**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

**ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ**

На тему:

«Изучение практических основ информационной безопасности»

**Выполнил**: ст. гр. 241-351 Куманяев Н. Р.

**Руководитель**: Кесель С. А., к.т.н., доцент кафедры «Информационная безопасность»

**Место проведения**: Московский Политех, лаборатория «Программно-аппаратных средств обеспечения информационной безопасности»

**Москва – 2025**

ОГЛАВЛЕНИЕ

[ИЗУЧЕНИЕ MITRE ATT&CK 3](#_Toc194509725)

[ИЗУЧЕНИЕ OWASP 5](#_Toc194509726)

# 

# ИЗУЧЕНИЕ MITRE ATT&CK

MITRE – это некоммерческая организация из США, занимающаяся исследованиями в области регулирования и навигации воздушного пространства, систем глобального позиционирования (GPS), аэрокосмической отрасли, кибербезопасности и других направлений.

В дополнение к матрице MITRE ATT&CK, рассматриваемой в данной работе, у этой компании есть и другие открытые проекты в области кибербезопасности, такие как каталоги CVE (Common Vulnerabilities and Exposures, общедоступный стандартизированный список уязвимостей) и CWE (Common Weakness Enumeration, перечень дефектов безопасности программного обеспечения).

Аббревиатура «ATT&CK» расшифровывается как «Adversarial Tactics, Techniques and Common Knowledge». Эта матрица представляет собой общедоступную базу знаний, основанную на анализе реальных атак, структурированную по этапам. В ней содержится перечень тактик (заголовки столбцов), а также техник и подтехник (содержимое столбцов) для каждой тактики.

Матрица MITRE ATT&CK необходима для описания «паттернов поведения злоумышленников» и служит основой для разработки конкретных моделей угроз и методологий в области кибербезопасности. Существуют три версии матрицы MITRE ATT&CK: для корпоративных сетей и традиционных клиент-серверных приложений (Enterprise ATT&CK), для мобильных приложений (Mobile ATT&CK) и для промышленных систем управления (ICS ATT&CK).

