

Д. С. Антропов¹✉

Метод классификации киберинцидентов с использованием контекстных признаков и анализа временных закономерностей

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: a.Danila2001@yandex.ru

Аннотация. В статье представлен метод классификации киберинцидентов, основанный на совместном использовании контекстных признаков и анализа временных закономерностей последовательности событий безопасности. Предложено формальное описание киберинцидента как временно упорядоченной последовательности событий, каждое из которых характеризуется атрибутивными, контекстными и временными признаками. Разработана трехкомпонентная модель признакового пространства, включающая технические, контекстные и временные характеристики инцидента. На основе данной модели сформулирована процедура интегральной оценки принадлежности инцидента к заданному классу с использованием взвешенной линейной комбинации частных оценок и порогового критерия уверенности. Метод представлен в виде системы функциональных модулей, взаимодействие которых описано формальными отображениями. Предложена UML-диаграмма деятельности, отражающая последовательность этапов обработки от поступления событий безопасности до формирования рекомендации по реагированию в интеллектуальной системе поддержки принятия решений. Приведены типовые сценарии классификации трех классов инцидентов с описанием характерных профилей признаков. Показано, что учет контекста и временной структуры инцидента позволяет разграничивать схожие по отдельным атрибутам инциденты, относящиеся к различным классам угроз. Метод ориентирован на интеграцию в интеллектуальные системы поддержки принятия решений в области информационной безопасности.

Ключевые слова: классификация киберинцидентов, контекстные признаки, временные закономерности, интеллектуальная система поддержки принятия решений, информационная безопасность, признаковое пространство

D. S. Antropov¹✉

Cyber incident classification method based on contextual features and temporal pattern analysis

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: a.Danila2001@yandex.ru

Abstract. The article presents a method for cyber incident classification based on the combined use of contextual features and temporal pattern analysis of security event sequences. A formal description of a cyber incident as a temporally ordered sequence of events is proposed, where each event is characterized by attributive, contextual, and temporal features. A three-component feature space model is developed, encompassing technical, contextual, and temporal characteristics of incidents. Based on this model, a procedure for integral membership assessment using a weighted linear combination of partial scores and a confidence threshold criterion is formulated. The method is represented as a system of functional modules with formally defined mappings. A UML activity diagram is proposed reflecting the processing pipeline from security event ingestion to recommendation generation within an intelligent decision support system. Typical classification scenarios for three incident classes -

credential brute force, account compromise, and unauthorized data exfiltration - are described with characteristic feature profiles. It is demonstrated that incorporating contextual and temporal structure enables discrimination between incidents sharing similar individual attributes but belonging to different threat classes. The method is intended for integration into intelligent decision support systems in the domain of information security.

Keywords: cyber incident classification, contextual features, temporal patterns, intelligent decision support system, information security, feature space

Введение

Рост масштабирования и уровня сложности корпоративных инфраструктур организаций сопровождается соразмерным увеличением числа и разнообразных киберинцидентов. SIEM-платформы, средства обнаружения вторжений, агенты конечных устройств генерируют значительные потоки событий, ручная обработка которых не позволяет обеспечить своевременное и корректное реагирование [1–3]. В этих условиях возникает потребность в методах интеллектуальной поддержки принятия решений, способных автоматизировать классификацию инцидентов и формировать обоснованные рекомендации по реагированию.

Традиционные подходы к классификации инцидентов опираются преимущественно на сигнатурный анализ и методы обнаружения вторжений по заранее заданным признакам, однако такие подходы не всегда учитывают контекст возникновения событий и динамику развития инцидента [4, 5]. Вместе с тем практика показывает, что одно и то же техническое событие, например, неуспешная попытка аутентификации, может являться элементом как атаки подбора учетных данных, так и штатной ошибки авторизованного пользователя [6]. Корректный анализ инцидента определяется как атрибутами отдельного события, так и совокупностью контекстных факторов:

- критичностью защищаемого актива
- ролью и типичным профилем поведения пользователя
- принадлежностью узла к сегменту сети
- временной структурой развития атакующего сценария [6, 7].

