УДК 004.056 Вестник УрФО № 4(58) / 2025, с. 44–52

Мельников Д. Ю.

10.14529/secur250405

СИСТЕМА АЛГОРИТМОВ ОБНАРУЖЕНИЯ КОМПЛЕКСНЫХ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ АНАЛИЗА ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ И СОПОСТАВЛЕНИЯ С БАЗОЙ ЗНАНИЙ MITRE ATT&CK

В статье описана система, состоящая из четырех ключевых алгоритмов, обеспечивающих реализацию модели обнаружения комплексных компьютерных атак, основанную на анализе действий пользователей, сетевых взаимодействий, с применением методов машинного обучения и сопоставлении с базой знаний MITRE ATT&CK. Первый алгоритм предназначен для формирования и инкрементального обновления профилей действий пользователя с механизмами версионирования и защитой от целевого искажения данных. Второй алгоритм выполняет локальное обнаружение аномалий, объединяя результаты эвристического анализа, результаты работы автокодировщика и графового анализа взаимодействий с калибровкой выходных оценок. Третий алгоритм осуществляет группировку аномалий в логические группы событий на основе взвешенных метрик сходства. Четвёртый алгоритм сопоставляет группы событий с тактиками и техниками базы знаний MITRE ATT&CK с помощью байесовского объединения оценок и модели переходов между техниками, что позволяет восстанавливать наиболее вероятные сценарии атак и формировать уведомления. Основной вклад работы заключается в формализации внутренней логики каждого алгоритма, описании процедур калибровки и критериев принятия решений.

Ключевые слова: *Комплексная компьютерная атака, обнаружение аномалий, профиль действий пользователя, графовые сверточные сети (GCN), MITRE ATT&CK.*

SYSTEM OF ALGORITHMS FOR DETECTING COMPLEX COMPUTER ATTACKS BASED ON ANALYSIS OF USER ACTIONS AND COMPARISON WITH THE MITRE ATT&CK KNOWLEDGE BASE

The article describes a system consisting of four key algorithms that enable the implementation of a model for detecting complex computer attacks based on the analysis of user actions and network interactions, using machine learning methods and comparison with the MITRE ATT&CK knowledge base. The first algorithm is designed to form and incrementally update user behavior profiles with versioning mechanisms and protection against targeted data corruption. The second algorithm performs local anomaly detection by combining the results of heuristic analysis, the results of the autoencoder, and graph analysis of interactions with output score calibration. The third algorithm groups anomalies into logical event groups based on weighted similarity metrics. The fourth algorithm matches event groups with tactics and techniques from the MITRE ATT&CK knowledge base using Bayesian estimation and a model of transitions between techniques, which allows the most likely attack scenarios to be reconstructed and notifications to be generated. The main contribution of the work is the formalization of the internal logic of each algorithm, the description of calibration procedures, and decision-making criteria.

Keywords: *Comprehensive computer attack, anomaly detection, user behavior profile, graph convolutional networks (GCN), MITRE ATT&CK.*

Введение

Современные информационные системы все чаще становятся объектами комплексных компьютерных атак [1]. В предыдущей работе [2] автором была предложена модель обнаружения комплексных компьютерных атак (далее — ККА), основанная на анализе действий пользователей, сетевых взаимодействий, с помощью метода машинного обучения - автокодировщика и графовых сверточных сетей (далее — GCN) и сопоставлении обнаруженных аномалий с базой знаний MITRE ATT&CK и введены ключевые обозначения Важной особенностью модели является возможность выявлять не только отдельные аномальные события, но и объединять их в логически связанные группы, отражающие этапы реализации атаки. Концептуально модель рассматривает ККА как последовательность взаимосвязанных групп событий, каждая из которых соотносится с определённой тактикой или техникой из базы знаний MITRE ATT&CK [3]. Такой способ представления позволяет преобразовывать поток данных в структурированные цепочки действий и оценивать их согласованность по времени, контексту и задействованным субъектам. В текущей статье подробно описываются четыре ключевых алгоритма, реализующие ранее описанную модель обнаружения ККА.

