УДК 004.056
Вестник УрФО № 3(61) / 2026, с. 30–47
DOI: 10.14529/secur260303

Мельников Д.Ю., Синадский Н.И.

РЕАЛИЗАЦИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ КОМПЛЕКСНЫХ КОМПЬЮТЕРНЫХ АТАК, ОСНОВАННОЙ НА АНАЛИЗЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ, СЕТЕВЫХ ВЗАИМОДЕЙСТВИЙ И СОПОСТАВЛЕНИИ ОБНАРУЖЕННЫХ АНОМАЛИЙ С ТАКСОНОМИЕЙ ТЕХНИК КОМПЬЮТЕРНЫХ АТАК

Melnikov D.Y., Sinadsky N.I.

IMPLEMENTATION OF A SYSTEM FOR DETECTING COMPLEX COMPUTER ATTACKS BASED ON ANALYSIS OF USER ACTIVITY, NETWORK INTERACTIONS, AND COMPARISON OF DETECTED ANOMALIES WITH THE TAXONOMY OF COMPUTER ATTACK TECHNIQUES

В статье представлена реализация системы обнаружения комплексных компьютерных атак, основанной на анализе действий пользователей, сетевых взаимодействий и сопоставлении обнаруженных аномалий с таксономией компьютерных атак. Обнаружение аномальных событий выполняется многоканальным детектором, объединяющим статистический, графовый и эвристический каналы. Также в системе формируется и актуализируется профиль действий пользователя. Выявленные аномальные события группируются с учётом временных, субъектных и контекстных связей. Из сформированных групп строятся цепочки групп аномальных событий, которые сопоставляются с таксономией компьютерных атак. При экспериментальной оценке системы на тестовом наборе сценариев комплексных компьютерных атак значения Precision, Recall и F1-меры на уровне отдельных событий составили 0,85, 0,79 и 0,82 соответственно. Средняя доля восстановленных этапов ККА составила 0,74, а доля полностью восстановленных цепочек 0,68. Апробация системы проведена при ретроспективной обработке анонимизированных данных, зарегистрированных в ходе реальной комплексной компьютерной атаки. В результате обработки данных аномальные события были объединены в связанные группы и цепочки групп аномальных событий, для которых выполнено сопоставление с таксономией компьютерных атак.

Ключевые слова: комплексные компьютерные атаки, обнаружение аномалий, профилизация действий пользователей, Apache Cassandra, графовые сверточные сети (GCN), MITRE ATT&CK

This article presents the implementation of a system for detecting complex computer attacks based on the analysis of user actions, network interactions, and the comparison of detected anomalies with a computer attack taxonomy. Anomalous events are detected by a multi-channel detector combining statistical, graph-based, and heuristic channels. The system forms and updates a user action profile. Detected anomalous events are grouped based on temporal, subject-based, and contextual links. Chains of anomalous event groups are then constructed and matched against the computer attack taxonomy. During the experimental evaluation of the system on a test set of complex computer attack scenarios, Precision, Recall, and F1-score at the individual event level were 0.85, 0.79, and 0.82, respectively. The average proportion of reconstructed attack stages was 0.74, while the proportion of fully reconstructed chains was 0.68. The system was evaluated through retrospective processing of anonymized data recorded during a real complex computer attack. As a result, anomalous events were combined into related groups and chains of groups, which were subsequently matched against the computer attack taxonomy.

Keywords: complex computer attacks, anomaly detection, user action profiling, Apache Cassandra, graph convolutional networks (GCN), MITRE ATT&CK

Введение

Современные информационные системы все чаще становятся объектами комплексных компьютерных атак [1]. Одной из проблем при обнаружении комплексных атак является необходимость совместного анализа разнородных данных и установления логических связей между отдельными аномальными событиями. Приказ ФСБ России № 554 [2] устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также для поиска признаков компьютерных атак. Системы обнаружения компьютерных атак (далее – СОА) должны реализовывать функции сбора и автоматического анализа событий информационной безопасности (далее - ИБ), корреляции разнородных событий, а также повторного анализа ранее зарегистрированных событий с целью выявления ранее не обнаруженных компьютерных инцидентов.

Вопросам обнаружения компьютерных атак (далее — КА) и анализа событий информационной безопасности посвящены работы [3-5]. В исследованиях [3,4] многошаговые КА рассматриваются как последовательность системных событий, отражающих взаимосвязанные действия злоумышленника. Для анализа таких последовательностей применяются методы машинного обучения и

механизмы представления знаний, используемые при анализе событий безопасности и идентификации отдельных этапов КА. В работе [5] исследованы архитектурные и функциональные аспекты построения подсистем предупреждения КА на объектах критической информационной инфраструктуры. В работах [6–14] представлены методы корреляции событий и машинного обучения для обнаружения аномалий и КА, включая автокодировщики и графовые нейронные сети, а также методы анализа сетевого трафика и SIEM-системы.

Рассмотренные подходы позволяют анализировать отдельные события и устанавливать связи между ними. При этом задача корреляции аномальных событий, относящихся к различным этапам комплексной компьютерной атаки (далее — ККА), остаётся актуальной.

Элементы предлагаемого подхода к обнаружению ККА ранее рассматривались в работах автора. В работе [15] предложена модель ККА, представляющая собой последовательность групп аномальных событий, соответствующих элементам базы знаний «MITRE ATT&CK», также описана модель обнаружения ККА. В рамках модели описан процесс построения и обновления профиля действий пользователей. Обнаружение аномальных событий осуществляется многоканальным детектором, включающим статистический канал на основе автокодировщика и графовый канал на основе графовой сверточной сети (GCN). В работе [16] разработана модель хранения данных в NoSQL-СУБД «Apache Cassandra» для системы обнаружения ККА, определены шесть целевых требований к системе хранения данных. Выполнены расчеты объемов хранения и размеров логически связанных групп записей. В работе [17] описана система алгоритмов обнаружения ККА, состоящая из четырех взаимосвязанных алгоритмов, обеспечивающих реализацию предложенной модели обнаружения ККА.

