МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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, основанная на анализе действий пользователей, сетевых взаимодействий и сопоставлении обнаруженных аномалий с таксономией компьютерных атак. В системе реализованы модуль формирования и поддержки профиля действий пользователя и многоканальный детектор аномалий, основанный на статистическом и графовом анализе с использованием эвристических правил. Для анализа связанных проявлений активности используется механизм группировки событий, а их интерпретация выполняется модулем сопоставления с таксономией компьютерных атак. Анализ объединённых записей позволяет реконструировать наиболее вероятную последовательность техник злоумышленника. Подсистема хранения данных реализована на основе NoSQL-СУБД «Apache Cassandra». В статье приведён пример работы системы на анонимизированном наборе журналов реального инцидента. Результаты демонстрируют возможность реконструкции временно распределённых цепочек атак в условиях фоновой легитимной активности и неполноты данных.

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

The 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 the taxonomy of computer attacks. The system implements a module for forming and maintaining a user activity profile and a multi-channel anomaly detector based on statistical and graph analysis using heuristic rules. An event grouping mechanism is used to analyze related activity manifestations, and their interpretation is performed by a module that compares them with the taxonomy of computer attacks. Analysis of the combined records allows the most likely sequence of techniques used by the attacker to be reconstructed. The data storage subsystem is implemented based on the NoSQL DBMS «Apache Cassandra». The article provides an example of the system's operation on an anonymized set of logs from a real incident. The results demonstrate the possibility of reconstructing temporarily distributed attack chains in conditions of background legitimate activity and incomplete data.

Keywords: complex computer attacks, anomaly detection, user behavior 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 проявлениями. Приказ ФСБ России № 554 [2] устанавливает новые 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), корреляцию разнородных событий, а также повторный анализ ранее зарегистрированных событий с целью выявления ранее не обнаруженных компьютерных инцидентов.

Вопросам обнаружения компьютерных атак (далее – КА) и анализа событий информационной безопасности посвящены ряд исследований [3,4,5]. В работах [3,4] рассматриваются методы выявления многошаговых компьютерных атак, основанные на анализе системных событий и выявлении последовательностей взаимосвязанных действий злоумышленника. Предложены подходы к обнаружению многоэтапных атак, использующие методы машинного обучения и механизмы представления знаний для анализа событий безопасности и идентификации сценариев КА. Данные методы ориентированы на выявление взаимосвязанных событий и последовательности действий нарушителя в информационной системе. В работе [5] рассматриваются архитектурные и функциональные аспекты построения подсистем предупреждения компьютерных атак на объектах критической информационной инфраструктуры, основанных на сборе, корреляции и анализе событий информационной безопасности. Представленные исследования демонстрируют перспективность применения методов анализа событий и корреляционного анализа для выявления комплексных компьютерных атак (далее – ККА). Вместе с тем, задача обнаружения ККА, остаётся актуальной и требует дальнейшего развития методов анализа событий безопасности и построения СОА.

В предыдущих работах автора представлены основные элементы подхода к обнаружению ККА, основанного на анализе действий пользователей, сетевых взаимодействий и сопоставлении обнаруженных аномалий с таксономией компьютерных атак. В работе [6] представлена модель ККА, представляющая собой последовательность групп событий, соответствующих конкретной тактике из базы знаний «MITRE ATT&CK», также описана модель обнаружения ККА. Описан процесс построения профиля нормальных действий пользователей, а также его динамическое обновление. Обнаружение аномалий осуществляется с помощью метода машинного обучения – автокодировщика и графового анализа на основе графовой сверточной сети (GCN). Разработан и описан механизм корреляции аномалий в адаптивной временной области. В работе [7] предлагается модель представления данных в NoSQL-СУБД «Apache Cassandra» для системы обнаружения ККА и сформулированы шесть целевых требований к системе хранения данных. Выполнены расчеты объемов хранения и размеров логически связанных групп записей, объединённых общим ключом и размещаемых на отдельных узлах распределённого хранилища «Apache Cassandra». В работе [8] описана си-

стема, состоящая из четырех ключевых алгоритмов, обеспечивающих реализацию модели обнаружения ККА. Формализована внутренняя логика каждого алгоритма, описаны процедуры калибровки, а также критерии принятия решений.