1. Алгоритм формирования и поддержки профиля действий пользователей

Профиль действий пользователей отражает типичные действия субъекта и служит эталоном для последующего выявления анома-

лий. На вход поступает поток нормализованных событий $e = (u,a,t,c)$, где u — пользователь, a — действие, t — время, c — контекст. Из этих событий формируется вектор текущих наблюдений O_t, агрегирующий количественные и категориальные признаки (частота действий, распределение по времени, уникальные контексты и т.д.). Эталонный профиль пользователя обозначается как $P_u(t)$. Для оценки различий между текущими наблюдениями и эталоном используется мера отклонения:

$$D = |O_t - P_u(t)|,$$

Если D не превышает порог τ, то значения обновляются по правилу экспоненциального сглаживания:

$$P_u(t+1) = (1 - \alpha)\, P_u(t) + \alpha f(e_t),$$

где $f(e_t)$ — вектор признаков события, а α — коэффициент сглаживания.

В случае значительного отклонения $D>\tau$ применяется процедура временного учёта, где новые данные учитываются временно, пока аналогичные изменения не подтвердятся из нескольких источников. После подтверждения изменений формируется новая версия профиля с указанием различий. Версионирование и контроль источников защищают от целенаправленного искажения данных (data poisoning). Порог τ и коэффициент α подбираются на валидационной выборке для минимизации ложных срабатываний и обеспечения устойчивости адаптации к изменениям в действиях пользователей. На Рисунке 1 представлена схема алгоритма формирования профиля действий пользователя.

2. Алгоритм обнаружение аномалий

Алгоритм выполняет обнаружение нетипичных соб ытий на уровне индивидуальных действий пользователей в реальном времени. Используются три уровня анализа: эвристический, статистический (автокодировщик), графовый анализ взаимодействий.

2.1. Эвристический уровень включает простые логические правила. Они дают бинарный индикатор S_r (1 — сработало, 0 — нет). Эвристический анализ может быть реализован на основе уже функционирующих средств защиты информации, которые фиксируют события информационной безопасности. Такие сигналы используются как готовые индикаторы, что позволяет снизить нагрузку на систему.