В настоящей работе представлена программная реализация системы обнаружения ККА и описывается её работа при ретроспективной обработке журналов событий реального инцидента ИБ. Целью исследования является оценка возможности разработанной системы выявлять ККА на основе анализа взаимосвязанных групп аномальных событий и их сопоставления с таксономией КА. В статье рассмотрены структура программного комплекса, функции его основных модулей, последовательность обработки событий и результаты апробации системы.

1. Архитектура и функциональные блоки программного комплекса

Система обнаружения ККА реализована в виде программного комплекса, построенного по модульному принципу. Программный комплекс обеспечивает последовательную обработку журналов событий и данных мониторинга информационной инфраструктуры, начиная с приёма первичных записей и заканчивая формированием результатов анализа и уведомлений о выявленных признаках

ККА. Архитектура системы ориентирована не на выявление отдельных аномальных событий, а на обнаружение взаимосвязанных групп аномальных событий. Архитектура программного комплекса предусматривает централизованное хранение данных в NoSQL‑СУБД «Apache Cassandra». В указанном хранилище консолидируются первичные записи журналов событий, версии профилей действий субъектов, векторные представления событий, группы аномальных событий, цепочки групп аномальных событий и итоговые результаты анализа. Архитектура системы обнаружения комплексных компьютерных атак представлена на рис. 1.

Модуль обработки событий (Event Processing Module) получает события из журналов аутентификации, системных журналов и иных источников данных. Поступившие данные приводятся к единому формату, выполняется синхронизация временных меток, проверка структуры и согласованности атрибутов. Для каждой записи сохраняются сведения об источнике данных и иные метаданные, необходимые для дальнейшей обработки. Далее события сохраняются в хранилище данных и передаются в аналитические модули системы.

Обработка данных выполняется в потоковом и пакетном режимах. В потоковом режиме поступающие события нормализуются, для них формируются признаки и рассчитывается первичная оценка аномальности. Пакетный режим применяется к накопленным данным. При повторной обработке пересчитываются признаковые описания событий, актуализируются профили действий субъектов и уточняются сформированные цепочки групп аномальных событий.

Модуль формирования и поддержки профиля действий пользователя (ProfileManager) обновляет профиль действий пользователя по мере поступления новых событий. События, признанные аномальными, при актуализации не учитываются. Профиль содержит агрегированные характеристики действий пользователя. В системе сохраняются версии профиля с указанием времени их формирования и набора событий, использованных при расчёте характеристик.

Многоканальный детектор (MultiChannelDetector) объединяет статистический, графовый и эвристический каналы. Каждый из них формирует частную оценку аномальности события, после чего оценки используются при расчёте итогового значения. Эвристический канал проверяет заданные формализованные правила. В статистическом канале применяется автокодировщик, обученный на данных нормальных действий пользователей: для признакового вектора события рассчитывается ошибка реконструкции, величина которой используется при определении частной оценки. Графовый канал анализирует взаимодействия субъектов и ресурсов информационной инфраструктуры. GCN формирует векторные представления вершин с учётом их связей и локального окружения, а оценка аномальности определяется по отклонению текущего представления