Настоящая статья описывает реализованный программный комплекс и иллюстрирует его работу на анонимизированном наборе журналов реального инцидента. Целью исследования является демонстрация корректности проектных решений и подтверждение архитектурной согласованности системы при восстановлении последовательности действий злоумышленника.

В тексте подробно рассмотрены механизмы обмена данными между компонентами, включая сквозные идентификаторы, хранение векторных представлений событий, ведение версий профилей и фиксацию метаданных происхождения записей. Кроме того, показаны процедуры формирования и агрегирования частичных оценок аномальности по аналитическим каналам, пакетная проверка накопленных групп событий и их семантическая интерпретация с сопоставлением к таксономии компьютерных атак.

1. Архитектура и функциональные блоки программного комплекса

Система реализована как программный комплекс, обеспечивающий последовательную обработку журналов событий и данных мониторинга информационной инфраструктуры, начиная с приёма первичных записей и заканчивая формированием инцидентов и сохранением результатов анализа. Архитектура системы ориентирована не на выявление отдельных изолированных аномалий, а на обнаружение логически связанных действий злоумышленника в компонентах информационной инфраструктуры. Архитектура программного комплекса предусматривает централизованное хранение всех категорий данных в NoSQL‑СУБД «Apache Cassandra». В указанном хранилище консолидируются первичные записи журналов событий, версионные профили действия субъектов, векторные представления событий, агрегированные группы аномалий, а также итоговые инциденты информационной безопасности. Архитектура системы обнаружения комплексных компьютерных атак представлена на рис. 1.



Рис. 1. Архитектура системы обнаружения комплексных компьютерных атак

Модуль обработки событий (Event Processing Module) принимает исходные данные из различных источников: журналы аутентификации, системные журналы и сетевые потоки. Модуль приводит записи к унифицированному формату, синхронизирует временные метки и выполняет проверку структурной корректности записей и логической согласованности их атрибутов. После проверки к каждой записи добавляются метаданные, содержащие сведения о источнике данных и оценку его надёжности. Нормализованные записи сохраняются в основном хранилище и формируют исходную базу для последующего анализа.

Обработка данных осуществляется в двух режимах. В потоковом режиме реализуются операции с низкой латентностью: первичная нормализация, вычисление основных характеристик и оперативная оценка аномальности. В пакетном режиме выполняются более ресурсоёмкие задачи: повторная нормализация агрегатов, углублённый пересчёт статистических метрик и процедуры переобучения моделей. Такое разделение обеспечивает оперативность реакции на события и позволяет проводить детальный ретроспективный анализ гипотез.

Центральным компонентом является подсистема формирования и поддержки профиля действий пользователя (ProfileManager). Профиль представляет собой агрегированное представление типичного поведения субъекта в

системе. Изменения профиля фиксируются с сохранением истории обновлений. Каждое обновление сопровождается временной отметкой и перечнем наблюдений, послуживших основанием для внесённых изменений. Обновление базовой модели профиля осуществляется только после накопления достаточного числа подтверждающих наблюдений; единичные аномалии не интегрируются немедленно. Это снижает риск целенаправленного искажения профиля.

Локальное обнаружение реализовано через многоканальный детектор (MultiChannelDetector). Детектор объединяет три аналитических канала:

– эвристический канал реализует набор правил и индикаторов для оперативного выявления явных признаков компрометации;

– статистический канал оценивает отклонение текущих признаков от профиля действий. Автокодировщик обучается на наборе данных нормальных действий пользователей. Ошибка реконструкции преобразуется в эмпирический перцентиль относительно распределения ошибок на обучающей выборке и используется как частичная оценка аномальности;

– графовый канал анализирует локальную структуру взаимодействий, вычисляя локальные графовые метрики и формируя векторные представления узлов с помощью графовой сверточной сети (GCN). Полученные векторные представления отражают контекст взаимодействий и применяются для вычисления графовой оценки аномальности.

Каждый канал возвращает стандартизованную частичную оценку аномальности и сопроводительные метаданные. Частичные оценки объединяются агрегатором по настраиваемой политике с конфигурируемыми весами и порогами, что позволяет регулировать соотношение полноты и точности обнаружения без изменения внутренней логики отдельных каналов.