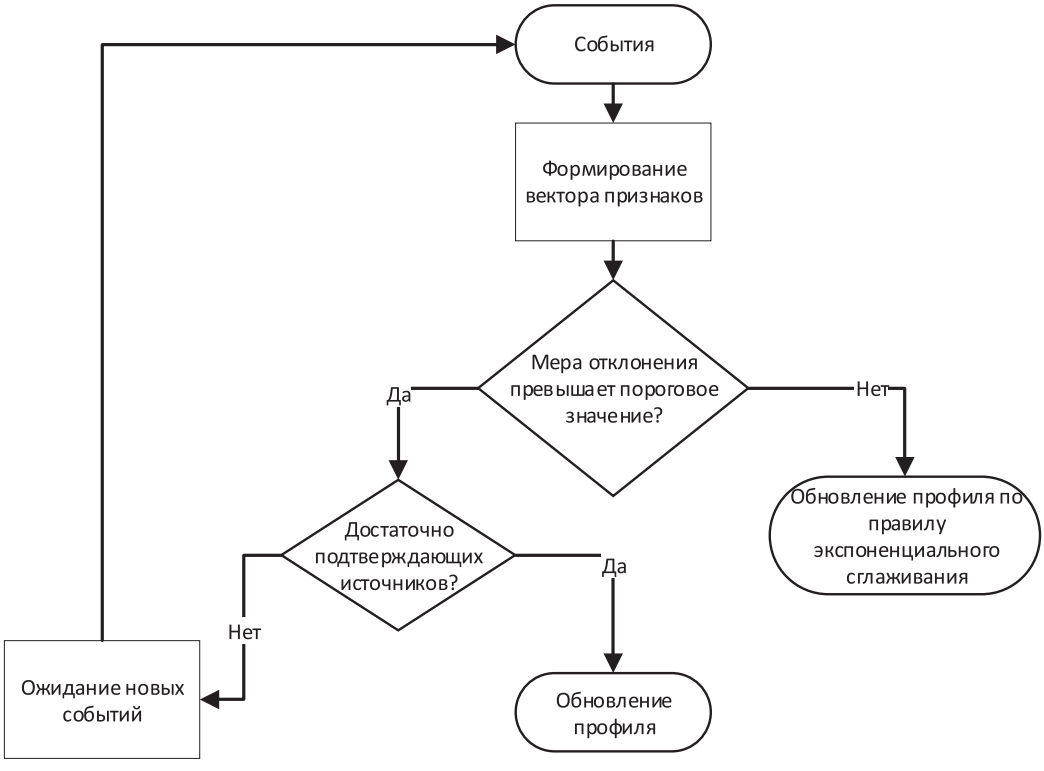

Рис. 1. Алгоритм формирования профиля действий пользователя

2.2. На статистическом уровне оценивается степень отклонения входного вектора O_t от профиля $P_u(t)$. Для этого применяется метод машинного обучения — автокодировщик, обученный на нормальных данных о действиях пользователей. Для каждого наблюдения вычисляется нормированная среднеквадратичная ошибка:

$$nMSE(X, X') = \frac{1}{d}\sum_{i=1}^{d}(X_i - X'_i)^2,$$

где d — число признаков, x — входной вектор, X'_i — восстановление. Ошибка восстановления нормируется, а результат переводится в шкалу от 0 до 1, формируя оценку S_s, посредством калибровочной функции, которая строится эмпирически. Порог обнаружения выбирается на валидации.

2.3. Для выявления структурных аномалий формируются локальные подграфы взаимодействий вокруг сущностей. Узлы представляют пользователей, устройства, процессы и файлы. Рёбра кодируют различные семантики взаимодействий (аутентификация, сетевые соединения, файловые операции). В качестве признаков используются частотные агрегаты, временные характеристики и контекстные метрики. GCN извлекают векторные представления подграфов, далее структурная оценка определяется как отклонение векторных представлений от эталонных значений, после чего значение нормируется. Результат графового анализа выражается через S_g, приведённый к аналогичной шкале.

2.4 Итоговая оценка аномальности вычисляется по агрегированной формуле:

$$S = w_1 S_r + w_2 S_s + w_3 S_g,$$

где w_i — весовые коэффициенты, определяемые по результатам калибровки. Первичные результаты трёх уровней анализа калибруются на валидации (перцентильное нормирование) и приводятся к сопоставимой шкале [0,1]. Веса w_i и порог τ_S подбираются оптимизацией метрик (F1, precision, FP, FN). После маркировки события передаются в модуль группировки. На рисунке 2 представлена схема алгоритма обнаружения аномалий.