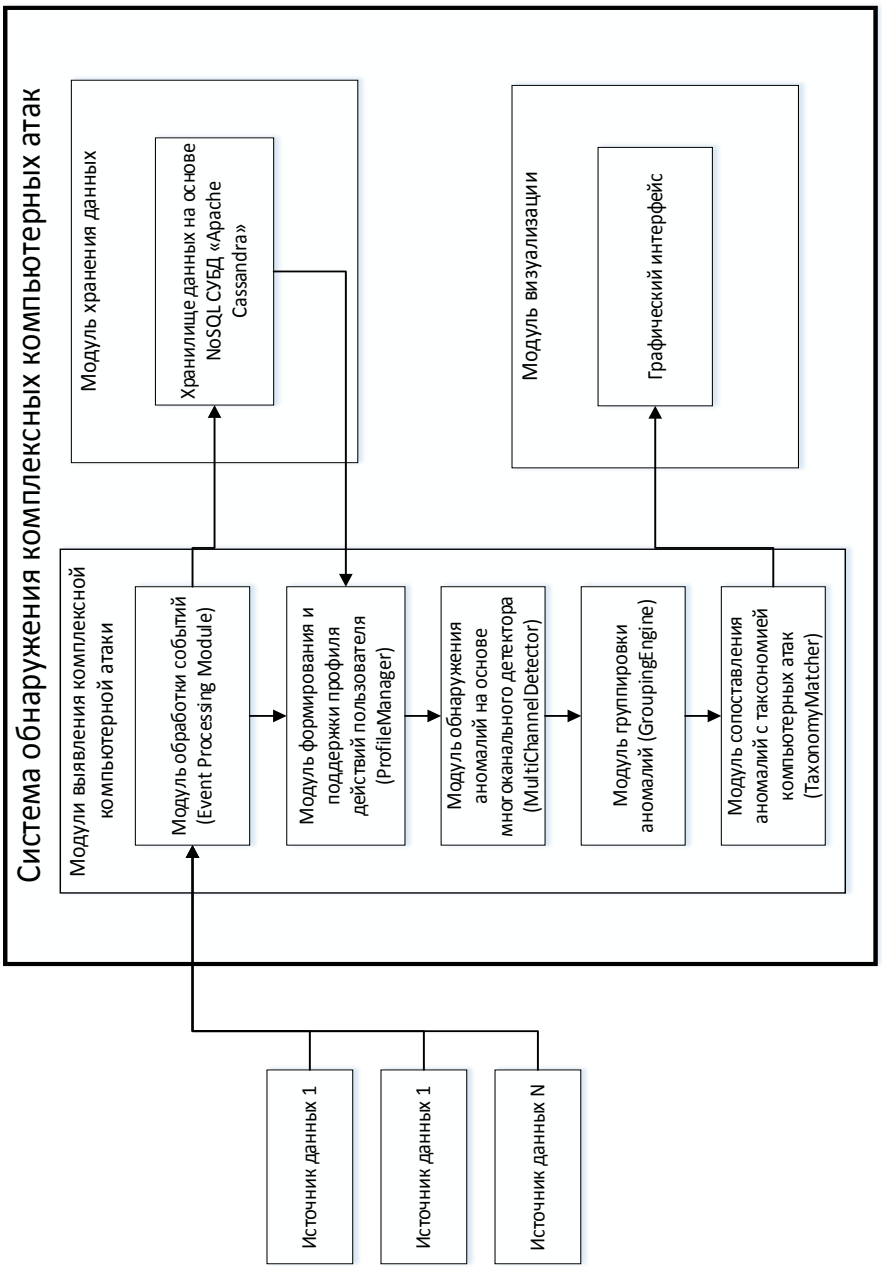

Рис. 1. Архитектура системы обнаружения комплексных компьютерных атак

от представлений, характерных для нормального функционирования информационной инфраструктуры.

На основе частных оценок MultiChannelDetector рассчитывает итоговую оценку аномальности события. Если она превышает установленное пороговое значение, событие признаётся аномальным и поступает в модуль группировки аномалий (GroupingEngine). При группировке учитываются временная близость событий, связи субъектов и ресурсов и сходство контекстных признаков. Для

сформированной группы сохраняются входящие в неё события, временные границы и оценки аномальности. Если в течение установленного интервала новые связанные аномальные события не поступают, группа считается завершённой. Связанные группы рассматриваются в порядке возникновения и объединяются в цепочки возможных этапов ККА.

Модуль сопоставления аномалий с таксономией компьютерных атак (TaxonomyMatcher) получает сформированные цепочки групп аномальных событий и сопоставляет их с элементами таксономии КА. При этом анализируются признаки входящих в цепочку групп, их последовательность и временные связи, а также сведения о субъектах и контексте действий. Результатом сопоставления является оценка соответствия цепочки элементам таксономии. Если оценка превышает установленное пороговое значение, то принимается решение о наличии признаков ККА. Результаты анализа сохраняются в хранилище данных.

Централизованное хранение данных в программном комплексе реализовано на основе NoSQL-СУБД «Apache Cassandra». В ней сохраняются исходные и нормализованные события, версии профилей действий пользователей и результаты работы аналитических каналов. Отдельно хранятся векторные представления, группы аномальных событий, цепочки групп, результаты сопоставления с таксономией КА и итоговые уведомления. Структура хранения выбрана с учётом запросов, используемых аналитическими модулями системы. Расчёты объёмов данных и обоснование выбранной структуры приведены в работе [16].

Для хранения векторных представлений, учёта связей между сущностями и формирования оповещений в программном комплексе также используются дополнительные компоненты. Информация об основных модулях системы приведена в табл. 1.

Таблица 1

Основные модули системы обнаружения ККА

Модуль	**Назначение и функции**
Модуль обработки событий (Event Processing Module)	Обеспечивает приём событий из различных источников и их приведение к единому внутреннему представлению. Выполняет проверку временной согласованности записей, контроль структуры и формирование набора атрибутов, используемых на последующих этапах анализа
Модуль формирования и поддержки профиля действий пользователя (ProfileManager)	Формирует и актуализирует профиль действий пользователя

Окончание табл. 1

Многоканальный детектор (MultiChannelDetector)	Выполняет выявление аномальных действий на уровне отдельных событий, формирует итоговую оценку аномальности события на основе частных оценок аналитических каналов
Модуль группировки аномалий (GroupingEngine)	Выполняет группировку взаимосвязанных аномальных событий и формирование цепочек групп аномальных событий с учётом временных, субъектных и контекстных связей.
Модуль сопоставления аномалий с таксономией компьютерных атак (TaxonomyMatcher)	Выполняет сопоставление сформированных цепочек групп аномальных событий с элементами таксономии КА.
Модуль хранения данных на основе NoSQL-СУБД «Apache Cassandra»	Обеспечивает хранение исходных событий, профилей действий пользователей, результатов аналитической обработки, групп аномальных событий, результатов сопоставления с таксономией КА и уведомлений

2. Описание работы системы при обнаружении комплексной компьютерной атаки

2.1. Описание ККА

Начальным этапом ККА стала целевая фишинговая рассылка. Сотрудник организации открыл вредоносное вложение с макросом для удалённого выполнения кода. На одном из узлов информационной инфраструктуры после этого были зафиксированы запуск «PowerShell», загрузка вспомогательного исполняемого файла и регистрация новой службы для закрепления вредоносного программного обеспечения. Сведения об этих действиях содержались в системных журналах и журналах файловых операций.

Для получения учётных данных из памяти процессов злоумышленник использовал «mimikatz». Полученные данные затем применялись при перемещении между узлами информационной инфраструктуры. Удалённый запуск процессов выполнялся с использованием «PsExec» и «WinRM». Также были зарегистрированы подключения по протоколам «RDP» и «SMB». В результате связанные с действиями злоумышленника события были зафиксированы на нескольких узлах информационной инфраструктуры.