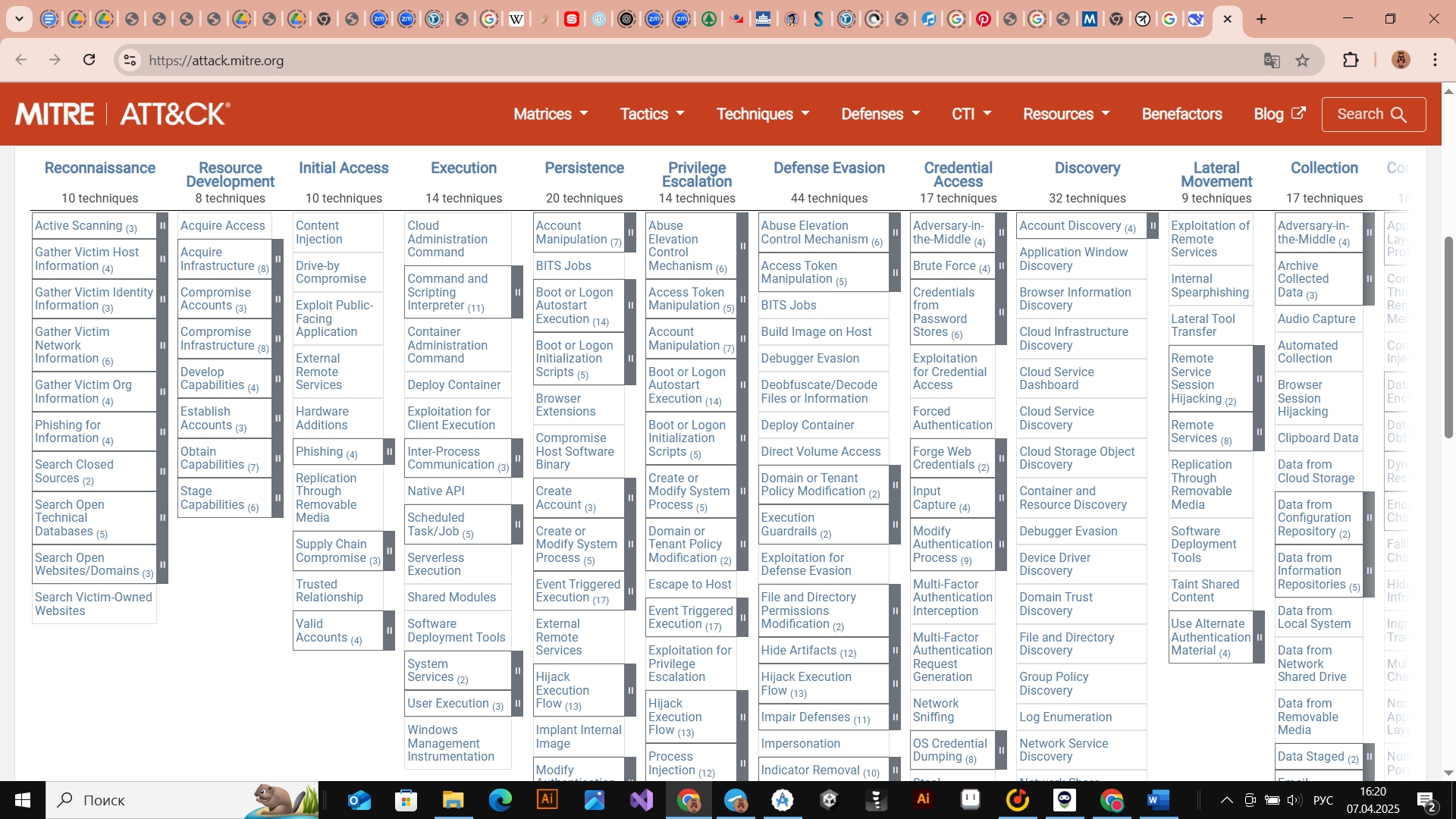


Рис. 1, неполная матрица MITRE ATT&CK

Также, на сайте MITRE ATT&CK, кроме матриц и информации о тактиках, техниках и подтехниках, можно найти информацию о «группировках» («кластерах активности с общими названиями») злоумышленников, а также информацию об их «типичном поведении» (рис. 2).

