенитет: защита национальных цифровых ресурсов» (разработка проекта по защите критической информационной инфраструктуры)	Март 2027	Гражданское воспитание. Патриотическое воспитание	Формирование патриотических чувств и понимания важности защиты информационного суверенитета страны
11	**Мероприятия, посвящённые «Дню Космонавтики»:** – воркшоп «Безопасность космических систем	Апрель 2027	Гражданское воспитание. Творческая деятельность	Стимулирование интереса к исследовательской деятельности, применение

	связи» (анализ угроз для спутниковых каналов); – интеллектуальная викторина «Космос далёкий и близкий» (с элементами криптографии и радиотехники)			навыков реверс-инжиниринга в космической отрасли
12	**Мероприятия, посвящённые «Дню Победы»:** – акция памяти «Они героями останутся на век» – создание цифрового архива или веб-сайта с воспоминаниями и историческими данными о вкладе связистов и шифровальщиков в Победу;	Май 2027	Нравственное воспитание. Гражданско-патриотическое воспитание	Формирование моральных качеств: долг, ответственность, честь, любовь к Родине, к истории своей страны, через изучение вклада специалистов по защите информации в Великую Победу

4. Организационно-методические условия реализации Программы

4.1. Требования к помещению

Для обеспечения занятий необходимо:

- помещение, отвечающее санитарно-гигиеническим требованиям: просторное, с хорошим дневным освещением, хорошо налаженной вентиляцией;
- помещение должно быть оборудовано необходимой мебелью (столы, стулья, шкафы, доска, стеллажи);
- освещение может быть электрическое, лучи света должны падать на изображаемый объект под углом 45º;
- окна должны быть защищены от воздействия прямых солнечных лучей (занавес, жалюзи).

4.2. Материально-техническое и информационное обеспечение

Материально-техническое обеспечение:

- ноутбук тип 1 (13 шт.);
- веб-камера (1 шт.);
- наушники с микрофоном (13 шт.);
- мышь (13 шт.);
- многофункциональное устройство (1 шт.);
- моноблочное интерактивное устройство (1 шт.);
- мобильная напольная стойка (1 шт.);
- флипчарт (1 шт.);
- стол ученический 2-местный (с экраном между столов) (6 шт.);
- стул ученический (12 шт.);
- стол преподавателя (1 шт.);
- шкаф (2 шт.);
- стул преподавателя (1 шт.).

Информационное обеспечение:

- операционная система (желательно Windows);
- поддерживаемые браузеры (для работы LMS): Yandex Browser, Chrome, Chrome Mobile, Firefox, Opera.

СПИСОК ЛИТЕРАТУРЫ

Нормативные документы:

Нормативные документы:

1. Федеральный Закон №273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»;

2. Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»;

3. Концепция развития дополнительного образования детей до 2030 года (утверждена распоряжением Правительства РФ от 31.03.2022 № 678-р);

4. Постановление Правительства Российской Федерации от 26.12.2017 № 1642 «Об утверждении государственной программы Российской Федерации «Развитие образования» (с изменениями и дополнениями, действующими в 2026 году);

5. Стратегия развития образования в Российской Федерации до 2036 года с перспективой до 2040 года (утверждена распоряжением Правительства РФ от 18.05.2026 №1106-р);

6. Стратегия развития воспитания в Российской Федерации на период до 2030 года (утверждена распоряжением Правительства Российской Федерации от 29 мая 2015 № 996 р, с изменениями);

7. Приказ Министерства просвещения Российской Федерации от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (с изменениями, внесенными приказом Минпросвещения России от 30.01.2024 №55);

8. Письмо Министерства просвещения Российской Федерации от 19.03.2024 №05-545 «О направлении информации» (с обновленными методическими рекомендациями);

9. Постановление Главного государственного санитарного врача Российской Федерации от 02.06.2026 № 19 «Об утверждении СП 2.4.2.4283-26

Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

10. Конвенция ООН о правах ребёнка.

Учебная литература:

1. Мессье Р. Изучаем Kali Linux. Проверка защиты, тестирование на проникновение, этичный хакинг. — 2-е изд. — СПб.: Питер, 2025. — 512 с.: ил. (Серия «Библиотека программиста»).

2. Грей Дж. Социальная инженерия и этичный хакинг на практике / пер. с англ. В. С. Яценкова. — М.: ДМК Пресс, 2023. — 226 с.: ил.

