АНО «Развитие человеческого капитала»
Обособленное подразделение «Техноград»

УТВЕРЖДЕНО
Приказом Генерального директора
АНО «Развитие человеческого капитала»
№ ОД-339/25 от «7» октября 2025 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

Наименование программы

«Компьютерные сети и информационная безопасность»

Категория слушателей: начинающие инженеры по информационной безопасности, техники по защите информации, аналитики, DevOps-инженеры, архитекторы ИТ-инфраструктур, инженеры по сетям, пентестеры (этичные хакеры), специалисты по кибербезопасности, специалисты баз данных (DBA), криптографы, кураторы информационной безопасности, консультанты по безопасности личного профиля, системные инженеры, разработчики облачных систем, вирусные аналитики, инженеры по криптозащите, специалисты по информационной борьбе, IT-специалисты, директора по информационным технологиям, специалисты по сетевой безопасности, аналитики в области информационной безопасности, техники по компьютерным сетям, системные администраторы, лица старше 18 лет, заинтересованные в получении новых компетенций, студенты высших учебных заведений и учреждений СПО, обучающиеся по специальностям «Сетевое и системное администрирование», «Информационные системы и технологии», «Информационная безопасность»

Объем: 24 часа

Форма обучения: очная с применением дистанционных технологий

Форма документа, выдаваемого по результатам освоения программы: сертификат о прохождении курса

УЧЕБНЫЙ ПЛАН

Наименование компонентов программы	Обязательные аудиторные учебные занятия (ч.)		Внеаудиторная (самостоятельная) учебная работа (ч.)	Всего учебной нагрузки (ч.)
	всего	в т.ч. практических и семинарских занятий		
Тема 1. Сетевые основы (модель OSI).	**4**	3	-	**4**
Тема 2. IP, подсети, базовая аутентификация.	**4**	3	-	**4**
Тема 3. Протоколы TCP/UDP, DNS, HTTP, HTTPS, подготовка виртуальной машины.	**4**	3	-	**4**
Тема 4. Угрозы, фишинг, AI-практики.	**4**	3	-	**4**
Тема 5. Криптография, TLS, VLAN.	**4**	3	-	**4**
Тема 6. SSH, VPN, мониторинг.	**4**	3	-	**4**
ИТОГО:	**24**	**18**	**0**	**24**

Календарный учебный график

Период обучения (недели/дни)	Наименование модуля
1 день	**Тема 1.** Сетевые основы (модель OSI).
2 день	**Тема 2.** IP, подсети, базовая аутентификация.
3 день	**Тема 3.** Протоколы TCP/UDP, DNS, HTTP, HTTPS, подготовка виртуальной машины.
4 день	**Тема 4.** Угрозы, фишинг, AI-практики.
5 день	**Тема 5.** Криптография, TLS, VLAN.
6 день	**Тема 6.** SSH, VPN, мониторинг.

СОДЕРЖАНИЕ ПРОГРАММЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ, РАЗДЕЛАМ (МОДУЛЯМ)

Наименование тем, разделов (разделов)	Содержание тем, разделов (модулей)
Тема 1. Сетевые основы (модель OSI).	Технологии передачи данных между открытыми системами, выполнение набора задач в режиме реального времени с помощью обмена данных в автоматическом режиме, объемы трафика, типы узлов в сети (промежуточные и конечные устройства), передача данных (беспроводные, электрические, оптические сигналы), сетевая топология (физическая, логическая), point-to-point, ring, bus, star, полносвязная, ячеистая, иерархическая звезда, смешанная, сетевые устройства (концентратор, домен коллизий, коммутатор, MAC-адрес, маршрутизатор, ARP-таблица), модель OSI (7 уровней: physical, data link, network, transport, session, presentation, application), инкапсуляция, декапсуляция, практика работы в Cisco Packet Tracer, инициация ping, PDU, IP-пакеты, кадры (фреймы), передача битового потока. Анализ трафика через Wireshark (данные, адрес пользователя, порты, сервер), проверка на наличие петли. **Практическое задание № 1. Настроить параметры протокола для отправки данных на определенный ПК с получением обратной связи.**
Тема 2. IP, подсети, базовая аутентификация.	Интернет-протокол сетевого уровня модели OSI, IPv4 (32-битные адреса), IPv6 (128-битные адреса), типы адресации (статические, динамические), протокол DHCP, структура адреса (числа в двоичном и десятичном видах, октет, сетевая и хвостовая части), IP-калькулятор, сетевой адрес, хост, широковещательный адрес, маска подсети, таблица истинности, длина префикса, логическая операция and, CLI роутера, список команд для работы с интерфейсом. Пароли, методы подбора (по «словарям», посимвольный, хэширование, bcrypt), менеджеры паролей, файл-ключ, таймер блокировки, alt-символы, двухфакторная аутентификация, команды для маршрутизатора, человеческий фактор, фишинг. **Практическое задание № 2. Подключить несколько вариантов сетей с добавлением адресов, генерацией протоколов, обработкой запросов.**