События, превышающие порог аномальности, направляются в модуль группировки аномалий (GroupingEngine). Его задачей является адаптивное объединение связанных по времени, субъектам, узлам или семантическому контексту записей в устойчивые группы. Механизм группировки предусматривает частичное несоответствие отдельных атрибутов и опирается на комбинированные меры сходства. Для каждой группы поддерживается состояние активности. Группа может продлеваться при поступлении подтверждающих сигналов и закрываться при длительной неактивности. Сформированные группы представляют собой промежуточные аналитические объекты и подлежат последующей пакетной проверке.

Для семантической интерпретации групп используется модуль сопоставления аномалий с таксономией компьютерных атак (TaxonomyMatcher). На первом этапе для каждого события формируются признаки (текстовые, структурные и контекстно-графовые) и измеряется степень сходства между этим представлением события и описаниями техник таксономии. Полученные сходства преобразуются в нормализованные оценки соответствия. На втором этапе оценки соответствия агрегируются по группе событий и применяются совместно с моделью вероятностей переходов между техниками для определения последовательности техник. В результате модуль возвращает упорядоченный список техник с оценками уверенности и комментариями.

В качестве базы данных используется распределённая NoSQL-СУБД «Apache Cassandra». В базе данных сохраняются первичные записи, версии профилей, векторные представления событий, записи взаимодействий, агрегаты групп и итоговые инциденты. Объединение записей по заданному критерию обеспечивает равномерное распределение нагрузки и масштабируемость системы. В работе [2] приведены расчёты объёмов хранения и рекомендации по выбору схем объединения записей.

Помимо основных аналитических модулей, комплекс включает вспомогательные компоненты, обеспечивающие хранение векторных представлений, учёт связей между сущностями и формирование оповещений, что гарантирует воспроизводимость расчётов и интеграцию результатов в процесс реагирования. Архитектура комплекса предусматривает фиксацию идентификаторов и ссылочных связей между результатами обработки на различных этапах, обеспечивая уникальное и воспроизводимое сопоставление результатов анализа. В табл. 1 представлены обобщённые сведения по ключевым модулям системы обнаружения ККА.

Таблица 1

Обобщённая информация по ключевым модулям системы ККА

Модуль	**Назначение и функции**
Модуль обработки событий (Event Processing Module)	Обеспечивает приём событий безопасности из различных источников и их приведение к единому внутреннему представлению. Выполняет проверку временной согласованности записей, контроль структуры и содержательной согласованности событий, а также формирование

	набора атрибутов, используемых на последующих этапах анализа
Модуль формирования и поддержки профиля действий пользователя (ProfileManager)	Поддерживает динамическое агрегированное представление действий пользователя
Многоканальный детектор (MultiChannelDetector)	Выполняет выявление аномальных отклонений на уровне отдельных событий с использованием нескольких аналитических каналов
Модуль группировки аномалий (GroupingEngine)	Объединяет связанные аномальные события в устойчивые группы, отражающие эпизоды подозрительной активности
Модуль сопоставления аномалий с таксономией компьютерных атак (TaxonomyMatcher)	Выполняет интерпретацию сгруппированных событий путём сопоставления наблюдаемых аномалий с таксономией компьютерных атак
База данных на основе NoSQL «Apache Cassandra»	Обеспечивает хранение исходных событий, состояний профилей действий пользователей, результатов аналитической обработки, групп событий и итоговых записей по инцидентам

2. Описание работы системы при обнаружении комплексной компьютерной атаки

2.1. Описание ККА

В рассматриваемом случае злоумышленник реализовал ККА. Начальный доступ был получен посредством целевого фишинга. Сотрудник организации открыл электронное сообщение с вредоносным вложением, в котором содержался макрос, обеспечивавший удалённое выполнение кода при открытии документа. В результате на одном из узлов сети инициировался запуск «PowerShell», был загружен и сохранён вспомогательный исполняемый файл, а для обеспечения устойчивости вредоносного компонента в системе была зарегистрирована новая служба. Эти действия отразились в системных журналах и в записях о файловых операциях.