Исследования в области интеллектуальной поддержки принятия решений в информационной безопасности подчеркивают значимость комплексного анализа признаков пространства [8–11]. В работах [12–15] показано, что учет временных закономерностей, последовательностей событий, журналов безопасности и сетевых потоков повышает точность разграничения классов инцидентов, имеющих схожие технические атрибуты. Однако большинство предложенных решений либо ограничиваются одной группой признаков, либо не формализуют процедуру классификации в терминах, пригодных для интеграции в интеллектуальные системы поддержки принятия решений (СППР).

Актуальность настоящего исследования обусловлена необходимостью разработки метода, обеспечивающего классификацию киберинцидентов на основе одновременного использования технических, контекстных и временных признаков и формализации его структуры в виде, допускающем интеграцию в интеллектуальные системы поддержки принятия решений области информационной безопасности.

Целью исследования является разработка и описание метода классификации киберинцидентов, интегрирующего контекстные признаки и анализ временных закономерностей последовательности событий.

Предлагаемое решение

Под киберинцидентом понимается не одиночное событие, а упорядоченная во времени совокупность взаимосвязанных событий безопасности, отражающих развитие деструктивного или потенциально опасного сценария воздействия на информационную систему. Пусть множество событий безопасности определено как $E = \{e_1, e_2, \dots, e_n\}$. Каждое событие e_i представляется кортежем:

$$e_i = [a_i, c_i, t_i], \quad (1)$$

где a_i - атрибутивные технические признаки события; c_i - контекстные признаки; t_i - временные характеристики. Тогда киберинцидент I определяется как временно упорядоченная последовательность:

$$I = [e_1, e_2, \dots, e_n], t_1 < t_2 < \dots < t_n \quad (2)$$

Задача классификации состоит в построении отображения $\Phi: I \rightarrow K$, где $K = \{k_1, k_2, \dots, k_6\}$ - заданное множество классов киберинцидентов. Выделяется 6 классов:

- 1) k_1 - подбор учетных данных;
- 2) k_2 - компрометация учетной записи;
- 3) k_3 - повышение привилегий;
- 4) k_4 - несанкционированный доступ к ресурсу;
- 5) k_5 - эксфильтрация данных;
- 6) k_6 - действия внутреннего нарушителя.

Выделение указанных классов согласуется с тактиками и техниками атак, представленными в MITRE ATT&CK и с подходами к обработке компьютерных инцидентов, указанных в руководстве NIST SP 800-61 Rev. 2 [16, 17].

Признаковое пространство инцидента строится как объединение трех компонент. Такие практики соответствует общему подходу к комплексному анализу событий безопасности и построению систем защиты информации [18].

Первая выделяемая компонента - технические признаки $X_S(I)$. В ней выделяются компоненты такие, как:

- 1) тип события и источник;
- 2) адреса и порты узлов-участников;
- 3) используемый протокол;
- 4) код результата операции;
- 5) тип учетной записи;
- 6) вид задействованного ресурса.

Вторая компонента - контекстные признаки $X_C(I)$. В ней классифицируются:

- 1) уровень критичности актива;
- 2) принадлежность узла к сегменту сети;
- 3) роль и уровень привилегий пользователя;
- 4) тип временного интервала (рабочее/нерабочее время);
- 5) статус доверенности устройства;
- 6) степень отклонения от нормального поведенческого профиля пользователя.

Третья компонента - временные признаки $X_T(I)$. Данный тип содержит такие метрики, как:

- 1) средний, минимальный и максимальный интервалы между событиями;
- 2) частота событий (f) на заданном временном окне;
- 3) показатель плотности событий ρ ;
- 4) длина цепочки l .