3. Этичный хакинг. Практическое руководство по взлому. — СПб.: Питер, 2023. — 384 с.: ил. (Серия «Библиотека программиста»).

4. Бирюков А. А. Реверсивный инжиниринг приложений под Windows. — М.: ДМК Пресс, 2023. — 400 с.: ил.

5. Blue Fox: взлом и реверс-инжиниринг ARM. — СПб.: Питер, 2025. — 320 с.: ил.

6. Реверс-инжиниринг встраиваемых систем. — М.: ДМК Пресс, 2025. — 280 с.: ил.

7. Харрис Ш., Харпер А., Игл К., Несбитт Дж. Gray Hat Hacking: The Ethical Hacker‘s Handbook. — 6th ed. — McGraw-Hill Education, 2022. — 640 p.

8. О'Лири Д. Reverse Engineering for Beginners. — Leanpub, 2020. — 450 p.

9. Кеннеди Д., О'Горман Д., Кирнс Д., Ахмед М. Metasploit: The Penetration Tester's Guide. — No Starch Press, 2011. — 328 p.

10. Стоунс Р. Основы безопасности сетей: протоколы, уязвимости и методы атак. — М.: Вильямс, 2022. — 480 с.

11. Солдатова Г. У., Рассказова Е. И. Психология цифровой безопасности: основы компетентной и безопасной личности в интернете. — М.: Смысл, 2022. — 320 с.

12. Шнайер Б. Криптография и безопасность сетей. — М.: Вильямс, 2020. — 680 с.

13. Фролов А. В., Фролов Г. В. Ассемблер для Windows: реверс-инжиниринг и отладка. — М.: Диалог-МИФИ, 2021. — 432 с.

14. Ефимова Л. Л., Кочерга С. А. Информационная безопасность детей: российский и зарубежный опыт: Монография. — М.: ЮНИТИ-ДАНА, 2013.

15. Федоров А. В. Медиаобразование: вчера и сегодня. — М.: МОО ВПП ЮНЕСКО «Информация для всех», 2009.

Интернет-ресурсы:

1. Kali Linux — официальный сайт дистрибутива для тестирования на проникновение. Режим доступа: https://www.kali.org

2. OWASP Foundation — открытый проект по безопасности веб-приложений (OWASP Top 10, инструменты, документация). Режим доступа: https://owasp.org

3. Хакер — российский журнал и портал о кибербезопасности, этичном хакинге и реверс-инжиниринге. Режим доступа: https://xakep.ru

4. Habr — раздел «Информационная безопасность» на ведущем IT-ресурсе. Режим доступа: https://habr.com/ru/hub/infosecurity/

5. GitHub — Hacker Security Resources — коллекция инструментов, скриптов и учебных материалов по этичному хакингу (репозиторий Omar Santos). Режим доступа: https://github.com/The-Art-of-Hacking/h4cker[reference:14] [reference:15]

6. GitHub — Ethical Hacking Roadmap — структурированный план обучения этичному хакингу с подборкой инструментов и ссылок. Режим доступа: https://github.com/rodrigohenrik/Ethical-Hacking-Roadmap[reference:16]

7. GitHub — Russian Hacker Books — коллекция русскоязычных книг и материалов по кибербезопасности, этичному хакингу, программированию и реверс-инжинирингу. Режим доступа: https://github.com/fadik22/Russian-hacker-books[reference:17]

8. HackerOne — платформа для баг-баунти, где можно практиковаться в этичном взломе на реальных программах. Режим доступа: https://www.hackerone.com

9. TryHackMe — интерактивная платформа для обучения кибербезопасности с практическими заданиями. Режим доступа: https://tryhackme.com

10. Hack The Box — платформа с виртуальными машинами для отработки навыков пентеста и реверс-инжиниринга. Режим доступа: https://www.hackthebox.com

11. CTFtime — агрегатор соревнований Capture The Flag по кибербезопасности. Режим доступа: https://ctftime.org

12. CyberChef — веб-инструмент для криптографии, кодирования и анализа данных. Режим доступа: https://gchq.github.io/CyberChef/

13. VirusTotal — сервис для анализа подозрительных файлов и URL-адресов. Режим доступа: https://www.virustotal.com

14. CVE Details — база данных известных уязвимостей (Common Vulnerabilities and Exposures). Режим доступа: https://www.cvedetails.com