На следующем этапе злоумышленник применил инструменты класса «mimikatz» для извлечения учётных данных из памяти процессов. Полученные учётные данные были использованы для латерального перемещения внутри корпоративной сети. Скомпрометированный узел инициировал удалённые подключения к другим узлам с помощью средств удалённого исполнения (включая PsExec и WinRM) и стандартных сервисов (RDP, SMB), что

обеспечило удалённый запуск процессов и перенос полезных нагрузок на целевые серверы.

Далее злоумышленник выполнял массовые операции чтения в файловых хранилищах и базах данных и применял утилиты архивирования для упаковки собранных данных. Для передачи подготовленных объёмов информации использовались кратковременные зашифрованные HTTPS-сессии, поток данных дробился на серию коротких соединений к внешнему адресу с целью маскировки активности. По завершении активной фазы были предприняты действия по сокрытию следов и обеспечению персистентности. Выполнялись операции удаления временных файлов, предпринимались попытки очистки журналов аудита и создавались задания в планировщике для возобновления работы вредоносного кода после перезагрузки узла.

Во время проведения ККА присутствовала легитимная активность пользователей, поэтому выявление атаки опиралось не на анализ отдельных записей, а на устранение повторяющихся наблюдений и установление логических связей между событиями. Продолжительность ККА составила около 96 часов. Скомпрометировано несколько узлов, объём собранных данных составил несколько десятков гигабайт. На рис. 2 представлено схема ККА.

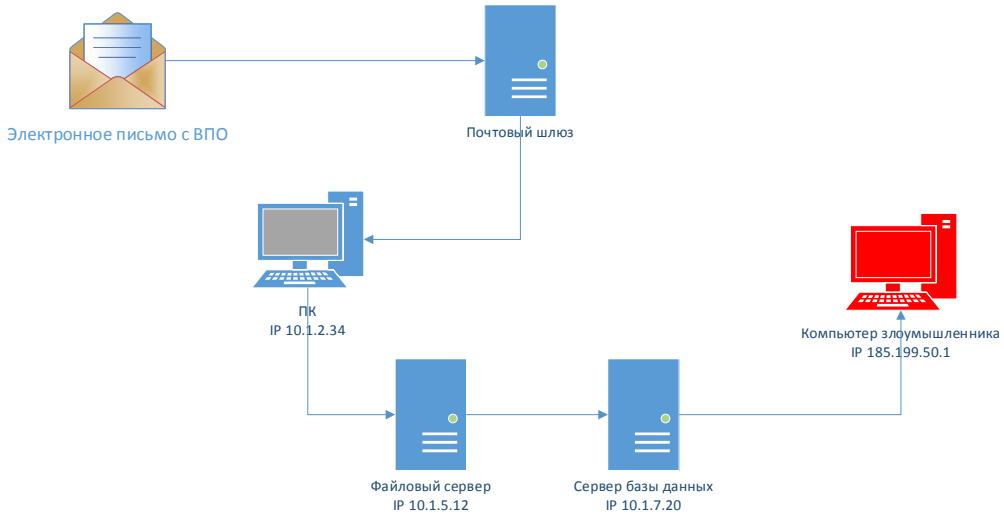


Рис. 2. Схематичное представление ККА

Следует отметить, что на момент реализации рассматриваемого сценария, КА не была обнаружена существующими средствами защиты. Это обусловлено тем, что отдельные действия злоумышленника по отдельности не формировали выраженных признаков КА. Используемые инструменты и процессы (например, «PowerShell», средства удалённого администрирования

и утилиты архивирования) применяются в легитимной деятельности администраторов и пользователей, вследствие чего их запуск не всегда интерпретируется как признак КА. Кроме того, действия злоумышленника были распределены во времени и выполнялись на различных узлах инфраструктуры, а соответствующие события фиксировались различными источниками данных. Ограниченные возможности используемых средств защиты информации, а также особенности их конфигурации могут дополнительно затруднять выявление взаимосвязанных последовательностей действий злоумышленника. В результате анализ отдельных журналов событий не позволял установить логические связи между наблюдаемыми событиями и представить полный сценарий ККА.

2.2. Описание работы системы при обработке комплексной компьютерной атаки.

В данном разделе демонстрируется функционирование программного комплекса при ретроспективной обработке журналов событий, в том числе инцидента информационной безопасности, экспортированных из информационной инфраструктуры предприятия. Все идентифицирующие сведения далее в тексте анонимизированы для сохранения конфиденциальности. Данные взяты из журналов аутентификации, системных журналов узлов сети, журналов активных процессов и сетевого трафика. Набор событий и их временная последовательность сохранены в полном объёме.