В ходе ККА были зарегистрированы массовые обращения к файловым хранилищам и базам данных, а также использование средств архивирования. Собранные данные передавались на внешний IP-адрес по зашифрованным HTTPS-соединениям. Для сокрытия следов злоумышленник удалял временные файлы и очищал журналы. Отдельно были выявлены задания планировщика, предназначенные для повторного запуска вредоносного программного обеспечения после перезагрузки узла.

Во время проведения ККА присутствовала легитимная активность пользователей. Связанные с ККА события были распределены во времени и относились к различным узлам информационной инфраструктуры. При анализе учитывались не только отдельные аномальные события, но и временные и логические связи между ними. Продолжительность ККА составила около 100 часов. Скомпрометировано несколько узлов, объём собранных данных составил несколько десятков гигабайт. На рисунке 2 представлена схема рассматриваемой ККА.

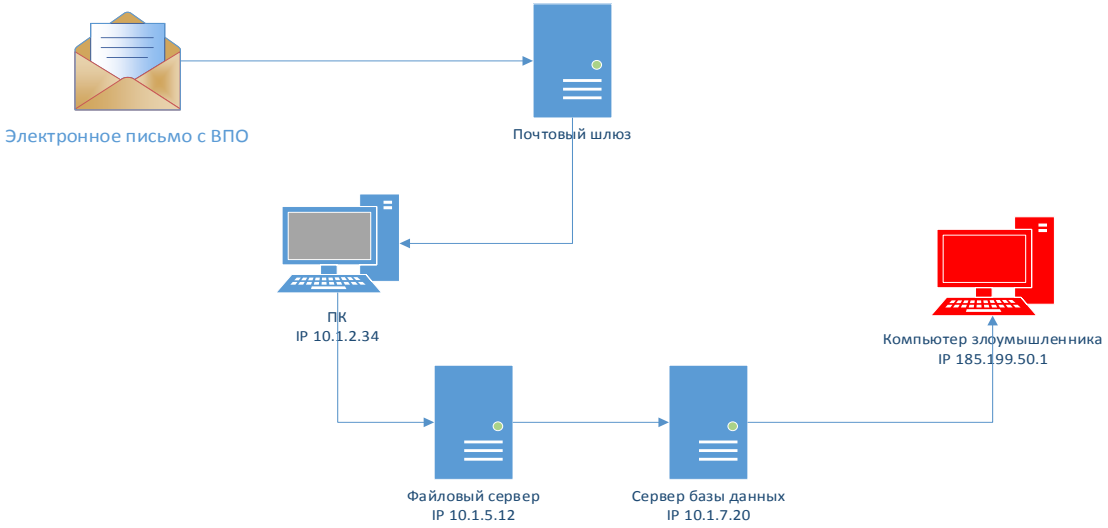

Рис. 2. Схематичное представление ККА

Следует отметить, что на момент реализации рассматриваемого сценария ККА не была обнаружена применявшимися средствами защиты. Отдельные зарегистрированные события не являлись однозначными признаками КА.

Используемые в ходе ККА инструменты, включая «PowerShell», средства удалённого администрирования и утилиты архивирования, применяются также в легитимной деятельности администраторов и пользователей. Поэтому сам факт их запуска не является однозначным признаком КА. Действия злоумышленника выполнялись в различное время и на нескольких узлах информационной инфраструктуры, а связанные с ними события регистрировались различными источниками данных. Ограничения применявшихся средств защиты и особенности их настройки могли затруднять установление связей между событиями. При раздельном анализе журналов полный сценарий ККА восстановить не удалось.

2.2. Описание работы системы при обработке комплексной компьютерной атаки

Для ретроспективной обработки использовались данные информационной инфраструктуры, подвергшейся ККА. Идентифицирующие сведения в исходных данных были анонимизированы. Набор включал журналы аутентификации

и активных процессов, системные журналы узлов сети, а также сетевой трафик. При подготовке данных состав событий и их временная последовательность не изменялись.

Для обучения и калибровки аналитических модулей использовались журналы, отражающие нормальные действия пользователей информационной инфраструктуры. Данные охватывали 31 день и включали около 300 уникальных учётных записей и 1,86 млн событий. На их основе были сформированы векторные представления событий и определены пороговые значения. После обучения система была проверена на тестовом наборе сценариев ККА. Полученные значения приведены в табл. 2.

Таблица 2

Результаты работы системы на тестовом наборе данных

Уровень оценки	**Показатель**	**Значение**
Событие	Precision	0,85
Событие	Recall	0,79
Событие	F1-мера	0,82
Группа	F1-мера	0,78
Цепочка	Доля восстановленных этапов ККА	0,74
Цепочка	Доля полностью восстановленных цепочек	0,68
Таксономия	Top-1 соответствие	0,71
Таксономия	Top-3 соответствие	0,84

Для оценки восстановления сценария использовались два показателя. Доля полностью восстановленных цепочек рассчитывалась как отношение числа тестовых сценариев, для которых были восстановлены все заданные этапы в эталонной последовательности, к общему числу тестовых сценариев. Top-1 равен доле случаев, в которых эталонный элемент получил наибольшую оценку соответствия. Top-3 равен доле случаев, в которых эталонный элемент вошёл в тройку элементов с наибольшими оценками.

В таблице 3 представлены ключевые события, используемые при анализе ККА. Отдельные записи сформированы путём сопоставления атрибутов событий, полученных из нескольких источников данных. Таблица не содержит полного набора событий, зарегистрированных в ходе ККА.

