***К. Д. Андреев, Е. А. Милютина, С. В. Бегичева***
*Уральский государственный экономический университет, г. Екатеринбург*
**УДК 004.056**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТРИЦ ТЕХНИК КИБЕРАТАК MITRE ATT&CK и ФСТЭК БДУ

**Аннотация.** В работе представлен анализ матриц техник кибер-преступлений MITRE ATT&CK и ФСТЭК, выполнено сравнение матриц с выделением их преимуществ и недостатков. Выявлена наиболее полная и актуальная база данных по угрозам и техникам.

**Ключевые слова:** матрица, информационная безопасность, база данных, анализ, кибер угрозы, критическая информационная инфраструктура.

**Введение.** В настоящее время наблюдается переход от индустриального общества к информационному. Так, постоянный рост количества пользователей сети Интернет позволяет каждому воспользоваться всеми ее информационными преимуществами. Однако вместе с новыми возможностями эта инфраструктура принесла и новые угрозы, а, следовательно, повышается важность защиты информационных технологий и информации с помощью инструментов информационной безопасности. Актуальная тема обнаружения вторжений, методам и моделям выявления нарушителей кибербезопасности рассматривается во многих исследованиях [1, 2].

**Проблема исследования.** Ежедневно большое количество компаний подвергаются кибератакам со стороны злоумышленников. Киберпреступники хотят повлиять на работу инфраструктуры государственных и коммерческих организаций ради финансовой или личной выгоды. С ростом количества кибератак, совершенствуется функционал инструментов по противодействию цифровой агрессии и создаются организации, изучающие киберпреступления и техники их совершения. Так, в 2013 году американская компания MITRE разработала базу данных классификации и описания кибератак «ATT&CK» (The Adversarial Tactics, Techniques, and Common Knowledge). Чуть позже, в 2015 году, российскими специалистами Федеральной службы по техническому и экспортному контролю был разработан свой банк данных угроз в сфере кибербезопасности.

Правильный выбор классификации угроз может положительно повлиять на деятельность всех организаций и исключить недостаток знаний в области типов атак на критическую инфраструктуру. Цель настоящей статьи — определить наиболее информативную и актуальную матрицу техник и угроз для использования.

**Материалы и методы.** В настоящей работе анализируются следующие источники данных: БДУ ФСТЭК (банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю) и ATT&CK (The Adversarial Tactics, Techniques, and Common Knowledge). Эти источники содержат подробную информацию о техниках, тактиках, процедурах предотвращения и опережения атак. Для сравнительного анализа важно понимать суть и структуры БДУ ФСТЭК и MITRE ATT&CK.

Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (далее — БДУ ФСТЭК) — это единый отечественный ресурс, который включает в себя всю необходимую информацию, связанную с уязвимостями программного обеспечения [3]. БДУ ФСТЭК содержит в себе перечень и описание угроз безопасности

информации критической инфраструктуры информации. Так «Новый раздел угроз», разработанный в 2021 году, представляет собой матрицу, которая разбивает все угрозы безопасности на их подвиды и способы их реализации. Такая структура позволяет производить моделирование угроз и определять меры защиты в зависимости от ситуации.

MITRE ATT&CK — это общедоступная база знаний тактик и методов, которые могут использоваться киберпреступниками. MITRE ATT&CK создается и пополняется данными наблюдений за реальными атаками [4]. Большинство организаций пользуются именно этой базой (матрицей) при создании моделей угроз, используемых для проверки безопасности среды. Основная цель применения MITRE ATT&CK организациями заключается в упрощении задачи реагирования на вторжения.

**Результаты.** При сравнении БДУ ФСТЭК и MITRE ATT&CK было выявлено, что каждая из матриц содержит, помимо названия и кода угрозы: краткое описание угрозы, ее вероятные источники, объекты воздействия и последствия, которые повлечет за собой реализация этой угрозы. При этом при внешнем сходстве указанных баз данных основное различие заключается в их структуре. Так, у БДУ ФСТЭК по столбцам расположены виды атак, а по строкам — способы их реализации, а у MITRE ATT&CK в столбцах содержится информация о тактиках, а в строках — о техниках.

БДУ ФСТЭК содержит информацию о 222 угрозах, распределенных между 11 типами атак. В свою очередь матрица MITRE содержит данные 227 угроз, распределенных между 14 тактиками нарушений. БДУ ФСТЭК может показаться менее «насыщенной» информацией, однако, это не так: данная база данных содержит в себе все типы угроз, которые были замечены в Российской Федерации. При этом, матрица MITRE содержит в себе устаревшие угрозы, которые неактуальны на протяжении последних 20 лет. Кроме того, методика ФСТЭК содержит больше технических деталей и описаний сценариев атак, чем матрица MIT

Следующее отличие БДУ ФСТЭК и MITRE ATT&CK — это возможности практического применения этих баз. В модернизированном разделе БДУ ФСТЭК можно сформировать перечень угроз с учетом негативных последствий, их объектов, компонентов, способов реализации, типов нарушителей с учетом прав доступа, а также в зависимости от мер защиты объекта критической инфраструктуры. Такая структура БДУ позволяет произвести прогнозирование и профилактику возможной атаки. Структура MITRE ATT&CK позволяет специалистам быстро ориентироваться и понимать все связи между любыми компонентами угроз. На странице техники можно узнать о ее описании, различных вариациях, используемых инструментах в совокупности с техникой, а также ознакомиться с историей применения на практике. Матрица MITRE ATT&CK используется специалистами во время атак, а модернизированный раздел БДУ ФСТЭК позволяет не только анализировать угрозы, но и усовершенствовать систему защиты информации в зависимости от текущих уязвимостей.

**Заключение.** Результаты проведенного анализа позволяют сделать вывод о том, что база данных угроз информации ФСТЭК является более информативной и функциональной в сравнении с матрицей MITRE ATT&CK. БДУ ФСТЭК содержит актуальную для Российской Федерации информацию об угрозах, обладает более удобной структурой, позволяет совершенствовать систему защиты информации в организации.

**СПИСОК ЛИТЕРАТУРЫ**


1. Котенко И.В., Хмыров С.С. Анализ актуальных методик атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры // Юбилейная X Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2021). — 2021. — СПб.: СПбГУТ, 2021. — Т. 1. — С. 536-541.
2. Котенко И. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров // Вопросы кибербезопасности. — 2022. — № 4 (50). — С. 52-79. — DOI 10.21681/2311-3456-2022-4-52-79. — EDN AIULIP.
3. Банк данных угроз безопасности информации [Электронный ресурс] URL: https://bdu.fstec.ru/ (дата обращения: 04.05.2024)
4. База техник, тактик и процедур, используемых злоумышленниками ATT&CK. — URL: https://attack.mitre.org/ (дата обращения: 04.05.2024).