МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ ЭЛЕКТРОННО-ИНФОРМАЦИОННЫХ СИСТЕМ

Кафедра интеллектуальных информационных технологий

# РЕФЕРАТ

по дисциплине

«Современные методы защиты компьютерных систем»

**Выполнил:** студент 4-го курса, ФЭИС,

группы ИИ-22

Нестерчук Д. Н.

Брест 2024

# ТЕМА 1

PowerShell и Bash — это две популярные командные оболочки, используемые для автоматизации задач и администрирования систем. PowerShell в первую очередь ориентирован на пользователей Windows, хотя доступен и на Linux и macOS в виде PowerShell Core. Он отличается тем, что работает с объектами .NET, что позволяет обрабатывать данные не как текст, а как полноценные объекты с методами и свойствами. В PowerShell используется концепция командлетов — небольших команд, выполняющих конкретные задачи (например, Get-Process для получения списка процессов), а также мощные пайплайны, передающие объекты между командами.

Bash, в свою очередь, является основной оболочкой в Unix-подобных системах (Linux, macOS, BSD). В отличие от PowerShell, Bash работает с текстовыми строками, и его основная сила заключается в текстовой обработке с помощью утилит, таких как awk, sed, и регулярных выражений. Bash активно использует пайплайны, но они передают не объекты, а текстовые данные, что делает его идеальным для задач, связанных с фильтрацией и обработкой строковых данных.

PowerShell более мощный для работы с Windows-системами и позволяет взаимодействовать с различными объектами операционной системы через cmdlets. Он также поддерживает удаленное управление, что делает его подходящим для администрирования больших инфраструктур. Bash, с другой стороны, является стандартом для администрирования в Linux и других Unix-подобных системах, его простота и текстовая обработка делают его незаменимым инструментом для системных администраторов в этих средах.

Основные различия между ними: PowerShell использует объекты и командлеты, работает хорошо с Windows, в то время как Bash ориентирован на текстовую обработку и идеально подходит для Unix-систем.

# ТЕМА 2

**Cyber Kill Chain** — это модель, описывающая этапы кибератаки от её начала до достижения цели, разработанная компанией Lockheed Martin. Она помогает понять процесс атаки и эффективно противодействовать угрозам.

1. **Reconnaissance (Разведка)** — на этом этапе злоумышленники собирают информацию о цели, используя открытые источники, сканирование уязвимостей и социальную инженерию.
2. **Weaponization (Подготовка оружия)** — создание или подготовка вредоносного ПО для эксплуатации уязвимостей системы жертвы.
3. **Delivery (Доставка)** — передача вредоносного кода на систему цели, например, через фишинг или уязвимости в приложениях.
4. **Exploitation (Эксплуатация)** — использование уязвимости для выполнения кода на машине жертвы и получения доступа.
5. **Installation (Установка)** — установка вредоносного ПО, такого как руткиты или бэкдоры, для обеспечения постоянного контроля.
6. **Command and Control (Командование и контроль)** — установление связи между атакующим и зараженной системой для управления ею.
7. **Actions on Objectives (Действия с целями)** — финальные действия атакующих, такие как кража данных, уничтожение информации или блокировка доступа.

Cyber Kill Chain помогает определить и остановить атаку на каждом её этапе, улучшая защиту системы.

# ТЕМА 3

**MITRE ATT&CK** — это база знаний, которая описывает поведение злоумышленников на разных этапах кибератаки, включая методы и тактики, которые они используют для достижения своих целей. Модель разделена на несколько категорий: тактики (цели, которые атакующие пытаются достичь, например, сбор разведывательной информации или получение привилегий), и техники (конкретные методы или инструменты, которые используются для достижения этих целей, например, фишинг или использование уязвимостей). ATT&CK помогает организациям анализировать угрозы, выявлять уязвимости в системе и улучшать защиту, предоставляя подробные описания действий злоумышленников, которые могут быть использованы для построения эффективных стратегий защиты и мониторинга.

# ТЕМА 4

**STEM** — это аббревиатура, которая обозначает области науки, технологий, инженерии и математики (Science, Technology, Engineering, Mathematics). Эти дисциплины охватывают широкий спектр знаний и навыков, которые играют ключевую роль в развитии инноваций и решении современных глобальных проблем. STEM-образование направлено на подготовку специалистов, которые могут использовать эти знания для разработки новых технологий, научных исследований, создания инженерных решений и применения математических методов для анализа данных и решения сложных задач. STEM играет важную роль в экономическом росте, научных открытиях и технологическом прогрессе в различных областях, включая информационные технологии, медицину, энергетику и экологию.