Итоговый вектор признаков инцидента формируется как:

$$X(I) = [X_S(I), X_C(I), X_T(I)] \quad (3)$$

Для обеспечения сопоставимости признаков каждая компонента переводится в безразмерную шкалу $[0; 1]$. Для числовых признаков используется линейная нормализация:

$$x^* = \frac{(x - x_{min})}{(x_{max} - x_{min})},$$

где x_{min} и x_{max} определяются по обучающей или размеченной выборке. Тогда частные оценки по группам признаков могут быть заданы в виде взвешенных сумм:

$$F_S(X_S(I), k_j) = \sum_{r=1}^p w_r^{(j)} * x_r, \quad (4)$$

$$F_C(X_C(I), k_j) = \sum_{q=1}^u w_q^{(j)} * c_q, \quad (5)$$

$$F_T(X_T(I), k_j) = \sum_{h=1}^z w_h^{(j)} * t_h, \quad (6)$$

где x_r – нормированные технические признаки инцидента,

c_q – нормированные контекстные признаки,

t_h – нормированные временные признаки,

$w_r^{(j)}, w_q^{(j)}, w_h^{(j)}$ – весовые коэффициенты признаков для класса k_j ,

p, u, z – количество технических, контекстных и временных признаков соответственно.

Для каждого класса $k_j \in K$ вычисляются три частные оценки принадлежности инцидента:

$$S_S^{(j)} = F_S(X_S(I), k_j), S_C^{(j)} = F_C(X_C(I), k_j), S_T^{(j)} = F_T(X_T(I), k_j),$$

где F_s, F_c, F_T – функции оценки по техническим, контекстным и временным признакам соответственно.

Интегральная оценка принадлежности инцидента к классу k_j определяется взвешенной линейной комбинацией:

$$S^{(j)} = \alpha * S_s^{(j)} + \beta * S_c^{(j)} + \gamma * S_T^{(j)}, \alpha + \beta + \gamma = 1, \alpha, \beta, \gamma \in [0, 1] \quad (8)$$

