Научная статья
УДК 004.89; DOI: 10.61260/2218-13X-2026-1-159-169

ФОРМАЛЬНАЯ МОДЕЛЬ КОМПЬЮТЕРНЫХ АТАК, ОСНОВАННАЯ НА ЗАПИСЯХ СИСТЕМНЫХ СОБЫТИЙ ОПЕРАЦИОННОЙ СИСТЕМЫ

✉**Павлычев Алексей Викторович.**
Дальневосточный федеральный университет, Владивосток, Россия
✉***pavlychev.av@dvfu.ru***

Аннотация. Современные компьютерные атаки отличаются сложностью выявления, комбинированием различных техник и активным использованием злоумышленниками новых технологий, что требует разработки интеллектуальных подходов к их обнаружению.

Целью данной работы является создание формальной модели, позволяющей выявлять признаки компьютерных атак на основе анализа системных событий операционной системы. В рамках практического применения разработанной модели получен размеченный датасет. Для выявления компьютерных атак применены различные алгоритмы машинного обучения. Сравнительный анализ показал, что наилучший результат демонстрирует алгоритм «случайный лес» (Random Forest). Точность разработанного классификатора составила 99,65 %.

Полученные результаты подтверждают высокую эффективность использования формальной модели в практической деятельности по выявлению компьютерных атак.

Ключевые слова: формальная модель, обнаружение кибератак, машинное обучение, классификация, анализ системных событий, Event ID, случайный лес, киберугрозы

Для цитирования: Павлычев А.В. Формальная модель компьютерных атак, основанная на записях системных событий операционной системы // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 1. С. 159–169. DOI: 10.61260/2218-13X-2026-1-159-169

Scientific article

FORMAL MODEL OF COMPUTER ATTACKS, BASED ON SYSTEM EVENT RECORDS OF THE OPERATING SYSTEM

✉**Pavlychev Aleksey V.**
Far Eastern Federal University, Vladivostok, Russia
✉***pavlychev.av@dvfu.ru***

Abstract. Modern computer attacks are characterized by the complexity of detection, the combination of various techniques and the active use of new technologies by attackers, which requires the development of intelligent approaches to their detection.

The purpose of this work is to create a formal model that makes it possible to identify signs of computer attacks based on the analysis of operating system system events. As part of the practical application of the developed method, a marked-up dataset was obtained. Various machine learning algorithms have been used to detect computer attacks. A comparative analysis showed that the «Random Forest» algorithm demonstrates the best result. The accuracy of the developed classifier was 99,65 %.

The results obtained confirm the high efficiency of using the formal model in practical activities for detecting computer attacks.

Keywords: formal model, cyber attack detection, machine learning, classification, system event analysis, Event ID, random forest, cyber threats

For citation: Pavlychev A.V. Formal model of computer attacks, based on system event records of the operating system // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2026. № 1. P. 159–169. DOI: 10.61260/2218-13X-2026-1-159-169

Введение

С развитием технологий расширились возможности доступа к информации, однако одновременно возросла и сложность обеспечения информационной безопасности. Повсеместное внедрение информационных систем во все сферы жизни привело к расширению спектра кибератак.

Современные компьютерные атаки представляют собой сложные и многоаспектные угрозы, которые сочетают в себе различные объекты воздействия и инструменты для достижения своих целей [1]. Они могут быть направлены на нарушение конфиденциальности, целостности или доступности данных, а также использовать как технические уязвимости, так и методы социальной инженерии [2]. Атаки часто включают в себя несколько этапов, таких как разведка, внедрение, эксплуатация и сокрытие следов, что делает их сложными для обнаружения и предотвращения [3].

Кроме того, злоумышленники активно применяют современные технологии, включая искусственный интеллект и машинное обучение [4], для автоматизации атак и повышения их эффективности. От специалистов по кибербезопасности требуется использование комплексных подходов, включающих не только традиционные методы защиты, но и передовые технологии анализа данных [5, 6], мониторинга и прогнозирования угроз.

Для успешного противодействия современным компьютерным атакам необходимо постоянно совершенствовать методы обнаружения и нейтрализации, а также учитывать их многообразие и сложность.

Целью настоящей работы является разработка формальной модели компьютерных атак на основе анализа событий операционной системы, предназначенной для выявления компьютерных атак.

Составление формальной модели компьютерных атак

В российской и зарубежной научной литературе встречаются различные подходы к составлению формальных моделей компьютерных атак.

Так, в работе [7] в основу модели положено определение степени опасности, для чего рассматриваются особенности их воздействия, характер проявления на элементах телекоммуникационной сети, таких как канал связи, маршрутизатор, коммутатор, автоматизированное рабочее место, сервер. Степень опасности задана матрицей вероятности воздействия, элементы которой получены с применений частных методик.

Для моделирования и выявления компьютерных атак авторы работы [8] используют различные системные и сетевые атрибуты, такие как процент использования процессора за последнюю секунду, доступная оперативная память для процессов, процент используемой оперативной памяти, количество операций чтения дискового ввода-вывода, количество отправленных и полученных байтов, общее количество ошибок при получении и отправки пакетов и др. (всего 39 атрибутов).

Авторы работы [9] для построения модели обнаружения компьютерных атак также используют сетевые события: сетевой адрес и порт, протокол передачи данных, число переданных пакетов, количество потерянных пакетов и др.

Иной подход сформулирован в работе [10]. Авторы при составлении формальной модели вводят такие атрибуты как степень удаленности потенциального атакующего, сложность эксплуатации, требуемый уровень привилегий (прав), необходимый для проведения атаки, оценка степени влияния атаки на конфиденциальность, целостность и доступность информации.

