Приложение 3

Евразийская академия

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ЕВРАЗИЙСКАЯ АКАДЕМИЯ"

УТВЕРЖДАЮ
Ректор
_____ /Замлелый А.Ю./

"05" июня 2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Защита от DDoS-атак и других сетевых угроз»

Дополнительная профессиональная программа
«Информационные и коммуникационные технологии»

г. Москва
Территория Инновационного центра Сколково

Наименование учебной дисциплины: Защита от DDoS-атак и других сетевых угроз.

Цель освоения учебной дисциплины: достижение запланированных результатов освоения образовательной программы - формирование установленных в образовательной программе компетенций.

Задачи освоения учебной дисциплины: достижение запланированных в настоящей рабочей программе результатов освоения дисциплин - приобретение обучающимся запланированных знаний, умений, навыков.

Планируемые результаты освоения учебной дисциплины
Обучающийся должен сформировать следующие результаты освоения дисциплины «Защита от DDoS-атак и других сетевых угроз»:

Знания: Знания о современных сетевых угрозах, помимо DDoS-атак, таких как взлом, фишинг, malware, botnet-сети; методов и технологий обнаружения и предотвращения вторжений (IDS/IPS); принципов работы межсетевых экранов и систем обнаружения аномалий; методов анализа уязвимостей и управления рисками информационной безопасности.

Умения: Навыки работы с инструментами анализа сетевой безопасности, такими как сканеры уязвимостей, анализаторы трафика; конфигурирования межсетевых экранов и систем предотвращения вторжений; анализа логов безопасности для выявления и расследования инцидентов; реагирования на инциденты информационной безопасности и восстановления работоспособности систем.

Навыки: Умение проводить аудит безопасности сети на предмет уязвимостей к различным сетевым угрозам; конфигурировать и администрировать системы защиты от сетевых угроз, такие как firewall, IDS/IPS, антивирусное ПО; разрабатывать и внедрять политики безопасности для защиты от сетевых угроз; анализировать инциденты информационной безопасности и разрабатывать меры по их устранению и предотвращению.

Объем (трудоемкость) учебной дисциплины: определен в учебном плане образовательной программы.

Форма промежуточной аттестации по учебной дисциплине определена в учебном плане образовательной программы.

Текущий контроль успеваемости осуществляется посредством аналитического отчета обучающегося по дисциплине.

Структура и содержание учебной дисциплины определяется тематическим планом учебной дисциплины.

Тематический план учебной дисциплины

Тема N° 1: Введение в DDoS-атаки
Тема N° 2: Классификация DDoS-атак
Тема N° 3: Объемные атаки (UDP Flood, ICMP Flood, SYN Flood)
Тема N° 4: Протокольные атаки (Slowloris, SYNACK Flood)

Тема N° 5: Атаки на прикладном уровне (HTTP Flood, DNS Flood)
Тема N° 6: Инструменты для проведения DDoS-атак
Тема N° 7: Ботнеты и их роль в DDoS
Тема N° 8: Влияние DDoS-атак на бизнес
Тема N° 9: Методы обнаружения DDoS-атак
Тема N° 10: Анализ трафика и выявление аномалий
Тема N° 11: Поведенческий анализ пользователей
Тема N° 12: Системы обнаружения вторжений (IDS)
Тема N° 13: Системы предотвращения вторжений (IPS)
Тема N° 14: Механизмы защиты от объемных атак
Тема N° 15: Фильтрация трафика по IP-адресам
Тема N° 16: Ограничение скорости соединения
Тема N° 17: Использование черных и белых списков
Тема N° 18: Механизмы защиты от протокольных атак
Тема N° 19: SYN Cookies и SYN Proxy
Тема N° 20: Ограничение количества открытых соединений
Тема N° 21: Механизмы защиты от атак на прикладном уровне
Тема N° 22: Веб-приложения Firewall (WAF)
Тема N° 23: Кэширование контента
Тема N° 24: CAPTCHA и другие методы проверки пользователей
Тема N° 25: Облачные решения для защиты от DDoS
Тема N° 26: CDN (Content Delivery Network)
Тема N° 27: DDoS Mitigation Services
Тема N° 28: Аппаратные решения для защиты от DDoS
Тема N° 29: Преимущества и недостатки различных решений
Тема N° 30: Выбор оптимальной стратегии защиты
Тема N° 31: Планирование защиты от DDoS
Тема N° 32: Реагирование на DDoS-атаку
Тема N° 33: Анализ после атаки
Тема N° 34: Внедрение и настройка систем защиты
Тема N° 35: Мониторинг и анализ эффективности защиты
Тема N° 36: Другие сетевые угрозы: Введение
Тема N° 37: Вредоносное ПО (Malware)
Тема N° 38: Фишинг (Phishing)
Тема N° 39: Man-in-the-middle атаки
Тема N° 40: SQL-инъекции
Тема N° 41: Кросс-сайтовый скриптинг (XSS)
Тема N° 42: Уязвимости операционных систем
Тема N° 43: Уязвимости веб-приложений
Тема N° 44: Методы защиты от сетевых угроз
Тема N° 45: Firewall и VPN
Тема N° 46: Антивирусное ПО
Тема N° 47: Системы управления информационной безопасностью (SIEM)
Тема N° 48: Практические занятия по анализу трафика