Аналитические модули системы обучались и калибровались на наборе журналов событий нормальных действий пользователей информационной инфраструктуры (31 день записи журналов событий, порядка 300 уникальных учётных записей, 1,86 млн. событий), что позволило построить векторные представления событий, выполнить калибровку порогов автокодировщика и настроить перцентильную нормализацию. В табл. 2 представлены ключевые анонимизированные события, используемые для демонстрации корреляции и анализа сценария атаки.

Таблица 2

Ключевые события

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

Окончание табл. 2

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	4688	ProcessStart	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	Audit-LogClear	wevtutil.exe	DO-MAIN\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 / —

Далее последовательно описаны этапы атаки и действия компонентов системы. Каждая стадия снабжена ссылкой на соответствующие записи в табл. 2.

Начальные проявления включали открытие целевого почтового вложения (табл. 2, № 1), после чего был зафиксирован нетипичный запуск интерпретатора сценариев на рабочей станции (табл. 2, № 2). Непосредственно после этого зарегистрирован запуск загруженного вспомогательного исполня-

емого файла (табл. 2, № 3) и запись о создании/регистрации службы, обеспечивающей устойчивость вредоносного компонента (табл. 2, № 4). После приёма и нормализации событий модуль приёма передал записи обработчику признаков, который сформировал векторные представления событий. Эвристический канал зарегистрировал нетипичную активность интерпретатора, статистический канал зафиксировал отклонение от профиля действий пользователя, а подсистема формирования и поддержки профиля аккумулировала подтверждающие наблюдения и приостановила автоматическое обновление базовой модели до поступления дополнительных подтверждений. На рис. 3 представлено схематичное описание работы системы при обработке ККА.

	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

Далее в журнале появились события, характерные для использования утилит извлечения учётных данных (табл. 2, № 6). Для соответствующих процессов были сформированы векторные представления. Автокодировщик зафиксировал повышенную ошибку реконструкции, эвристические правила дали высокую оценку по индикаторам компрометации, а подсистема профилей классифицировала учетную запись как потенциально скомпрометированную.

Скомпрометированные учётные данные использовались для удалённых подключений и запуска процессов на других узлах сети (табл. 2, № 7). Графовый модуль пересчитал локальные топологические признаки, сохранил

векторные представления узлов и зафиксировал сетевые взаимодействия. Повышение значений локальных графовых метрик инициирующего узла усилили вклад графового канала в суммарную оценку, после чего механизм группировки аккумулировал связанные события в агрегат для пакетной обработки.

На серверах были зарегистрированы массовые операции чтения и архивации данных, (табл. 2, № 8). По сформированному агрегату была выполнена пакетная обработка: повторная нормализация признаков, пересчёт метрик автокодировщика и уточнение векторных представлений, что привело к согласованию частичных оценок всех каналов и повышению достоверности агрегата.

Краткие зашифрованные исходящие соединения и операции по архивированию данных, позволили модулю корреляции привязать сетевые потоки к ранее сформированному агрегату (табл. 2, № 9). Перед операциями по очистке журналов зафиксирован запуск команд/скриптов удаления временных файлов (табл. 2, № 10), затем очистка журналов аудита (табл. 2, № 11) и создание задания планировщика (табл. 2, № 12). Эти события снабжены метаданными происхождения и связаны с сформированным уведомлением. Отдельные события с высокой эвристической оценкой подвергались ручной валидации в контексте совокупных доказательств для минимизации риска ложных срабатываний.

Для формализованного описания сценария ККА выполнено сопоставление выявленных этапов атаки с тактиками и техниками базы знаний «MITRE ATT&CK» и соответствующими тактикам из методики оценки угроз ФСТЭК России, представленное в табл. 3.