Тема 3. Протоколы TCP/UDP, DNS, HTTP, HTTPS, подготовка виртуальной машины.	Протокол TCP (разделение данных на потоки, управление соединениями), подтверждение передачи данных на ПК (кумулятивное, выборочное), UDP (высокая скорость отправления файлов), широковещательная передача (broadcast), транспортный порт, доменный сервер, сетевые службы, протокол http, обмен информацией между браузером и сервером, виды запросов (get, post, put, delete), https (шифрование данных), протоколы SSL/TLS, почтовые протоколы SMTP, POP3, IMAP, SFTP, SSH. Подготовка виртуальной машины, образы Ubuntu, Linux Kali, настройка интерфейсов, конфигурирование через SSH, виды операций в системе, права, группы пользователя. **Практическое задание № 3. Создать локальную сеть с возможностью внесения изменений в использование протоколов, адресов серверов.**
Тема 4. Угрозы, фишинг, AI-практики.	DOS и DDOS-атаки, нарушение (снижение) доступности веб-ресурса, ложные запросы, блокировка источника угрозы, ботнет, поток трафика с нескольких устройств, обнаружение зараженной сети, классификация атак по протоколам (ICMP, GRE, IPIP, ESP, AH, SCTP), IP Null-атака, SYN и UDP-флуд, ping of death, атака медленными сессиями, SQL-инъекции, изменение запроса, XSS-атака через JavaScript, выполнение произвольного кода на чужом сервере, вирусы (ПО: Brain, черви, трояны, ILOVEYOU, методы социальной инженерии, шифровальщик WannaCry, Trojan Emotet, фишинг: смишинг, вишинг), рекомендации по профилактике кибератак. LLM, бесплатные нейросервисы, AI-triage, первичная обработка и сортировка инцидентов информационной безопасности с помощью ИИ, оценка риска, фильтрация веб-трафика в Wireshark, экспорт артефактов, follow stream, запуск сессии, проверка устройств, поиск проблем и аномалий в сети. **Практическое задание № 4. Проверить через протокол SSH наличие возможных потенциальных уязвимостей на виртуальной модели ОС.**
Тема 5. Криптография, TLS, VLAN.	Шифрование симметричное и ассиметричное, преобразование данных в код, использование ключей для шифрования и расшифровки информации, AES, DES, Blowfish, преимущества и недостатки, публичный и приватный ключи, RSA, ECC, JWT (токен для безопасного обмена данных с подтверждением цифровой подписью), полезная нагрузка, веб-токен для доступа к защищенным ресурсам, аутентификация, авторизация, взаимодействие между микросервисами, access, refresh. SSL/TLS-протоколы, безопасная связь между браузером и

	сайтом, цифровые сертификаты, «рукопожатие» (параметры соединения и шифрования), алгоритм Диффи-Хеллмана (договор о секретном ключе без передачи), TLS 1.2 и 1.3. VLAN и сегментация сети, управление сетевым трафиком, логическая локальная сеть, тегирование и разделение трафика, маршрутизация, правила доступа, ограниченные домены, снижение перегрузки и широковещательного «шторма», L3-коммутаторы, политика QoS, команды для отделов, загрузка комплекса правил настройки сети. **Практическое задание № 5. Построить локальную сеть в формате VLAN с передачей данных по отдельным сегментированным каналам.**
Тема 6. SSH, VPN, мониторинг.	SSH, ключевая аутентификация (двухфакторная, мультифакторная), целостность данных, подключение к удаленным системам, администрирование серверов, защищенный доступ к облачным сервисам, копирование файлов. VPN, доступ к корпоративным ресурсам, канал для передачи данных с защитой от хакерских атак и прослушивания в доступном месте, обход ограничений (интернет-цензуры), wireguard (Anmezia), ТСПУ, proxy server, команды SSH для работы на виртуальной машине, утилита socket statistic, process tree, SSHD, scp, numeric, btop, Grafana, Prometheus. **Практическое задание № 6. Осуществить передачу публичного ключа с Linux Kali на Ubuntu через настройку протокола SSH.**