**Фанг Дук Ан Туан,** курсант,
Краснодарское высшее военное училище

**Сидельников Олег Васильевич,** преподаватель,
Краснодарское высшее военное училище

# МОДЕЛИРОВАНИЕ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ МАТРИЦЫ MITRE ATT&CK

**Аннотация.** В данной статье рассматривается применение базы знаний MITRE ATT&CK для построения моделей нарушителей информационной безопасности на объектах информационной инфраструктуры (ИИ). В отличие от традиционных подходов, ориентированных исключительно на статические индикаторы компрометации (IoC), в данном исследовании предлагается методика, позволяющая осуществить переход от пассивной модели защиты к проактивной, основанной на анализе поведения злоумышленника (TTPs – тактик, техник и процедур).

**Ключевые слова:** Модель нарушителя, MITRE ATT&CK, информационная инфраструктура (ИИ), статические индикаторы компрометации (IoC), кибербезопасность, оценка рисков, тактик, техник и процедур (TTPs).

ATT&CK (Adversary Technique, Tactic & Common Knowledge) – это глобально доступная база знаний о тактике и методах противника, основанная на реальных наблюдениях. База знаний ATT&CK используется в качестве основы для разработки конкретных моделей и методологий угроз в частном секторе, в государственных структурах и в сообществе продуктов и услуг по кибербезопасности. Проект ATT&CK открыт и доступен для бесплатного использования любым лицом или организацией.

Основная структура модели нарушителя включает следующие элементы:

**Тактики (Tactics):** тактические цели злоумышленника, причины совершения действий (например: первоначальный доступ, закрепление в системе, повышение привилегий, сбор информации и т. д.).

**Техники (Techniques):** конкретные способы достижения цели в рамках соответствующей тактики (например, для тактики «Получение учетных данных» применяются техники: Brute Force, Network Sniffing, OS Credential Dumping и т. д.).

**Группы (Groups):** изучение и прогнозирование деятельности известных хакерских группировок и их целей (например: APT29, Cobalt Group и т. д.).

**Меры защиты (Mitigations):** механизмы и средства защиты, направленные на предотвращение реализации конкретных техник».


Рисунок 1

Выше представлена обобщенная схема выбора тактик (верхний горизонтальный ряд) и соответствующих техник (вертикальные столбцы). Для обеспечения практической применимости предлагается пятиэтапный процесс построения модели нарушителя, который позволит специалистам по информационной безопасности: четко определить потенциального противника (какие группы обычно атакуют данную сферу?); понять его намерения и инструментарий (какие техники используются для проникновения?); и визуализировать маршрут атаки (построение карты путей атаки – Attack Path).

**Этап 1: Идентификация и группировка активов** Вместо простого перечисления, активы группируются в соответствии с их функциональным назначением:

- **Данные:** управляющая информация, телеметрия, персональные данные.
- **Инфраструктура:** SCADA-серверы, инженерные рабочие станции, программируемые логические контроллеры (ПЛК).
- **Связь:** сетевые протоколы (Modbus, IEC 104), VPN-шлюзы.

**Этап 2: Выбор соответствующих тактик и техник MITRE** На основе типов активов определяются техники, которые с наибольшей вероятностью могут быть использованы нарушителем. С использованием библиотеки тестов **Atomic Red Team** на платформе (framework) **CALDERA** (автоматизированная система эмуляции действий нарушителя) данный процесс может быть реализован в виде следующего цикла:

1. Выбор техники ATT&CK.
2. Выбор теста для данной техники.
3. Выполнение процедуры теста.
4. Анализ детектирования (обнаружения).
5. Внесение изменений в защитные механизмы.

**Этап 3: Построение «Дерева атак» для визуализации маршрута передвижения нарушителя** Базовая структура дерева атак включает:

- **Корень (Root):** конечная цель нарушителя (например: нарушение процесса электроснабжения).
- **Ветви (Branches):** тактики (Tactics), используемые для достижения этой цели.
- **Листья (Leaves):** конкретные техники (Techniques) с указанием идентификаторов (ID) из базы MITRE ATT&CK.