Таблица 3

Ключевые события

№	**Время (UTC)**	**Источник данных**	**Идентификатор записи / EventID**	**Тип события**	**Процесс / приложение**	**Пользователь**	**SrcIP / DstIP**
1	2025-11-08 18:47:22	Mail gateway / Endpoint agent	mail-003	AttachmentOpen	WINWORD.EXE	DOMAIN\employeeA	10.1.2.34 / —

Окончание табл. 3

2	2025-11-08 19:03:41	Endpoint agent	4688	ProcessStart	PowerShell.exe	DOMAIN\employeeA	10.1.2.34 / —
3	2025-11-08 19:04:10	Endpoint agent	4688	ProcessStart	payload.exe	DOMAIN\employeeA	10.1.2.34 / —
4	2025-11-08 19:05:00	Windows Event	7045	ServiceInstall	svc_persist	DOMAIN\employeeA	10.1.2.34 / —
5	2025-11-10 09:12:34	Endpoint agent	4688	ProcessStart	PowerShell.exe	DOMAIN\employeeA	10.1.2.34 / —
6	2025-11-10 11:05:12	Endpoint agent	4688	ProcessStart	mimikatz.exe	DOMAIN\employeeA	10.1.2.34 / —
7	2025-11-11 02:18:10	Endpoint agent / Network flow	4688	ProcessStart / RemoteConnection	PsExec.exe	DOMAIN\employeeA	10.1.2.34 / 10.1.5.12
8	2025-11-11 06:42:01	Endpoint agent	4688	ProcessStart	7z.exe	DOMAIN\dbsvc	10.1.7.20 / —
9	2025-11-11 07:58:12	Proxy / Network flow	nf-00160	NetworkConn	curl.exe	DOMAIN\dbsvc	10.1.7.20 / 185.199.50.1
10	2025-11-11 09:10:00	Endpoint agent	4688	ProcessStart	PowerShell.exe	DOMAIN\svc_admin	10.1.7.20 / —
11	2025-11-11 09:20:10	Windows Event	1102	AuditLogClear	wevtutil.exe	DOMAIN\svc_admin	10.1.7.20 / —
12	2025-11-12 23:01:18	Endpoint agent	4688	ProcessStart	schtasks.exe	DOMAIN\svc_admin	10.1.7.20 / —

После нормализации для событий начального этапа ККА (табл. 3, № 1–4) были сформированы признаковые представления, которые поступили в многоканальный детектор. Для событий запуска «PowerShell», исполняемого файла и регистрации службы были рассчитаны итоговые оценки аномальности. События, признанные аномальными, поступили в модуль группировки аномалий. Остальные могли использоваться при последующей актуализации профиля действий субъекта. Последовательность обработки событий показана на рис. 3.

	События № 1-4	События № 5-6	Событие № 7	События № 8-9	События № 10-12
Модуль обработки событий (Event Processing Module)	Приём событий, нормализация	Приём событий, нормализация	Приём событий, нормализация	Приём событий, нормализация	Приём событий, нормализация
Модуль формирования и поддержки профиля действий пользователя (ProfileManager)	Фиксация первичных отклонений, приостановка автообновления профиля	Подтверждение устойчивых отклонений, маркировка аномальной учётной записи	Регистрация активности на новом узле, обновление профиля действий	Выявление аномальной активности сервисной учётной записи	Регистрация действий, подготовка профиля к архивации
Многоканальный детектор (MultiChannelDetector)	Определение оценок отклонений нетипичных действий	Фиксация высокой ошибки реконструкции, агрегация оценок	Перерасчёт топологических метрик, фиксация новых рёбер, повышение вклада графового канала	Фиксация массового архивирования и внешних соединений	Фиксация очистки журналов аудита и персистентности
Модуль группировки аномалий (GroupingEngine)	Накопление первичных событий	Объединение событий № 1-6 в единый агрегат	Расширение существующего агрегата, перерасчёт веса	Пакетная обработка агрегата, пересчёт метрик достоверности; привязка сетевых потоков к агрегату	Присоединение событий № 10-12 к основному агрегату, добавление метаданных
Модуль сопоставления аномалий с таксономией компьютерных атак (TaxonomyMatcher)		Сопоставление с техниками	Добавление тактик	Сопоставление с техниками и тактиками	Итоговое сопоставление с техниками и тактиками
База данных на основе NoSQL «Apache Cassandra»	Сохранение необработанных данных и первичных оценок	Сохранение аномалий, обновление профиля, фиксация агрегата	Обновление графовых представлений, расширение агрегата	Сохранение записей и финальных оценок агрегата	Завершение записи агрегата инцидента, подготовка данных для уведомления

Рис. 3. Описание работы системы при обработке ККА

Для события запуска «mimikatz» (таблица 3, № 6) было сформировано признаковое представление, после чего многоканальный детектор рассчитал итоговую оценку аномальности. В статистическом канале ошибка реконструкции оказалась выше значений, характерных для событий нормальной активности. Эвристический канал сформировал частную оценку по заданным правилам, связанным с использованием средств извлечения учётных данных. Обе частные оценки были учтены при расчёте итогового значения.

При построении графа взаимодействий субъектов и ресурсов были учтены события удалённых подключений и запуска процессов на других узлах (табл. 3, № 7). Для связанных с ними вершин GCN сформировала векторные представления с учётом существующих связей. Полученная графовая оценка вошла в итоговую оценку аномальности события. При превышении порогового значения соответствующее событие было передано в модуль группировки аномалий.