Тема N° 49: Практические занятия по настройке систем защиты
Тема N° 50: Индивидуальные проекты по защите от сетевых угроз
Тема N° 51: Этические хакерство и пентестинг
Тема N° 52: Законодательство в области кибербезопасности
Тема N° 53: Будущее защиты от DDoS и сетевых угроз

Содержание самостоятельной работы обучающихся по учебной дисциплине: подготовка к занятиям: изучение теоретического материала, чтение учебников и дополнительных источников, конспектирование; подготовка к промежуточной аттестации; самостоятельное изучение дополнительных материалов; анализ и интерпретация данных – составление аналитического отчета обучающегося по дисциплине.

Условия реализации рабочей программы дисциплины

Материально-техническое обеспечение реализации дисциплины соответствует материально-техническому обеспечению, указанному в разделе 3 образовательной программы.

Учебно-методическое обеспечение (электронные учебно-методические материалы) освоения учебной дисциплины

Электронные учебные издания
Куклина, Е. Н. Организация самостоятельной работы студента / Е. Н. Куклина, М. А. Мазниченко, И. А. Мушкина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 235 с. — (Высшее образование). — ISBN 978-5-534-06270-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562503
Зорина, Е. М. Метапредметная компетенция преподавателей и обучающихся / Е. М. Зорина. — Москва : Издательство Юрайт, 2025. — 130 с. — (Высшее образование). — ISBN 978-5-534-17997-2. — Текст : электронный // Образовательная платформа Юрайт [сайт].

Электронные методические издания
Мотивация студентов к обучению и воспитательная деятельность — Москва : Издательство Юрайт, 2023. — 1 с. — (Юрайт.Академия). — ISBN 978-5-534-14536-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/533252
Мотивация студентов к обучению и профессиональному развитию — Москва : Издательство Юрайт, 2022. — 5 с. — (Юрайт.Академия). — ISBN 978-5-534-14536-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/509597

Информационное обеспечение освоения учебной дисциплины представляет собой перечень информационных технологий, используемых при осуществлении образовательного процесса, включая перечень программного обеспечения и информационных справочных систем.

Каждый обучающийся обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной системе (цифровой (электронной) библиотеке) «ЮРАЙТ» (https://urait.ru/), содержащей издания учебно-методической и иной литературы.

Каждый обучающийся обеспечивается индивидуальным неограниченным доступом к федеральной государственной информационной системе «Национальная электронная библиотека» (https://rusneb.ru/).

Состав необходимого комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства: Яндекс Браузер (реестровая запись №3722 от 23.07.2017 в едином реестре российских программ для электронных вычислительных машин и баз данных); Яндекс.Телемост (реестровая запись №13556 от 20.05.2022 в едином реестре российских программ для электронных вычислительных машин и баз данных)

Электронные информационные ресурсы (ресурсы информационно-телекоммуникационной сети «Интернет»):

- Состав современных профессиональных баз данных
Федеральная служба государственной статистики (https://rosstat.gov.ru/)
Открытые данные России (https://data.gov.ru/)
Статистический Отдел Организации Объединенных Наций (United Nations Statistics Division) (http://data.un.org/)
База данных ЮНЕСКО (https://www.unesco.org/en/key-data)

- Состав информационных справочных систем
База знаний Открытого правительства (http://wiki.ac-forum.ru/)
Высшая аттестационная комиссия при Министерстве науки и высшего образования Российской Федерации (https://vak.minobrnauki.gov.ru/main)
Российский фонд фундаментальных исследований (https://www.rfbr.ru/)
Официальный интернет-портал правовой информации (Государственная система правовой информации) (http://pravo.gov.ru/)
Система обеспечения законодательной деятельности (https://sozd.duma.gov.ru/)
Собрание законодательства Российской Федерации (https://www.szrf.ru/)
Государственная автоматизированная система Российской Федерации «Правосудие» (ГАС «Правосудие») (https://sudrf.ru/)
Нормативные правовые акты в Российской Федерации. Министерство юстиции Российской Федерации (http://pravo.minjust.ru/)

- Иные информационные ресурсы - информационные ресурсы органов государственной власти
Президент России (http://kremlin.ru/)
Правительство России (http://government.ru/)
Министерство науки и высшего образования РФ (https://www.minobrnauki.gov.ru/)
Министерство просвещения РФ (https://edu.gov.ru/)
Министерство экономического развития Российской Федерации (https://www.economy.gov.ru/)
Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (https://digital.gov.ru/)

- Иные информационные ресурсы - периодическими издания

ТАСС (https://tass.ru/)
РИА НОВОСТИ (https://ria.ru/)
Коммерсантъ (https://www.kommersant.ru/)
RT (https://rt.com/)

- Информационные поисковые системы
Яндекс (https://ya.ru/)
MAIL.RU (https://www.mail.ru/)