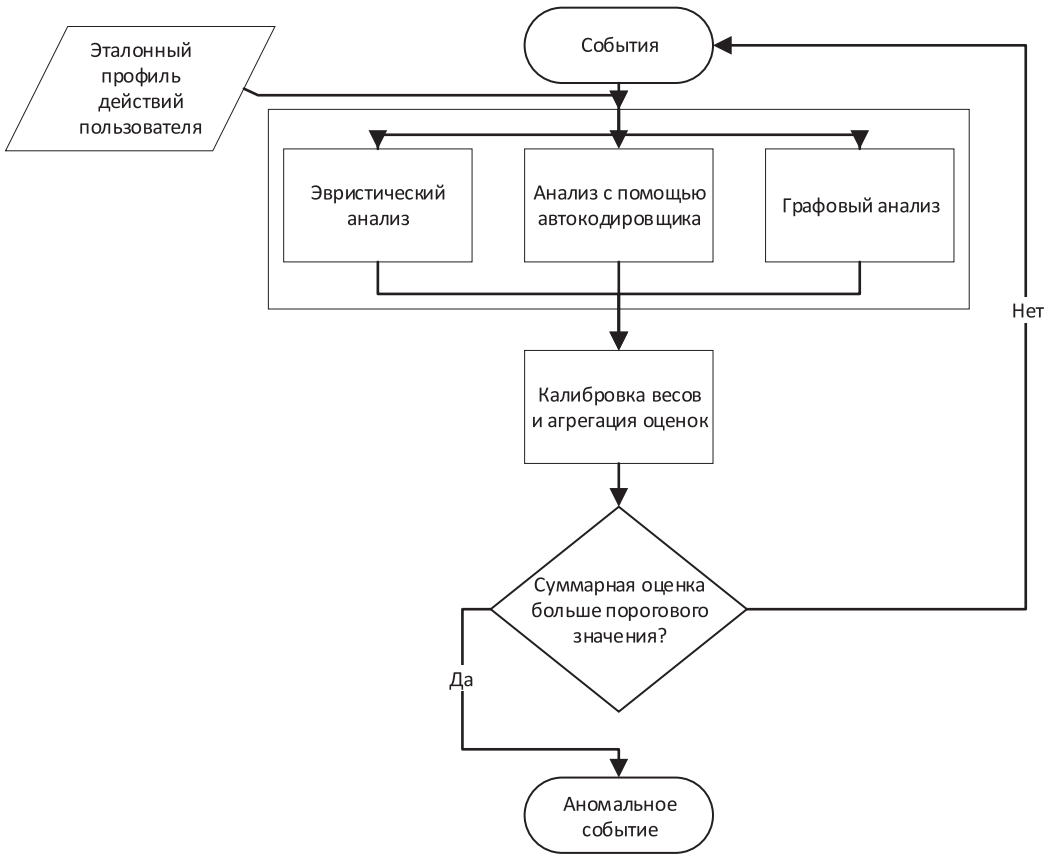

Рис. 2. Алгоритм обнаружения аномалий

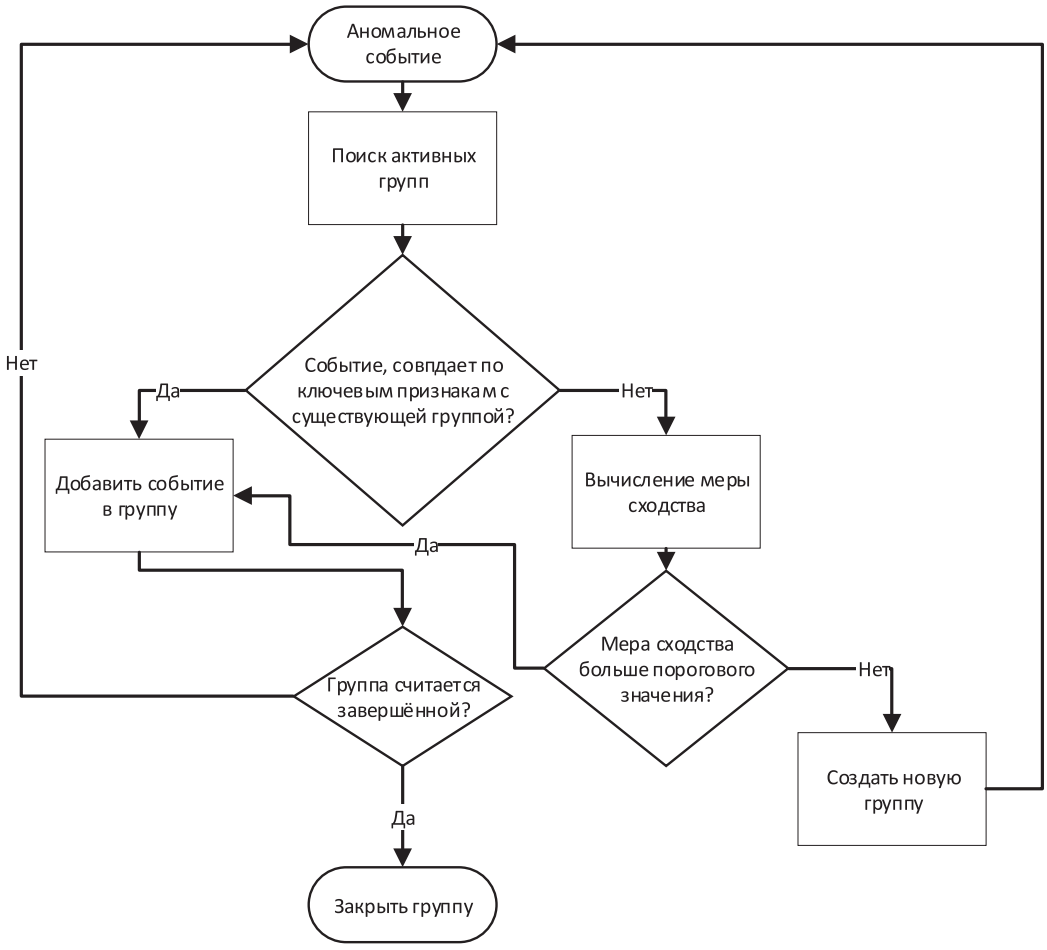

Рис. 3. Алгоритм группировки аномалий

3. Алгоритм группировки аномалий

После обнаружения отдельные аномалии объединяются в группы событий — потенциальные этапы комплексной атаки. Каждое новое событие сравнивается с уже существующими группами G_i. Если совпадают ключевые признаки (учётная запись, IP-адрес и т.д.), то событие приписывается к группе. Если соответствия нет, то вычисляется мера сходства:

$$A(G_i, e) = \sum_j w_j \cdot sim_j(G_i, e),$$

где sim_j— частные меры схожести (по времени, контексту, субъекту и т.д.), а w_j— их веса. При условии того, что агрегированная мера $A(G_i,e)$ превышает порог, событие включается в группу, в противном случае создаётся новая. После добавления события агрегированные параметры группы обновляются (временные границы, средняя аномальность и список задействованных субъектов). Группа считается завершённой, если не поступают новые события в течение заданного времени. На рисунке 3 представлена схема алгоритма группировки аномалий.

4. Алгоритм сопоставления с базой знаний «MITRE ATT&CK»

Каждая группа событий G сопоставляется с техниками и тактиками из базы знаний MITRE ATT&CK. Для каждого события оценивается вероятность его соответствия технике T_k:

$$P(T_k \mid e) \propto P(e \mid T_k) P(T_k),$$

где $P(e|T_k)$ оценивается по шаблонам действий или обученной модели, а $P(T_k)$ — априорная частота встречаемости техники. Для группы вычисляется суммарная степень соответствия каждой тактике:

$$C_G(T) = \sum_{e_i \in G} s(e_i, T),$$

и выбирается тактика T^*, для которой $C_G(T^*)$ максимально. По последовательности группы событий восстанавливается сценарий атаки в соответствии с базой знаний MITRE ATT&CK. К примеру: «Initial Access - Privilege Escalation - Lateral Movement – Exfiltration».

Если интегральная оценка вероятности атаки превышает порог γ, то система фиксирует факт комплексной компьютерной атаки и формирует отчёт с указанием событий, признаков, задействованных тактик и временных рамок инцидента. На рисунке 4 представлена схема сопоставления с базой знаний «MITRE ATT&CK»

5. Пример работы

Описанный пример основан на реальных данных, экспортированных из информационной инфраструктуры предприятия. Все идентифицирующие сведения далее в тексте анонимизированы для сохранения конфиденциальности. Данные взяты из журналов аутентификаций, системных журналов узлов сети, данные об активных процессах и сетевой трафик. Набор событий и их временная последовательность сохранены в полном объёме.