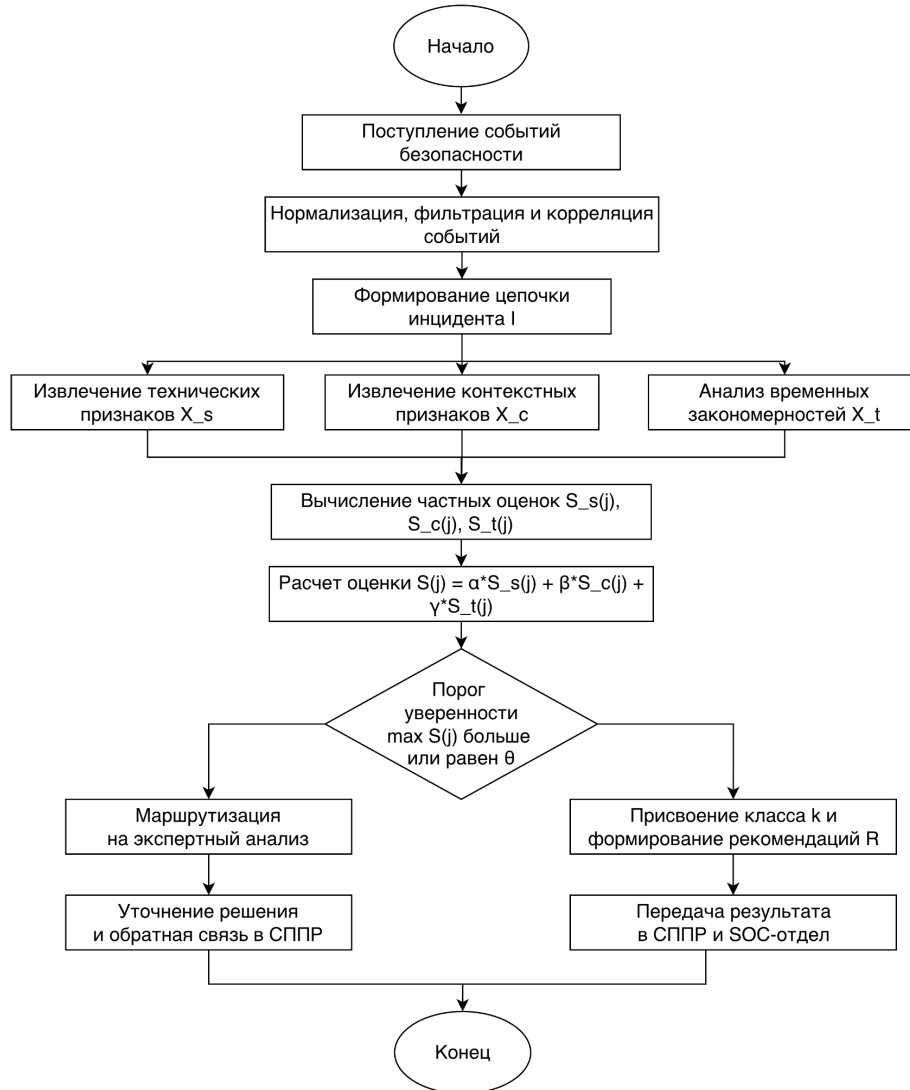


Рис. 1. Блок-схема метода классификации киберинцидентов

Класс инцидента выбирается по критерию максимума с пороговым условием уверенности:

$$\hat{k} = \arg \max S^{(j)}, \text{если } S^{(j)} \geq \theta, \text{ иначе } \hat{k} - \text{неопределенное событие.} \quad (9)$$

Введенный порог θ обеспечивает передачу инцидентов с недостаточной уверенностью на экспертный анализ, что будет повышать надежность функционирования СППР в условиях неполноты данных.

Последовательность обработки изображена на блок-схеме (рис. 1), где иллюстрируются этапы, начиная с поступления сырых событий безопасности через предобработку, извлечение признаков, расчет оценок и проверку порога уверенности, заканчивая формированием рекомендаций и передачи результата аналитику. При результате анализа ниже порогового значения инцидент направляется в SOC-отдел для дальнейшего исследования и принятия решения по противодействию.

Результаты

В результате проведенного исследования разработан метод классификации киберинцидентов, описывающий инцидент как временно упорядоченную последовательность событий с трехкомпонентным вектором признаков. Метод проверяется на типовых сценариях и сопоставляется с более простыми подходами, использующими только сигнатурные или только технические признаки.

Сигнатурный подход выявляет уже известные шаблоны атак. Подход, основанный лишь на технических признаках, повышает охват, но сохраняет неоднозначность при анализе цепочек с похожими начальными событиями. Предлагаемый метод нивелирует эту проблему за счет совместного учета критичности актива, поведенческого профиля, частоты срабатывания событий и структуры временных переходов между фазами инцидента.

Табл. 1 содержит сводную характеристику профилей признаков для рассмотренных сценариев.

Предложенный метод отличается от традиционных сигнатурных подходов тем, что классифицирует инцидент по структуре его развития в контексте возникновения в виде совокупности различных факторов. Введение контекстных признаков позволяет разграничивать инциденты. Например, неуспешные попытки аутентификации в рабочее время со стороны пользователя с историей аналогичных ошибок получают значительно меньшую оценку принадлежности к определенному классу, чем аналогичные события в нерабочее время с нетипичного ip-адреса.

Включение временных признаков обеспечивает разграничение инцидентов, демонстрирующих схожую начальную фазу, но существенно различающихся по динамике. Нормированное расстояние до эталонного временного профиля класса позволяет формализовать это различие в виде непрерывной оценки, допускающей градацию степени уверенности.