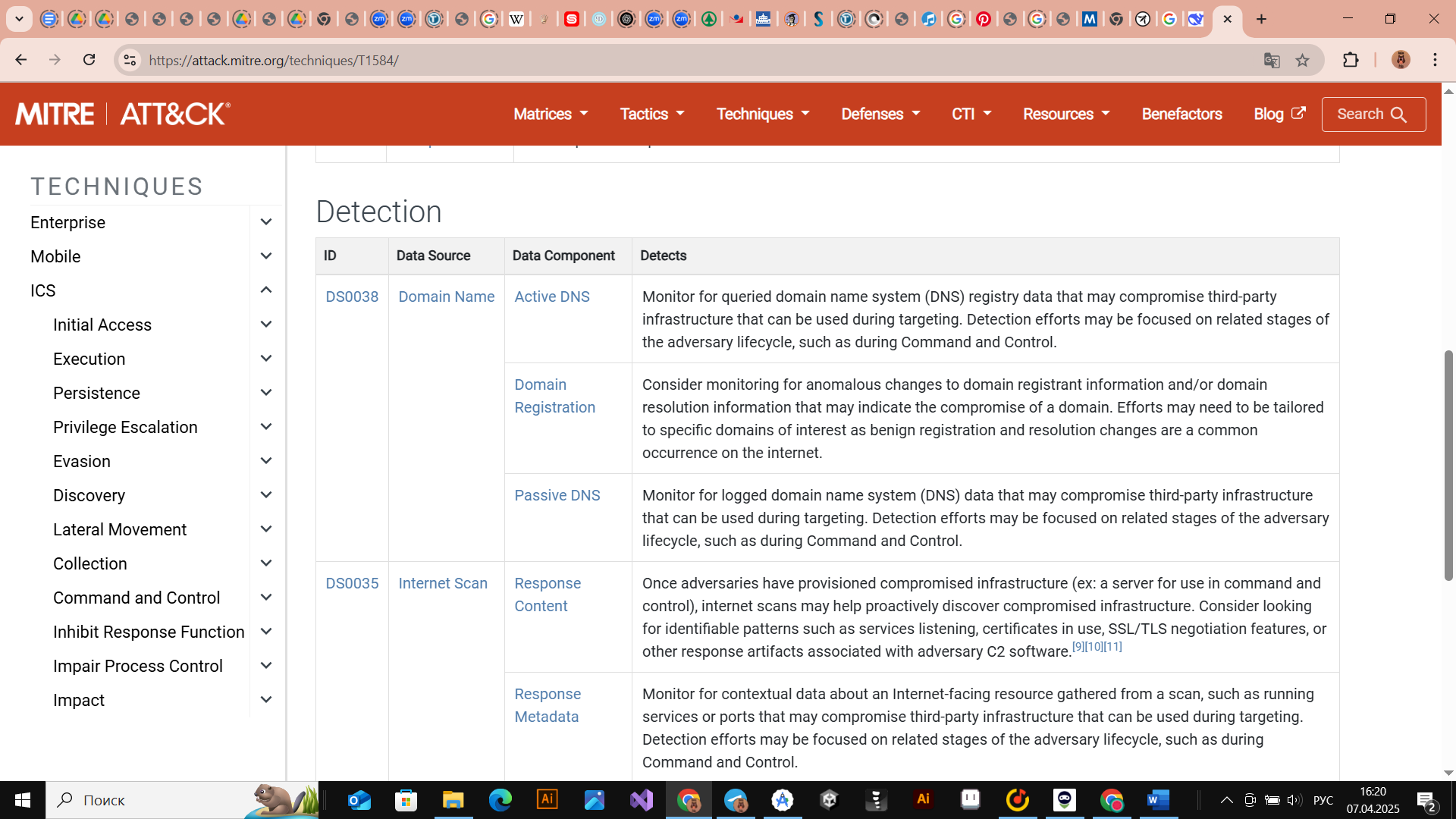


Рис. 2, информация об Detection в разделе «Compromise Infrastructure

»

# ИЗУЧЕНИЕ OWASP

OWASP, или «Open Worldwide Application Security Project», представляет собой международную некоммерческую организацию, целью которой является повышение безопасности веб-приложений и другого программного обеспечения. Один из ключевых принципов OWASP заключается в том, что все их материалы доступны для общественности и могут быть найдены на их официальном сайте.

Наиболее известным проектом OWASP является OWASP Top-10 — это периодически обновляемый отчет, в котором перечислены 10 наиболее распространенных проблем безопасности (уязвимостей) веб-приложений. В настоящее время актуальна версия 2021 года, однако в первой половине 2025 года ожидается выход нового отчета.