15. Портал «Дополнительное образование детей» — ресурс для педагогов дополнительного образования. Режим доступа: http://vidod.edu.ru[reference:18]

16. Федеральный портал «Российское образование» — общий образовательный портал. Режим доступа: http://www.edu.ru[reference:19]

17. Сайт Министерства просвещения РФ — официальный сайт ведомства. Режим доступа: https://edu.gov.ru

Приложение 1

Календарно-тематическое планирование

Группа – ЭХ1, ЭХ2

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
Введение		**2**	**1**	**1**		
1	Вводный инструктаж по ТБ. Входной контроль. Знакомство с этичным хакингом и реверс-инжинирингом.	2	1	1	01.09	
Раздел 1. Основы этичного хакинга и информационной безопасности (12 занятий)		**24**	**6**	**18**		
2	Понятие этичного хакинга. Виды хакеров. Правовые и этические аспекты.	2	0	2	03.09	
3	Основы информационной безопасности: угрозы, уязвимости, риски.	2	0	2	08.09	
4	Методологии тестирования на проникновение (OSSTMM, PTES, OWASP).	2	1	1	10.09	
5	Сбор информации из открытых источников (OSINT). Инструменты и методы.	2	1	1	15.09	
6	Практика OSINT: поиск данных о доменах, IP-адресах, сотрудниках.	2	0	2	17.09	
7	Знакомство с операционной системой Kali Linux. Установка и настройка.	2	1	1	22.09	
8	Основы работы в командной строке Linux. Навигация, управление файлами.	2	0	2	24.09	
9	Сетевые основы: модель OSI, стек TCP/IP, основные протоколы.	2	1	1	29.09	
10	Сканирование сети с помощью Nmap: определение портов,	2	1	1	01.10	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	служб, ОС.					
11	Анализ результатов сканирования. Составление отчёта.	2	0	2	06.10	
12	Введение в криптографию: симметричные и асимметричные алгоритмы.	2	0	2	08.10	
13	Практика: шифрование и дешифрование данных с использованием OpenSSL.	2	0	2	13.10	
Раздел 2. Сетевые технологии и атаки (12 занятий)		**24**	**8**	**6**		
14	Уязвимости сетевого уровня: ARP-спуфинг, MAC-флудинг.	2	1	1	15.10	
15	Проведение ARP-атаки в локальной сети (лабораторный стенд).	2	0	2	20.10	
16	Анализ сетевого трафика с Wireshark. Фильтрация и перехват.	2	1	1	22.10	
17	Основы безопасности беспроводных сетей Wi-Fi. Типы шифрования.	2	1	1	27.10	
18	Атаки на Wi-Fi: перехват рукопожатия, подбор пароля (aircrack-ng).	2	0	2	29.10	
19	Защита Wi-Fi сетей: настройка WPA2, использование VPN.	2	1	1	03.11	
20	Атаки на уровне приложений: веб-уязвимости (обзор).	2	1	1	05.11	
21	Инструменты для анализа веб-трафика: Burp Suite, OWASP ZAP.	2	0	2	10.11	
22	Практика: перехват и модификация HTTP-запросов.	2	0	2	12.11	
23	Дениал-оф-сервис (DoS) атаки: типы и защита.	2	1	1	17.11	
24	Настройка межсетевого экрана (iptables) для защиты сети.	2	1	1	19.11	
25	Обнаружение вторжений (IDS/IPS) на примере Snort.	2	1	1	24.11	
Раздел 3. Основы программирования для задач безопасности (8 занятий)		**16**	**4**	**12**		
26	Введение в Python для кибербезопасности. Синтаксис,	2	1	1	26.11	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	переменные, циклы.					
27	Функции и модули. Работа со строками и файлами.	2	0	2	01.12	
28	Сетевые библиотеки Python: socket, requests, scapy.	2	1	1	03.12	
29	Написание простого портового сканера на Python.	2	0	2	08.12	
30	Создание сниффера для перехвата HTTP-трафика.	2	0	2	10.12	
31	Автоматизация атак: брутфорс форм авторизации.	2	0	2	15.12	
32	Безопасное программирование: типичные уязвимости в коде.	2	1	1	17.12	
33	Использование статических анализаторов кода (Bandit, Pylint).	2	1	1	22.12	
