



АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ЕВРАЗИЙСКАЯ АКАДЕМИЯ"

УТВЕРЖДАЮ
Ректор
_____ /Замельный А.Ю./

"05" июня 2025 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Антивирусная защита и меры против вредоносного ПО»**

Дополнительная профессиональная программа
«Информационные и коммуникационные технологии»

г. Москва
Территория Инновационного центра Сколково

Наименование учебной дисциплины: Антивирусная защита и меры против вредоносного ПО.

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 «Антивирусная защита и меры против вредоносного ПО»:

Знания: Знания основ классификации вредоносного ПО (вирусы, черви, трояны, руткиты, шпионское ПО, программы-вымогатели и т.д.), принципов их работы, методов распространения и потенциального ущерба. Знания о современных антивирусных решениях, их архитектуре и функциональных возможностях (сигнатурный анализ, эвристический анализ, песочницы, поведенческий анализ). Знания о методах и средствах защиты информации от вредоносного ПО, включая организационные, технические и программно-аппаратные меры. Знания о современных угрозах информационной безопасности и актуальных методах противодействия им. Знания об основах безопасной работы в сети Интернет и принципах информационной гигиены.

Умения: Навыки настройки и администрирования антивирусных программ и систем защиты от вредоносного ПО. Навыки обнаружения, анализа и удаления вредоносного ПО. Навыки использования специализированных инструментов для анализа вредоносного ПО (песочницы, отладчики, дизассемблеры). Навыки безопасной работы в сети Интернет и использования электронной почты. Навыки создания резервных копий данных и восстановления системы после заражения.

Навыки: Умение анализировать потенциальные угрозы информационной безопасности, связанные с вредоносным ПО. Умение выбирать и применять соответствующие антивирусные решения и средства защиты информации. Умение проводить анализ вредоносного ПО с использованием специализированных инструментов. Умение разрабатывать и внедрять политики безопасности для защиты от вредоносного ПО. Умение реагировать на инциденты безопасности, связанные с заражением вредоносным ПО.

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 № 1: Введение в антивирусную защиту

Тема № 2: Классификация вредоносного ПО

Тема № 3: Вирусы: механизмы работы и распространения

Тема № 4: Черви: особенности и методы борьбы

Тема № 5: Троянские программы: виды и опасности

Тема № 6: Руткиты: скрытие и обнаружение

Тема № 7: Шпионское ПО: кража информации и конфиденциальности

Тема № 8: Рекламное ПО: нежелательная реклама и методы защиты

Тема № 9: Вымогатели: шифрование данных и способы противодействия

Тема № 10: Бэкдоры: удаленный доступ и контроль

Тема № 11: Ботнеты: зомби-сети и их использование

Тема № 12: Вредоносные скрипты и макросы

Тема № 13: Уязвимости программного обеспечения

Тема № 14: Социальная инженерия и фишинг

Тема № 15: Методы анализа вредоносного ПО

Тема № 16: Статический анализ: сигнатурный и эвристический

Тема № 17: Динамический анализ: песочницы и виртуальные машины

Тема № 18: Антивирусные программы: принципы работы и сравнение

Тема № 19: Фаерволы: защита сети от вторжений

Тема № 20: Системы обнаружения и предотвращения вторжений (IDS/IPS)

Тема № 21: Защита от спама и фишинга

Тема № 22: Безопасность веб-браузера и расширения

Тема № 23: Безопасность электронной почты

Тема № 24: Защита мобильных устройств от вредоносного ПО

Тема № 25: Политики безопасности и лучшие практики

Тема № 26: Резервное копирование данных и восстановление системы

Тема № 27: Управление паролями и двухфакторная аутентификация

Тема № 28: Шифрование данных: защита информации от несанкционированного доступа

Тема № 29: Анализ журналов безопасности

Тема № 30: Инциденты безопасности: реагирование и расследование

Тема № 31: Криминалистический анализ вредоносного ПО

Тема № 32: Правовые аспекты информационной безопасности

Тема № 33: Этические хакеры и пентестинг

Тема № 34: Современные тенденции в развитии вредоносного ПО

Тема № 35: Методы защиты от новых угроз

Тема № 36: Облачная безопасность и виртуализация

Тема № 37: Интернет вещей и безопасность устройств IoT

Тема № 38: Защита критической инфраструктуры

Тема № 39: Будущее антивирусной защиты

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/>)