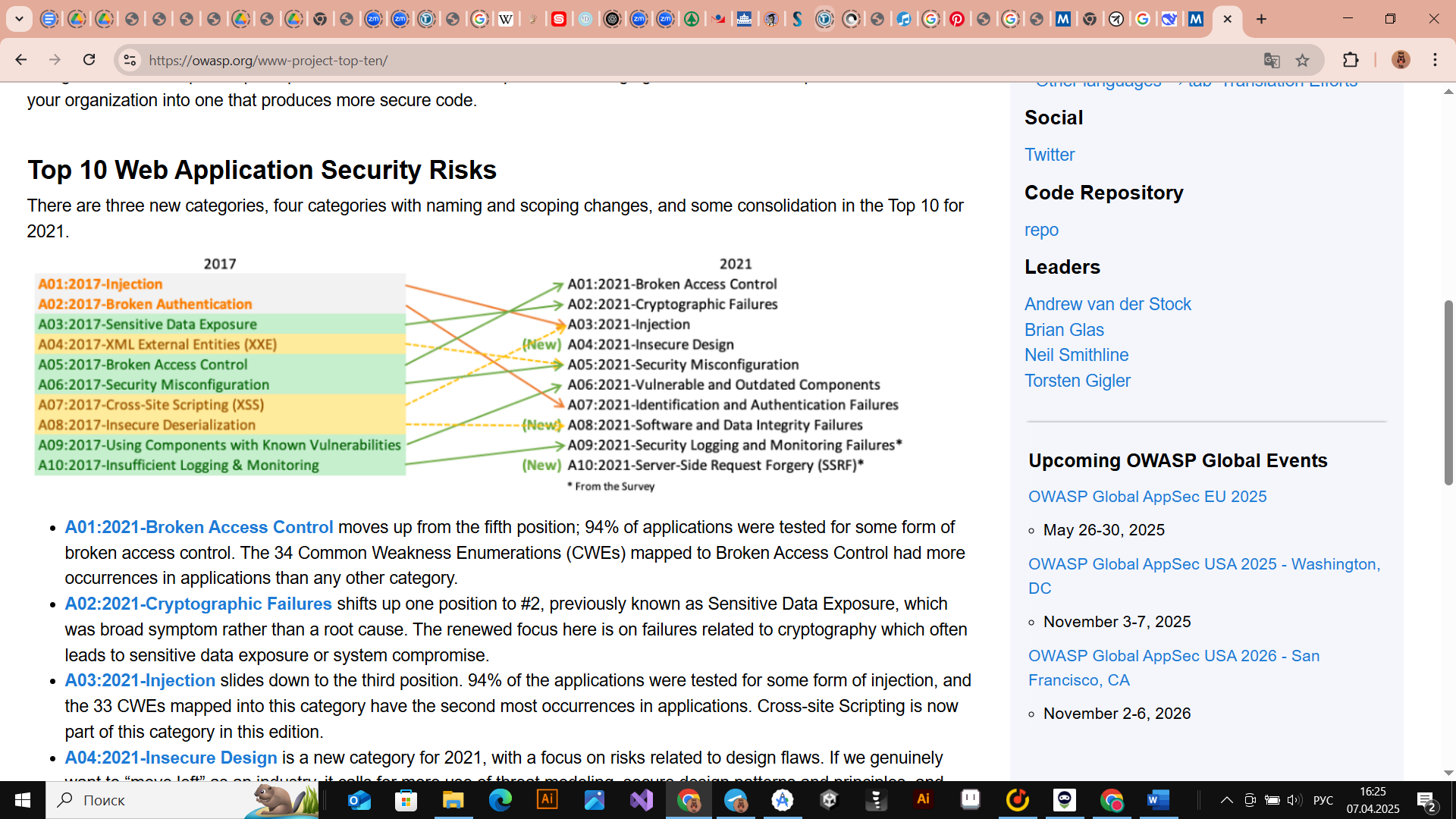


Рис. 3, Отчет OWASP Tоp-10

OWASP ASVS (Application Security Verification Standard) – это инициатива OWASP, представляющая собой стандарт для оценки уровня безопасности приложений. Основная цель данного проекта заключается в «нормализации диапазона охвата и уровня строгости при проверке безопасности веб-приложений».

Предусматривается использование ссылок на требования ASVS в установленном формате, что служит различным целям, включая указания для разработчиков и сторонних специалистов, занимающихся обеспечением безопасности приложений. Формат ссылки выглядит следующим образом: <chapter>.<section>.<requirement>, где каждая из трех позиций обозначается числом. Также может быть указана версия ASVS, в этом случае формат будет изменен на v<version>-<chapter>.<section>.<requirement>; если версия не указана, ссылка подразумевает требование из самой последней версии.

OWASP Gen AI – это проект, посвященный обеспечению безопасности генеративного искусственного интеллекта. В рамках этого проекта был создан список «OWASP Top-10 LLM and Gen AI», который включает 10 основных уязвимостей для языковых моделей и генеративного ИИ. На сайте проекта доступен документ на русском языке под названием «Топ-10 OWASP для приложений LLM 2025», датированный 11 марта 2025 года, в котором представлены наиболее распространенные уязвимости, объясняются их причины и предлагаются методы их устранения (документ доступен также на других языках).