Рассмотрен профиль действий пользователя предприятия (Таблица 1), сотрудника экономического отдела. Профиль отражает основные характерные действия данного пользователя, сформированные на основе

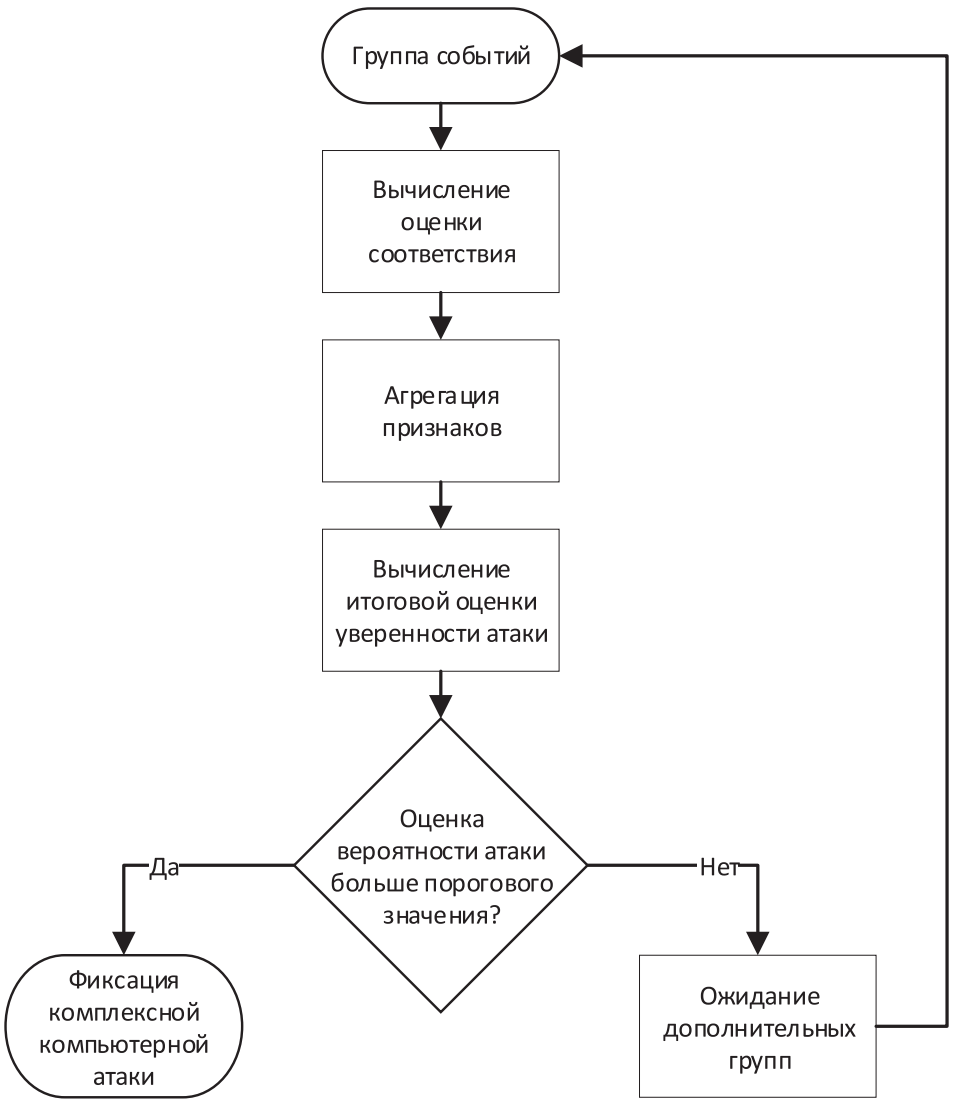

Рис. 4. Сопоставление с базой знаний «MITRE ATT&CK»

Таблица 1

Профиль действий пользователя

Параметр	Значение	Примечание
Должность / отдел	Экономический отдел	Работает с финансовыми документами и отчётами
Нормальное время активности	08:00–17:00	Рабочие часы (понедельник–пятница)
Нормальное значение времени	0.375	Нормированное значение в модели профиля
Основные устройства	Корпоративный ПК	Входы только с закреплённого рабочего места
Часто используемые приложения / сайты	Офисные программы (бухгалтерские и экономические)	
Частота неудачных входов	≤ 1 за сессию	Возникают редко, обычно после смены пароля
Новизна контекста (доля новых IP)	0.05	Низкая, входы почти всегда с одного IP
Изменчивость контекстов	0.10	Низкая, работа в однородной среде
Средний исходящий трафик (рабочее время)	≈ 200 МБ/час	Связан с передачей отчётов и выгрузок