В формируемую группу аномальных событий вошли события, связанные с массовыми обращениями к файловым ресурсам и запуском «7z.exe» (табл. 3, № 8). После пакетной обработки были уточнены состав группы и её связи с другими группами.

Сведения об исходящем HTTPS-соединении с внешним узлом (табл. 3, № 9) были рассмотрены совместно с ранее выявленными событиями архивирования. Позднее были зарегистрированы запуск «PowerShell» (табл. 3, №10), очистка журнала аудита (табл. 3, № 11) и запуск «schtasks.exe» (табл. 3, №12). Выявленные аномальные события были объединены в группы. С

учётом временной последовательности и связей между субъектами и ресурсами из сформированных групп была построена цепочка, характеризующая рассматриваемую ККА.

Для интерпретации выявленных этапов ККА выполнено сопоставление с тактиками и техниками базы знаний «MITRE ATT&CK» и техниками из «Методики оценки угроз безопасности информации ФСТЭК России» [18]. Результаты сопоставления представлены в табл. 4.

Таблица 4

Сопоставление этапов ККА с базой знаний «MITRE ATT&CK» и техниками «Методики оценки угроз безопасности информации ФСТЭК России»

Краткое описание этапа	**База знаний «MITRE ATT&CK»**	**Типовые техники «Методики оценки угроз безопасности информации ФСТЭК России»**
Целевой фишинг с вредоносным вложением и открытие файла пользователем	T1566.001 «Spearphishing Attachment», T1204.002 «User Execution: Malicious File»	Т2.8. «Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы»
Запуск «PowerShell» после открытия вредоносного вложения	T1059.001 «Command and Scripting Interpreter: PowerShell»	Т3.1. «Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии»
Регистрация службы «Windows» для закрепления в системе	T1543.003 «Create or Modify System Process: Windows Service»	Т3.14. «Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.»
Получение учётных данных из памяти с использованием «mimikatz»	T1003 «OS Credential Dumping»	Т6.1. «Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими»

Окончание табл. 4

Удалённый запуск процессов на других узлах с использованием «PsExec»	T1569.002 «System Services: Service Execution»	Т3.4. «Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами»
Получение доступа к другим узлам с использованием «WinRM», «RDP» и «SMB»	T1021.006 «Windows Remote Management», T1021.001 «Remote Desktop Protocol», T1021.002 «SMB/Windows Admin Shares»	Т8.2. «Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям»
Передача собранных данных во внешнюю сеть по «HTTPS»	T1048.002 «Exfiltration Over Asymmetric Encrypted Non-C2 Protocol»	Т9.3. «Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)»
Очистка журнала аудита «Windows»	T1685.005 «Disable or Modify Tools: Clear Windows Event Logs»	Т7.2. «Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей»
Создание задания планировщика для последующего запуска	T1053.005 «Scheduled Task/Job: Scheduled Task»	Т3.15. «Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур»

Результаты сопоставления показывают, что выявленные системой этапы ККА могут быть интерпретированы с использованием базы знаний «MITRE ATT&CK» и типовых техник «Методики оценки угроз безопасности информации ФСТЭК России». Сформированная последовательность взаимосвязанных групп аномальных событий отражает основные этапы рассматриваемого сценария ККА.

Разработанный программный комплекс сопоставлен с существующими решениями, такими как «Wazuh» [19], «Security Onion» [20], «Elastic Security» [21] и «Kaspersky Unified Monitoring and Analysis Platform» [22], по реализуемым функциям. Сопоставление не является количественным сравнением эффективности. Рассматриваемые решения обеспечивают мониторинг, сбор, корреляцию, анализ

событий и формирование оповещений. Разработанный комплекс реализует функции СОА. В разработанной системе анализируются отдельные события, взаимосвязанные группы аномальных событий и сформированные из них последовательности, относящиеся к возможным этапам ККА.

При ретроспективной обработке система выявила связанные аномальные события и сформировала из них группы аномальных событий. На основе групп была построена последовательность, которую система сопоставила с таксономией КА.

Заключение

В статье представлена реализация системы обнаружения комплексных компьютерных атак, основанной на анализе действий пользователей, сетевых взаимодействий и сопоставлении обнаруженных аномалий с таксономией КА. Программный комплекс построен по модульному принципу. Обработку событий, формирование профиля действий пользователя, многоканальное обнаружение аномалий, группировку аномальных событий и сопоставление с таксономией выполняют отдельные модули системы. Многоканальный детектор объединяет статистический, графовый и эвристический каналы. Для хранения данных используется NoSQL-СУБД «Apache Cassandra».

Экспериментальная проверка системы включала оценку на тестовом наборе сценариев ККА и отдельную ретроспективную обработку данных ККА. На тестовом наборе значения Precision, Recall и F1-меры при обнаружении аномальных событий составили 0,85, 0,79 и 0,82 соответственно. Средняя доля восстановленных этапов ККА составила 0,74, доля полностью восстановленных цепочек 0,68. При ретроспективной обработке система выявила взаимосвязанные аномальные события, сформировала цепочки групп и сопоставила их с таксономией КА. Проведённая апробация показала работоспособность системы при анализе взаимосвязанных событий, распределённых во времени.

Результаты обнаружения зависят от полноты и качества данных, использованных при обучении системы обнаружения ККА. Настройка параметров системы зависит от особенностей конкретной информационной инфраструктуры. Дальнейшие исследования связаны с расширением экспериментальных наборов данных, развитием графовых методов анализа и оценкой устойчивости системы при изменении характеристик регистрируемых действий пользователей.

Литература

1. CODE RED 2026: Актуальные киберугрозы для российских организаций - URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (дата обращения: 16.09.2026).