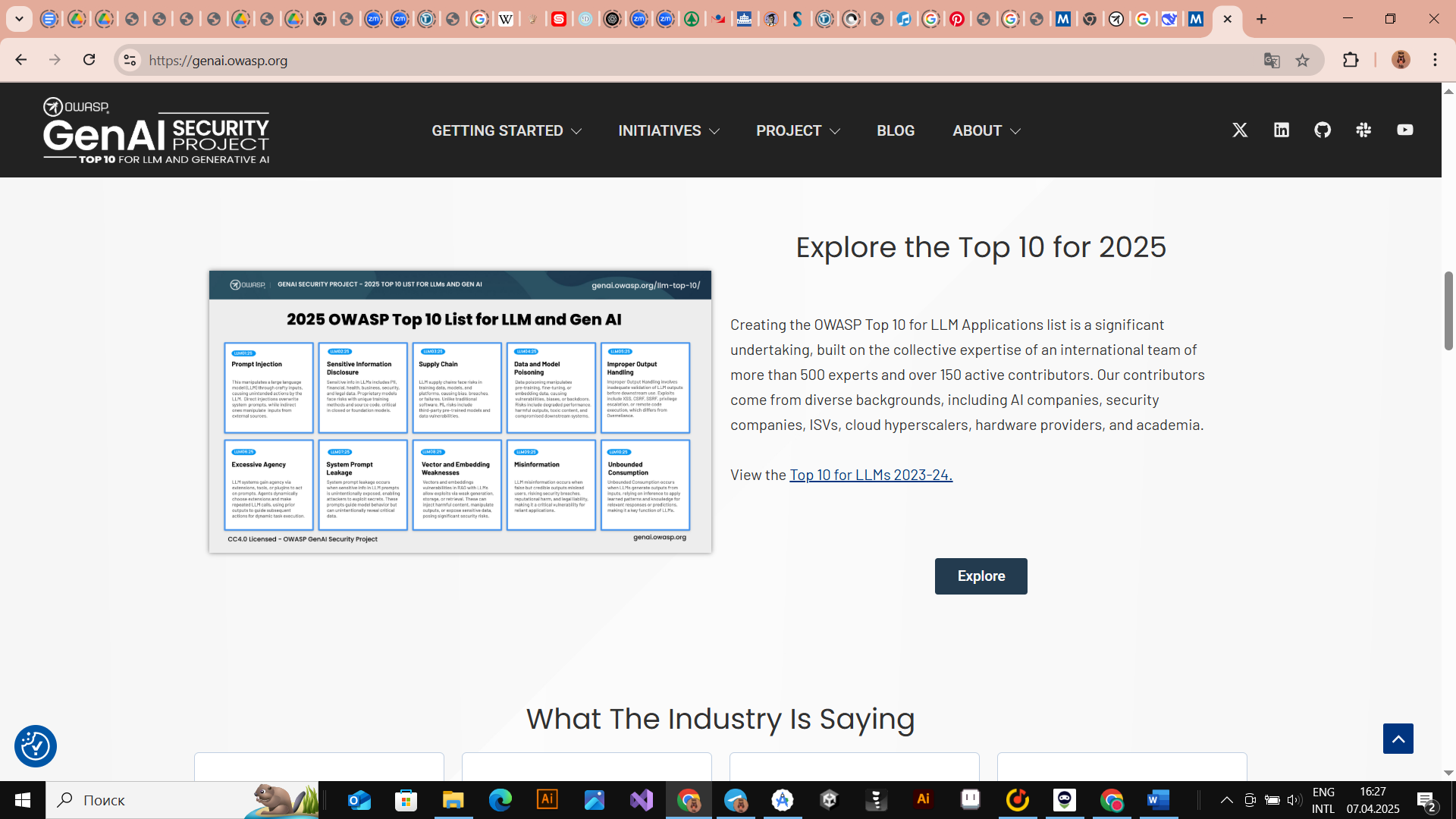


Рис. 4, OWASP Top-10 LLM and Gen AI 2025

OWASP Juice Shop – это «намеренно небезопасное» веб-приложение, разработанное для обучения в области безопасности, демонстрации уязвимостей, проведения командных турниров и тестирования инструментов безопасности. Оно включает в себя уязвимости из списка OWASP Top-10 и другие. В рамках лабораторных работ по дисциплине «проектная деятельность» я запускал это приложение в контейнере Docker и проводил тестирование на нем с использованием различных инструментов проверки безопасности.

OWASP MAS (Mobile Application Security) представляет собой стандарт безопасности для мобильных приложений (MASVS, Mobile ASVS) и подробное руководство по тестированию мобильных приложений (MASTG). Эти документы описывают процессы, методы и инструменты, применяемые при тестировании безопасности мобильных приложений, а также содержат исчерпывающий набор тестовых сценариев, позволяющих тестировщикам получать согласованные и полные результаты. Текущая версия MASVS составляет 2.1.0, а MASTG – 1.7.0.