Таблица 2

Данные, полученные из источников

№	Время	Источник данных	EventID	Тип события	Приложение / Процесс	Вх. трафик (MB)	Исх. трафик (MB)
1	16:57	Windows System Log	1074	Завершение работы	explorer.exe	0.00	0.00
2	21:03	Windows System Log	6005	Включение системы	system	0.02	0.01
3	21:04	Active Directory Security Log	4625	Неуспешная аутентификация	winlogon.exe	0.00	0.00
4	21:05	Active Directory Security Log	4625	Неуспешная аутентификация	winlogon.exe	0.00	0.00
5	21:06	Active Directory Security Log	4625	Неуспешная аутентификация	winlogon.exe	0.00	0.00
6	21:07	Active Directory Security Log	4624	Успешная аутентификация	winlogon.exe	0.03	0.02
7	21:11	Sysmon Log	7045	Установка ПО	anydesk.exe	0.05	0.15
8	21:27	NetFlow	—	Исходящее соединение	—	0.02	2430.00

данных, полученных за несколько недель нормальной работы пользователя. Эти характеристики хранятся в профиле как эталон действий и используются для оценки отклонений.

В таблице 2 представлены исходные данные, полученные из различных журналов узлов сети.

После поступления событий система формирует для каждого из них вектор наблюдений. Первое отклонение зафиксировано в момент включения компьютера в нетипичное для данного пользователя время 21:03, обычно активного с 8:00 до 17:00. Далее наблюдаются четыре последовательные неудачные попытки входа (события № 3–5), что рассма-

тривается системой как значимое отклонение от нормальной модели действий данного пользователя и служит основанием для перехода к расширенному анализу.

На этапе локального анализа начинают работать три параллельных канала. Эвристический канал срабатывает на сочетание признаков — вечернее время и серия неудачных входов подряд. Статистический канал сравнивает агрегированный вектор текущих наблюдений с эталонным профилем сотрудника — успешная аутентификация в 21:07 (событие № 6) существенно отличается от нормального распределения активности, и степень отклонения превышает порог. Структурный канал формирует локальный граф событий и фиксирует аномальную последовательность действий — сразу после успешного входа происходит установка программы удалённого доступа «AnyDesk» (событие №7), а затем фиксируется значительный объём исходящего трафика (событие №8). Такая цепочка событий для одного пользователя и одного узла сети нетипична и интерпретируется как возможный сценарий компрометации учётных данных и утечки данных за пределы информационной инфраструктуры.

Результаты трёх каналов приводятся к единой шкале и взвешиваются в соответствии с параметрами системы. Эвристический канал предоставил бинарный сигнал «аномалия», статистический канал зафиксировал значительное отклонение от профиля, а структурный подтвердил наличие нетипичной последовательности действий. Совокупная оценка превысила порог маркировки, и события №3–8 были отмечены как аномальные и переданы в модуль корреляции.

Модуль корреляции проверил временную и контекстную связанность событий. Все отмеченные события принадлежат одному пользователю и одному автоматизированному рабочему месту, а временные интервалы между ними не превышают нескольких минут. Вышеуказанные факты обеспечили высокую агрегированную меру сходства, превышающую порог приписывания, что позволило объединить записи в группу событий. В таблице 3 представлены значения используемых параметров в алгоритмах.

На этапе сопоставления каждая запись группы получила оценки соответствия техникам базы знаний MITRE ATT&CK. Серия неудачных аутентификаций и последующий успешный вход интерпретируются как техники «Credential Access» и «Initial Access», установка «AnyDesk» — как возможное исполнение с использованием внешнего инструмента «Remote Services», а исходящая передача данных — как техника «Exfiltration». Агрегированная поддержка по группе показала последовательность техник «Credential Access (T1110) — Initial Access (T1078) — Remote Services (T1021) — Exfiltration (T1041)». Суммарная уверенность превысила порог, и система создала уведомление, в котором указаны состав группы событий, временные рамки, перечислены ключевые признаки и техники базы знаний MITRE ATT&CK.