2. Приказ ФСБ России № 554 - URL: https://gossopka.ru/doc/npa/ normativnye-pravovye-akty-federalnykh-organov-ispolnitelnoy-vlasti/prikaz-fsb-rossii-ot-26-dekabrya-2025g-554-ob-ustanovlenii-trebovaniy-k-sredstvam-prednaznachennym-d-33266/ (дата обращения: 16.09.2026).

3. Котенко, И. В. Методы интеллектуального анализа системных событий для обнаружения многошаговых кибератак: использование методов машинного обучения / И. В. Котенко, Д. А. Левшун // Искусственный интеллект и принятие решений. – 2023. – № 3. – С. 3-15. – DOI 10.14357/ 20718594230301. – EDN SNNJFQ.

4. Котенко, И. В. Методы интеллектуального анализа системных событий для обнаружения многошаговых кибератак: использование баз знаний / И. В. Котенко, Д. А. Левшун // Искусственный интеллект и принятие решений. – 2023. – № 2. – С. 3-14. – DOI 10.14357/20718594230201. – EDN WOERTP.

5. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации / И. В. Котенко, И. Б. Саенко, Р. И. Захарченко, Д. В. Величко // Вопросы кибербезопасности. – 2023. – № 1(53). – С. 13-27. – DOI 10.21681/2311-3456-2023-1-13-27. – EDN WUUDFK.

6. Levshun D., Kotenko I. A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities // Artificial Intelligence Review. – 2023. – Vol. 56, No. 8. – P. 8547–8590. – DOI: 10.1007/s10462-022-10381-4.

7. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access. – 2022. – Vol. 10. – P. 43387–43420. – DOI: 10.1109/ACCESS.2022.3168976

8. Котенко И. В., Саенко И. Б., Лаута О. С., Крибель А. М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения // Информатика и автоматизация. – 2022. – Т. 21, № 6. – С. 1328–1358. – DOI: 10.15622/ia.21.6.9.

9. Левшун Д. А., Левшун Д. С., Котенко И. В. Обнаружение и объяснение аномалий в индустриальных системах Интернета вещей на основе автокодировщика // Онтология проектирования. – 2025. – Т. 15, № 1. – С. 96–113. – DOI: 10.18287/2223-9537-2025-15-1-96-113.

10. Sun Z., Teixeira A. M. H., Toor S. G. GNN-IDS: Graph neural network based intrusion detection system // Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024). – 2024. – Article No. 45. – DOI: 10.1145/3664476.3664515.

11. Ren W., Song X., Hong Y. et al. APT attack detection based on graph convolutional neural networks // International Journal of Computational Intelligence Systems. – 2023. – Vol. 16, No. 1. – Article 78. – DOI: 10.1007/s44196-023-00369-5.

12. Татарникова Т. М., Сикарев И. А. Обнаружение атак методом искусственных нейронных сетей // Проблемы информационной безопасности. Компьютерные системы. – 2023. – № 4. – С. 84–94. – DOI: 10.48612/jisp/u9zt-prru-97em.

13. Поздняк И. С., Макаров И. С. Использование алгоритмов машинного обучения для обнаружения аномального поведения трафика // Инфокоммуникационные технологии. – 2023. – Т. 21, № 3. – С. 20–27. – DOI: 10.18469/ ikt.2023.21.3.04.

14. Miloslavskaya, N. Survey of SIEM systems / N. Miloslavskaya, A. Tolstoy // Procedia Computer Science. – 2021. – Vol. 190. – P. 97–104.

15. 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.

16. Мельников, Д. Ю. Модель хранения данных в nosql-СУБД «Apache Cassandra» в задачах обнаружения комплексных компьютерных атак / Д. Ю. Мельников // Вестник УрФО. Безопасность в информационной сфере. – 2025. – № 3(57). – С. 30-39. – DOI 10.14529/secur250304. – EDN ASFKNG.

17. Мельников, Д. Ю. Система алгоритмов обнаружения комплексных компьютерных атак на основе анализа действий пользователей и сопоставления с базой знаний MITRE ATT&CK / Д. Ю. Мельников // Вестник УрФО. Безопасность в информационной сфере. – 2025. – № 4(58). – С. 44–52. – DOI 10.14529/secur250405. – EDN UUHFSA.

18. Методический документ ФСТЭК России от 05 февраля 2021 «Методика оценки угроз безопасности информации» [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 16.09.2026).

19. Wazuh Documentation [Электронный ресурс]. – URL: https:// documentation.wazuh.com (дата обращения: 16.09.2026).

20. Security Onion Documentation [Электронный ресурс]. – URL: https:// docs.securityonion.net (дата обращения: 16.09.2026).

21. Elastic Security Documentation [Электронный ресурс]. – URL: https:// www.elastic.co/security (дата обращения: 16.09.2026).

22. Kaspersky Unified Monitoring and Analysis Platform (KUMA) Documentation [Электронный ресурс]. – URL: https://support.kaspersky.com/kuma (дата обращения: 16.09.2026).

References

1. CODE RED 2026: Aktual'nye kiberugrozy dlja rossijskih organizacij - URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (accessed: 16.09.2026).

2. Prikaz FSB Rossii № 554 - URL: https://gossopka.ru/doc/npa/normativnye-pravovye-akty-federalnykh-organov-ispolnitelnoy-vlasti/prikaz-fsb-rossii-ot-26-dek-abrya-2025g-554-ob-ustanovlenii-trebovaniy-k-sredstvam-prednaznachennym-d-33266/ (accessed: 16.09.2026).