OWASP WSTG (Web Security Testing Guide) – это детальное руководство по тестированию безопасности веб-приложений и веб-сервисов, созданное специалистами в области кибербезопасности. OWASP называет его «сводом лучших практик, используемых тестировщиками на проникновение и организациями по всему миру». Формат ссылки на WSTG выглядит следующим образом: WSTG-<category>-<number>. Если необходимо указать версию документа, формат будет: WSTG-<version>-<category>-<number>.

OWASP ZAP – это бесплатный open-source сканер уязвимостей, аналогичный Burp Suite, который позволяет проводить как ручное, так и автоматическое сканирование веб-приложений.

OWASP Dependency-Check – это инструмент для анализа компонентов программного обеспечения (SCA), который предназначен для выявления известных уязвимостей в зависимостях проекта. Он был разработан после того, как уязвимость, связанная с использованием компонентов и библиотек с известными уязвимостями, попала в список OWASP Top-10 в 2013 году.

Это далеко не все проекты OWASP: на их GitHub представлено более 1300 репозиториев, и любой желающий может предложить свой проект. Однако перечисленные и описанные выше инициативы являются основными и наиболее широко используемыми.

# РАЗБОР ИНЦЕДЕНТА

В 2024 году наблюдалась повышенная активность киберпреступных группировок Head Mare и Twelve, которые начали осуществлять целенаправленные атаки на российские организации. Основной особенностью кампаний стало применение схожих инструментов и инфраструктуры, ранее ассоциируемых исключительно с группой Twelve. В частности, с середины 2024 года группа Head Mare стала использовать программные модули, средства закрепления в системах и вредоносные компоненты, совпадающие по сигнатурам с ранее известными разработками Twelve. Также были замечены совпадения в используемых командных серверах и методах эксфильтрации данных.

Атаки были направлены на широкий спектр целей, включая телекоммуникационные компании, промышленные предприятия, учреждения государственного сектора и организации, обеспечивающие работу критической инфраструктуры. Все зафиксированные кампании отличались высокой степенью организации и проводились в несколько этапов, начиная от проникновения в инфраструктуру жертвы и заканчивая внедрением вымогательского программного обеспечения или выводом данных на внешние ресурсы.

Первоначальный этап атаки предполагал получение доступа во внутреннюю сеть организации. Злоумышленники использовали фишинговые письма с вложенными вредоносными документами, а также эксплуатировали уязвимости во внешних веб-сервисах и шлюзах удалённого доступа. Получив начальный доступ, они разворачивали инструменты для внутренней разведки.

На следующем этапе происходил сбор данных о структуре сети. Злоумышленники применяли PowerShell-скрипты, а также специализированные инструменты, такие как Mimikatz, для извлечения учётных данных. После получения нужных привилегий они перемещались по сети с помощью встроенных системных средств, включая PsExec и WMI. Это позволяло им контролировать всё большее количество машин и сервисов в сети жертвы.

После установления контроля злоумышленники приступали к эксфильтрации данных — копировали и передавали конфиденциальную информацию на внешние управляющие серверы, находящиеся под их контролем. В ряде случаев происходило шифрование данных с применением программ-вымогателей, таких как Babuk и LockBit 3.0. Жертвам предоставлялось уведомление с требованиями оплаты выкупа за восстановление доступа к зашифрованным файлам.

В процессе анализа вредоносных программ, использованных в атаках, были обнаружены совпадения в коде, конфигурациях и подходах к созданию оболочек вредоносных компонентов. Программные фрагменты, ранее идентифицированные как принадлежащие Twelve, были замечены в новых кампаниях Head Mare. Также наблюдалось использование одних и тех же C2-серверов в различных атаках, что указывало на тесную техническую связанность между двумя группами.

Кроме того, в ходе атак применялись разнообразные методы маскировки активности: использование легитимных утилит Windows, минимизация следов присутствия, внедрение кода через PowerShell без записи на диск и другие техники, затрудняющие обнаружение угроз стандартными антивирусными решениями.