Таблица 3

Значения параметров

Параметр	Обозначение	Значение
Окно агрегации признаков	—	30 мин
Порог отклонения профиля	τ	0.5
Коэффициент экспоненциального сглаживания	α	0.2
Вес эвристического канала	w_r	0.2
Вес статистического канала	w_s	0.5
Вес графового канала	w_g	0.3
Порог итоговой аномалии	τ_S	0.6
Порог приписывания к группе событий	τ_A	0.6
Порог уверенности для фиксирования ККА	γ	1.5

Проведённое внутренне расследование показало, что злоумышленник, который является сотрудником организации получил несанкционированный доступ, посредством перебора, к учётной записи сотрудника экономического отдела. В вечернее время, когда сотрудник отсутствовал на рабочем месте злоумышленник, после нескольких неудачных попыток, смог авторизоваться на автоматизированном рабочем месте сотрудника и установить программу для удалённого доступа с целью передачи информации за периметр информационной инфраструктуры предприятия.

Заключение

В работе представлены четыре взаимосвязанных алгоритма обеспечивающие функционирование модели обнаружения комплексных компьютерных атак: формирование и инкрементальную поддержку профиля действий пользователей, локальное обнаружение аномалий, группировку аномалий в логические группы событий и сопоставление этих групп с тактиками и техниками из базы знаний MITRE ATT&CK. Для каждого этапа подробно описаны внутренняя логика, ключевые критерии принятия решений и процедуры калибровки оценок.

Элементы решения включают адаптивное обновление профиля действия пользователя с применением экспоненциального сглаживания, политику «мягкого слияния» профилей с версионированием и проверкой изменений по нескольким источникам, гибридную многоуровневую схему обнаружения сочетающую эвристический анализ, автокодировщик и графовый анализ при которой выходные оценки каждого уровня приводятся к единой шкале и объединяются с помощью весов, а также байесовский подход к сопоставлению групп событий с техниками базы знаний MITRE ATT&CK с учётом условных вероятностей.

Стоит отметить, что для корректной работы алгоритмов необходимы разнородные, синхронизированные данные, корректные временные метки и достаточная плотность нормальных данных для обучения автокодировщика.

В дальнейшем, планируется практическая реализация описанных алгоритмов и их экспериментальная валидация, с автоматической настройкой весов и повышением устойчивости к целенаправленным атакам на профили.

Литература

1. Актуальные киберугрозы: I–II кварталы 2025 года – URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (дата обращения:20.11.2025).

2. D. Melnikov, «A Model for Detecting Complex Computer Attacks Based on the Analysis of User Actions, Network Interactions and Comparison with the MITRE ATT&CK Knowledge Base,» 2025 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russian Federation, 2025, pp. 221-224, doi: 10.1109/USBEREIT65494.2025.11054096.

3. MITRE. «ATT&CK® Design and Philosophy», March 2020. URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (дата обращения: 20.10.2025).

References

1. Aktualnyye kiberugrozy: I–II kvartaly 2025 goda – URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (accessed: - 20.11.2025).

2. D. Melnikov, «A Model for Detecting Complex Computer Attacks Based on the Analysis of User Actions, Network Interactions and Comparison with the MITRE ATT&CK Knowledge Base,» 2025 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russian Federation, 2025, pp. 221-224, doi: 10.1109/USBEREIT65494.2025.11054096.

3. MITRE. «ATT&CK® Design and Philosophy», March 2020. URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (accessed: 20.10.2025).

МЕЛЬНИКОВ Дмитрий Юрьевич, аспирант Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: melnikovdima517@yandex.ru

MELNIKOV Dmitriy Yuryevich, graduate student at the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: melnikovdima517@yandex.ru