3. Kotenko, I. V. Metody intellektual'nogo analiza sistemnyh sobytij dlja obnaruzhenija mnogoshagovyh kiberatak: ispol'zovanie metodov mashinnogo obuchenija / I. V. Kotenko, D. A. Levshun // Iskusstvennyj intellekt i prinjatie reshenij. – 2023. – № 3. – S. 3-15. – DOI 10.14357/20718594230301. – EDN SNNJFQ.

4. Kotenko, I. V. Metody intellektual'nogo analiza sistemnyh sobytij dlja obnaruzhenija mnogoshagovyh kiberatak: ispol'zovanie baz znanij / I. V. Kotenko, D. A.

Levshun // Iskusstvennyj intellekt i prinjatie reshenij. – 2023. – № 2. – S. 3-14. – DOI 10.14357/20718594230201. – EDN WOERTP.

5. Podsistema preduprezhdenija komp'juternyh atak na ob#ekty kriticheskoj informacionnoj infrastruktury: analiz funkcionirovanija i realizacii / I. V. Kotenko, I. B. Saenko, R. I. Zaharchenko, D. V. Velichko // Voprosy kiberbezopasnosti. – 2023. – № 1(53). – S. 13-27. – DOI 10.21681/2311-3456-2023-1-13-27. – EDN WUUDFK.

6. Levshun D., Kotenko I. A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities // Artificial Intelligence Review. – 2023. – Vol. 56, No. 8. – P. 8547–8590. – DOI: 10.1007/s10462-022-10381-4.

7. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access. – 2022. – Vol. 10. – P. 43387–43420. – DOI: 10.1109/ACCESS.2022.3168976

8. Kotenko I. V., Saenko I. B., Lauta O. S., Kribel' A. M. Metodika obnaruzhenija anomalij i kiberatak na osnove integracii metodov fraktal'nogo analiza i mashinnogo obuchenija // Informatika i avtomatizacija. – 2022. – T. 21, № 6. – S. 1328–1358. – DOI: 10.15622/ia.21.6.9.

9. Levshun D. A., Levshun D. S., Kotenko I. V. Obnaruzhenie i ob#jasnenie anomalij v industrial'nyh sistemah Interneta veshhej na osnove avtokodirovshhika // Ontologija proektirovanija. – 2025. – T. 15, № 1. – S. 96–113. – DOI: 10.18287/2223-9537-2025-15-1-96-113.

10. Sun Z., Teixeira A. M. H., Toor S. G. GNN-IDS: Graph neural network based intrusion detection system // Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024). – 2024. – Article No. 45. – DOI: 10.1145/3664476.3664515.

11. Ren W., Song X., Hong Y. et al. APT attack detection based on graph convolutional neural networks // International Journal of Computational Intelligence Systems. – 2023. – Vol. 16, No. 1. – Article 78. – DOI: 10.1007/s44196-023-00369-5.

12. Tatarnikova T. M., Sikarev I. A. Obnaruzhenie atak metodom iskusstvennyh nejronnyh setej // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. – 2023. – № 4. – S. 84–94. – DOI: 10.48612/jisp/u9zt-prru-97em.

13. Pozdnjak I. S., Makarov I. S. Ispol'zovanie algoritmov mashinnogo obuchenija dlja obnaruzhenija anomal'nogo povedenija trafika // Infokommunikacionnye tehnologii. – 2023. – T. 21, № 3. – S. 20–27. – DOI: 10.18469/ikt.2023.21.3.04.

14. Miloslavskaya, N. Survey of SIEM systems / N. Miloslavskaya, A. Tolstoy // Procedia Computer Science. – 2021. – Vol. 190. – P. 97–104.

15. 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.

16. Mel'nikov, D. Ju. Model' hranenija dannyh v nosql-SUBD «Apache Cassandra» v zadachah obnaruzhenija kompleksnyh komp'juternyh atak / D. Ju. Mel'nikov // Vestnik

UrFO. Bezopasnost' v informacionnoj sfere. – 2025. – № 3(57). – S. 30-39. – DOI 10.14529/secur250304. – EDN ASFKNG.

17. Mel'nikov, D. Ju. Sistema algoritmov obnaruzhenija kompleksnyh komp'juternyh atak na osnove analiza dejstvij pol'zovatelej i sopostavlenija s bazoj znanij MITRE ATT&CK / D. Ju. Mel'nikov // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2025. – № 4(58). – S. 44-52. – DOI 10.14529/secur250405. – EDN UUHFSA.

18. Metodicheskij dokument FSTJeK Rossii ot 05 fevralja 2021 «Metodika ocenki ugroz bezopasnosti informacii» [Jelektronnyj resurs]. — Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (data obrashhenija: 16.09.2026).

19. Wazuh Documentation [Jelektronnyj resurs]. – URL: https://documentation.wazuh.com (accessed: 16.09.2026).

20. Security Onion Documentation [Jelektronnyj resurs]. – URL: https://docs.securityonion.net (accessed: 16.09.2026).

21. Elastic Security Documentation [Jelektronnyj resurs]. – URL: https://www.elastic.co/security (accessed: 16.09.2026).

22. Kaspersky Unified Monitoring and Analysis Platform (KUMA) Documentation [Jelektronnyj resurs]. – URL: https://support.kaspersky.com/kuma (accessed: 16.09.2026).

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

СИНАДСКИЙ Николай Игоревич, доктор технических наук, профессор, профессор учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий - РТФ Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002; г. Екатеринбург, ул. Мира, 19. E-mail: n.i.sinadsky@urfu.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

SINADSKY Nikolay, doctor of engineering, Professor, Educational and Scientific Center “Information Security”, Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Yekaterinburg, Mira str., 19. E-mail: n.i.sinadsky@urfu.ru