*Пример*:

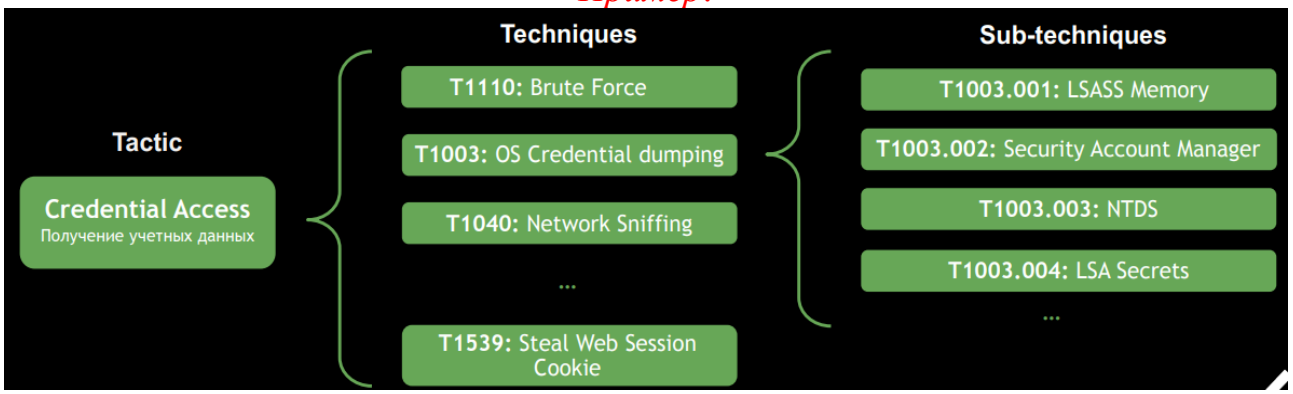


Рисунок 2

**Этап 4: Анализ пробелов в контроле (Gap Analysis)** На данном этапе проводится сопоставление существующих мер защиты с выявленными техниками атак. Оценка состояния

защиты осуществляется по четырем уровням: **None** (отсутствует), **Low** (низкий), **Medium** (средний), **Enough** (достаточный).

*Пример:* Многофакторная аутентификация (MFA) позволяет заблокировать технику T1110 (Brute Force), но может быть обойдена с помощью техники T1621 (MFA Request Generation).

**Этап 5: Формирование профиля нарушителя и плана реагирования** Итоговые данные объединяются в детальный профиль, который включает в себя: приоритетные техники, уровни угроз (Critical/High/Medium/Low) и перечень технологических решений, необходимых для устранения выявленных пробелов в безопасности.

Таким образом, моделирование нарушителя на основе MITRE ATT&CK позволяет сократить разрыв между теоретическими регламентами и практической деятельностью по обеспечению информационной безопасности объектов инфраструктуры. Вместо использования «статичных» документов, применение предложенного пятиэтапного процесса не только способствует раннему обнаружению атак, но и оптимизирует работу систем защиты.

*Список литературы:*

1. Xiong, W. et al., “Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix,” *Software and Systems Modeling*, vol. 21, pp. 157–177, 2022. URL: https://doi.org/10.1007/s10270-021-00898-7.

2. Center for Threat-Informed Defense, “Question 2: What could go wrong? (Threat Modeling with ATT&CK),” 2024. URL: https://center-for-threat-informed-defense.github.io/threat-modeling-with-attack/question-2/.

3. MITRE ATT&CK, “Technique T1584.008: Compromise Infrastructure: Network Devices,” 2025. URL: https://attack.mitre.org/techniques/T1584/008/.

4. Чаган, Н. Ф. “База знаний MITRE ATT&CK для построения модели нарушителя информационной безопасности,” *Тезисы докладов XXI Белорусско-российской НТК*, БГУИР, Минск, 2023, с. 95.

5. The MITRE Corporation, “MITRE ATT&CK for Industrial Control Systems,” 2021. URL: https://collaborate.mitre.org/attackics/.