Раздел 4. Реверс-инжиниринг и анализ вредоносного ПО (7 занятий)		**14**	**4**	**10**		
34	Архитектура процессора x86/x64. Регистры, стек, система команд.	2	0	2	24.12	
35	**Промежуточная аттестация** – практическое задание по анализу кода (тестирование навыков).	2	1	1	29.12	
36	Повторный инструктаж по ТБ. Статический и динамический анализ: дизассемблеры (IDA Pro, Ghidra) и отладчики (OllyDbg, x64dbg, GDB).	2	0	2	12.01	
37	Основы ассемблера и форматы исполняемых файлов (PE, ELF).	2	1	1	14.01	
38	Анализ вредоносных программ. Признаки, классификация, поведенческий анализ.	2	0	2	19.01	
39	Распаковка упакованных исполняемых файлов (UPX).	2	1	1	21.01	
40	Составление отчёта по результатам реверс-инжиниринга.	2	1	1	26.01	
Раздел 5. Инструменты пентеста и эксплуатация (16 занятий)		**32**	**8**	**24**		
41	Фреймворк Metasploit: структура, основные модули.	2	0	2	28.01	
42	Использование Metasploit для эксплуатации уязвимостей (на	2	1	1	02.02	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	примере).					
43	Написание собственного модуля для Metasploit.	2	1	1	04.02	
44	Постэксплуатация: сбор данных, повышение привилегий.	2	1	1	09.02	
45	Удалённое управление и закрепление в системе.	2	0	2	11.02	
46	Социальная инженерия: методы и защита.	2	0	2	16.02	
47	Создание фишинговой страницы (учебный пример).	2	1	1	18.02	
48	Веб-пентест с Burp Suite: перехват, повтор, изменение запросов.	2	0	2	25.02	
49	Эксплуатация SQL-инъекций на учебном стенде (DVWA).	2	0	2	02.03	
50	Эксплуатация XSS и CSRF уязвимостей.	2	1	1	04.03	
51	Настройка HTTPS и SSL/TLS. Самоподписанные сертификаты.	2	0	2	09.03	
52	Криптоанализ: взлом хешей (John the Ripper, Hashcat).	2	1	1	11.03	
53	Анализ и эксплуатация уязвимостей типа переполнение буфера.	2	0	2	16.03	
54	Использование ROP-гаджетов для обхода защиты.	2	1	1	18.03	
55	Практика по написанию эксплойтов.	2	0	2	23.03	
56	Отчёт по результатам пентеста: структура и оформление.	2	0	2	25.03	
Раздел 6. Веб-безопасность и криптография (9 занятий)		**18**	**4**	**14**		
57	Веб-технологии: HTTP, cookies, сессии, REST API.	2	1	1	30.03	
58	OWASP Top 10: обзор основных уязвимостей веб-приложений.	2	0	2	01.04	
59	SQL-инъекции: типы, методы обнаружения и защиты.	2	1	1	06.04	
60	XSS: типы, эксплуатация, защита с помощью CSP.	2	0	2	08.04	
61	CSRF: принцип атаки и методы предотвращения.	2	0	2	13.04	
62	Безопасная аутентификация: хеширование паролей, соли.	2	0	2	15.04	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
63	Основы цифровых подписей и сертификатов.	2	1	1	20.04	
64	Криптографические протоколы: TLS, SSH.	2	0	2	22.04	
65	Практика: анализ защищённости веб-приложения с использованием DVWA.	2	0	2	27.04	
Проектная деятельность (7 занятий)		**14**	**2**	**12**		
66	Выбор темы итогового проекта в области этичного хакинга или реверса.	2	0	2	29.04	
67	Планирование проекта. Поиск информации и литературы.	2	0	2	04.05	
68	Разработка инструмента или исследование уязвимости (обработка данных).	2	0	2	06.05	
69	Оформление проекта: отчёт, презентация, демонстрация.	2	1	1	11.05	
70	Работа над проектом: программирование, тестирование.	2	1	1	13.05	
71	Предзащита проектов. Рецензирование.	2	0	2	18.05	
72	Защита проектов.	2	0	2	20.05	
Итого:		**144**	**37**	**107**		

Приложение 2

Лист корректировки программы

Количество часов по программе (на начало учебного года) – 144 ч.
Количество часов по программе (на конец учебного года) -

№ занятия	Раздел	Планируемое кол-во часов	Фактическое кол-во часов	Причина корректировки	Способ корректировки	Согласованно