Таблица 1. Профили признаков для типовых сценариев классификации

Сценарий	Технические признаки	Контекстные признаки	Временные признаки
Подбор учетных данных (k_1)	Ошибки аутентификации, единый источник	Нетипичное время, отклонение профиля	Малый Δt , высокая f , большой l
Компрометация учетной записи (k_2)	Серия ошибок и успешный вход	Высокая критичность актива, резкое отклонение профиля	Перелом структуры цепочки, изменение Δt_{avg}
Эксфильтрация данных (k_5)	Операции чтения и передача, нестандартный порт	Максимальная критичность, нетипичный ресурс	Высокая плотность ρ , аномальное время завершения

Заключение

В работе разработан метод классификации киберинцидентов, основанный на совместном использовании технических, контекстных и временных признаков последовательности событий безопасности. Предложена формальная постановка задачи классификации как построения отображения из временно упорядоченной последовательности событий в заданное множество классов угроз. Сформулирована трехкомпонентная модель признакового пространства; введены нормализация признаков и интерпретируемые функции частных оценок. Также разработана процедура интегральной оценки с весовыми коэффициентами и пороговым критерием уверенности. Метод представлен в виде блок-схемы с описанием формул, используемых в нем

Метод ориентирован на интеграцию в интеллектуальные СППР в области информационной безопасности и может служить основой для дальнейшей работы на реальных событиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Интеллектуальная поддержка при принятии технических решений в информационной инфраструктуре предприятия // Защита информации. Инсайд. – 2020. – № 4. – С. 68–73.
2. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия // Защита информации. Инсайд. – 2021. – № 5 (101). – С. 16–25.
3. Liao H.-J. et al. Intrusion Detection System: A Comprehensive Review // Journal of Network and Computer Applications. – 2013. – Т. 36. – № 1. – С. 16–24.
4. Denning D. E. An Intrusion-Detection Model // IEEE Transactions on Software Engineering. – 1987. – Т. SE-13. – № 2. – С. 222–232.
5. Patcha A., Park J.-M. An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends // Computer Networks. – 2007. – Т. 51. – № 12. – С. 3448–3470.
6. Басыня Е. А., Худяков Д. С. Комплексный мониторинг информационной инфраструктуры предприятия // Защита информации. Инсайд. – 2020. – № 6. – С. 28–33.

7. Zakirova A. B. et al. Intelligent Support in Making Technical Decisions in the Enterprise Information Infrastructure // Journal of Theoretical and Applied Information Technology. – 2021. – Т. 99. – № 13. – С. 3144–3154.
8. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // 2010 IEEE Symposium on Security and Privacy. – IEEE, 2010. – С. 305–316.
9. Mirsky Y. et al. KITSUNE: An Ensemble of Autoencoders for Online Network Intrusion Detection // Network and Distributed System Security Symposium (NDSS). – 2018.
10. Buczak A. L., Guven E. A. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2016. – Т. 18. – № 2. – С. 1153–1176.
11. Shenfield A., Day D., Ayesh A. Intelligent Intrusion Detection Systems Using Artificial Neural Networks // ICT Express. – 2018. – Т. 4. – № 2. – С. 95–99.
12. Hu W. et al. AdaBoost-Based Algorithm for Network Intrusion Detection // IEEE Transactions on Systems, Man, and Cybernetics. – 2008. – Т. 38. – № 2. – С. 577–583.
13. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. – 2009. – Т. 41. – № 3. – С. 1–58.
14. Chen J. et al. Log2vec: A Heterogeneous Graph Embedding-Based Approach for Detecting Cyber Threats within Enterprise // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. – 2019. – С. 1777–1794.
15. Zhang J. et al. Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data // IEEE Access. – 2019. – Т. 7. – С. 37004–37016.
16. MITRE ATT&CK Framework [Электронный ресурс] // MITRE. URL: <https://attack.mitre.org> (дата обращения: 10.04.2025).
17. NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide [Электронный ресурс] // National Institute of Standards and Technology. URL: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final> (дата обращения: 10.04.2025).
18. Шелупанов А. А., Бабун Т. В. Методы и средства защиты информации. – Томск : ТУСУР-Пресс, 2017. – 228 с.

© Д. С. Антропов, 2026