Таблица 3

Сопоставление этапов ККА с базой знаний «MITRE ATT&CK» и тактиками методики оценки угроз ФСТЭК России

Краткое описание этапа	База знаний «MITRE ATT&CK»	Тактики модели угроз ФСТЭК России
Целенаправленный фишинг с вложением	T1566.001 «Spearphishing Attachment»	Т2.8 «Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы»
Выполнение PowerShell-	T1059.001 «Command and Scripting	Т3.1 «Автоматический запуск скриптов и исполняемых файлов

скриптов/команд на рабочей станции	Interpreter: PowerShell»	(включая использование скриптов/интерпретаторов)»
Регистрация службы, создание задания планировщика	T1543.003 «Create or Modify System Process: Windows Service»; T1053.005 «Scheduled Task/Job»	Т3.14 «Планирование запуска вредоносных программ при старте системы (правка реестра и автозапуск, в том числе запуск как сервис)»; Т3.15 – «Планирование запуска через планировщик заданий»
Извлечение паролей/учётных данных из памяти	T1003 «OS Credential Dumping»	Т6.1 «Получение данных для аутентификации и авторизации –поиск в памяти процессов или перехват в трафике»
Удалённый запуск процессов/подключения к другим хостам (PsExec, RDP, SMB)	T1021 «Remote Services»	Т5.1 «Удалённое управление через стандартные протоколы; использование средств удалённого администрирования»
Чтение больших объёмов, архивация данных	T1074 «Data Staged»	Т7.17 «Обфускация, шифрование, упаковка (защита паролем) при подготовке данных/кода»
Передача данных за пределы сети через короткие шифрованные соединения	T1041 «Exfiltration Over C2 Channel»	Т9.5 / Т9.7 «Отправка данных по известным протоколам / маскировка каналов передачи, проксирование трафика для маскировки»
Очистка журналов, удаление временных файлов	T1070 «Clear Windows Event Logs»	Т7.2 «Очистка/затирание истории команд и журналов регистрации»

Представленные результаты в табл. 3 отражают последовательность взаимосвязанных событий, выявленных системой в процессе анализа данных, соответствующая сценарию ККА.

Таким образом, предложенная система обеспечивает выявление распределённой во времени последовательности взаимосвязанных действий злоумышленника, которые по отдельности не формируют выраженных признаков КА. Полученный результат демонстрирует возможность обнаружения

ранее не выявленных компьютерных атак на основе анализа совокупности событий ИБ, что соответствует нормативно-правовым требованиям, предъявляемым к СОА [2].

Заключение

В данной работе представлена система обнаружения ККА, основанная на анализе действий пользователей, сетевых взаимодействий и сопоставлении обнаруженных аномалий с таксономией компьютерных атак. Система включает механизм динамической профилизации с накоплением данных по времени и подтверждением внесённых изменений, многоканальный детектор с автокодировщиком и графовым анализом на основе GCN, а также модуль группировки аномалий, функционирующие на базе NoSQL-СУБД «Apache Cassandra».

Экспериментальная апробация системы выполнена на анонимизированном наборе журналов событий, включающем ретроспективный разбор ККА. Полученные результаты иллюстрируют способность предлагаемых механизмов аккумулировать различные признаки, формировать и агрегировать частичные оценки аномальности по аналитическим каналам и восстанавливать логически связанные последовательности техник злоумышленника при пакетной проверке накопленных групп событий. Совокупное применение модели и алгоритмов обнаружения ККА с хранилищем данных на основе NoSQL-СУБД «Apache Cassandra» обеспечивает возможность анализа событий, сопоставления разнородных данных и формирование уведомлений о ККА на основе совокупных признаков.

Вместе с тем, ограничением подхода является зависимость качества обнаружения от полноты и достоверности исходных журналов событий, а также необходимость операционной калибровки параметров моделей при внедрении в конкретную информационную инфраструктуру. Дальнейшие исследования связаны с расширением обучающих выборок, развитием графовых методов анализа и повышением устойчивости системы к изменению паттернов 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: – 27.02.2026).

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: – 27.02.2026).

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. 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.

7. 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.

8. 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.

References

1. CODE RED 2026: Aktual'nye kiberugrozy dlja rossijskih organizacij – URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (accessed: - 27.02.2026).

2. Prikaz FSB Rossii № 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/ (accessed: – 27.02.2026).

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.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 (US-BEREIT), Yekaterinburg, Russian Federation, 2025, pp. 221-224, doi: 10.1109/USBEREIT65494.2025.11054096.

6. 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.

7. 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.

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