Авторы работы [11] предложили модель функционирования информационной системы в киберпространстве в виде сложной иерархической структуры с описанием динамических процессов, учитывающей одноуровневые и разноуровневые функциональные отношения между элементами в соответствии с моделью OSI. Разработанная модель многовариантного состояния позволяет любое состояние при функционировании информационной системы описать с достаточной для практики точностью, представив его конечным множеством параметров – индикатором состояния. Данный подход применим для выявления деструктивных действий в информационной системе, в том числе компьютерных атак.

События операционной системы как основа для построения формальной модели компьютерных атак описываются в работе [12]. Для выявления аномалий используются поиск стандартного отклонения в таких атрибутах как время события, количество событий, тип, категория, источник.

Поиск признаков конкретных видов атак с помощью анализа системных событий операционной системы и построения формальной модели подробно описан в работе [13].

Журналы событий – это файлы определенного формата, в которые записываются все события, происходящие в системе. В эти файлы записываются события получения доступа, создания, изменения или удаления файлов, изменения системных параметров, таких как, например, дата и время, изменения конфигураций системы и др. В них записываются миллионы событий, которые попадают в различные журналы.

Рассмотрим журналы системных событий на примере операционой системы Windows:

1. Журнал безопасности (Security). Любые события, имеющие значение для безопасности системы, записываются именно в этот журнал, например, удаление файлов, вход в систему, выход из системы и другие события.

2. Журнал системы (System). В журнале системы регистрируются события, зарегистрированные операционной системой, такие как ошибки или сбои при запуске жесткого диска.

3. Журнал приложений (Application). В данный журнал записываются события, определенные разработчиками того или иного программного обеспечения. Например, ошибки при запуске приложений.

В работе [14] авторами предлагается использование записей системных событий операционной системы для выявления вредоносного программного обеспечения. Данных подход можно адаптировать для выявления компьютерных атак.

Рассмотрим множество U – множество всех возможных наблюдаемых действий в системе:

$$U = \{A_1, \dots, A_k, L_1, \dots, L_m\},$$
$$n = k + m,$$

где A – множество действий злоумышленников; L – множество легитимных действий пользователей; n – количество всех возможных действий; k – количество всех возможных действий злоумышленников (компьютерные атаки); m – количество всех возможных действий легитимных пользователей.

Пусть множество $Sec = \{Sec_1, \dots, Sec_p\}$ – множество булевых функций, где p – количество всех возможных событий, отображаемых в журнале Security.

Каждый элемент множества Sec имеет следующий смысл: функция Sec_i имеет значение 1 тогда и только тогда, когда за время выполнения действия происходило i-е событие из множества Sec, множества всех возможных событий журнала Security.

Пусть множество $Sys = \{Sys_1, \dots, Sys_t\}$ – множество булевых функций, где t – количество всех возможных событий, отображаемых в журнале System.

Каждый элемент множества Sys имеет следующий смысл: функция Sys_i имеет значение 1 тогда и только тогда, когда за время выполнения действия происходило i-е событие из множества Sys, множества всех возможных событий журнала System.

Пусть множество $App = \{App_1, \dots, App_s\}$ – множество булевых функций, где s – количество всех возможных событий, отображаемых в журнале Application.

Каждый элемент множества App имеет следующий смысл: функция App_i имеет значение 1 тогда и только тогда, когда за время выполнения действия происходило i-е событие из множества App, множества всех возможных событий журнала Application.

Автор определяет любой элемент множества U (множества всех возможных действий) как набор следующих векторов.

Каждый элемент U_i из множества U имеет вид:

$$\mathrm{U_i} = \left\{ \begin{bmatrix} Sec_{1,i} \\ \dots \\ Sec_{p,i} \end{bmatrix}, \begin{bmatrix} Sys_{1,i} \\ \dots \\ Sys_{t,i} \end{bmatrix}, \begin{bmatrix} App_{1,i} \\ \dots \\ App_{s,i} \end{bmatrix} \right\}, i = \overline{1,n}.$$

Пусть $\varphi(U_i)\colon U_i \to \{0,1\}$ – функционал, обозначающий выполнение действия U_i и приводящий либо к безопасному состоянию системы (значение 0), либо к небезопасному состоянию (значение 1).

В силу стохастической природы событий и пересечения сигнатур атак с легитимной активностью необходимо дополнительное введение порога классификации θ: пусть $P(\phi(U_i) = 1)$ – это число, рейтинг угрозы от 0 до 1. Тогда правило классификации примет следующий вид: если $P(\phi(U_i) = 1) \geq \theta$, то действие считается атакой; если $P(\phi(U_i) = 1) < \theta$, то действие считается легитимным.

Определена область вероятностей компьютерной атаки как $V = \{U_i\colon U_i \in U, P(\varphi(U_i) = 1) \geq \theta\}$.

Исходя из вышеперечисленного, существуют множества L (множество всех легитимных действий) и множество A (множество всех компьютерных атак): $L = \{L_1, \dots, L_k\}$ и $A = \{A_1, \dots, A_m\}$.

Элемент $U_i \in U$ является элементом множества A тогда и только тогда, когда $U_i \in V$.

Элемент $U_i \in U$ является элементом множества L тогда и только тогда, когда $U_i \notin V$.

Предложенный подход позволяет представить рассматриваемый объект (действие) в виде набора признаков, соответствующих наступлению определенного события, которое фиксируется в журналах Security, System и Application.

Использование формальной модели для обнаружения компьютерных атак

Для применения формальной модели использовался датасет, полученный в рамках использования алгоритма формирование размеченного набора данных на основе смоделированных компьютерных атак [15]. Применено преобразование полученных данных о записях системных событий операционной системы в наборы признаков объекта (действия).

Каждый признак имеет числовое значение, соответствующее количеству зафиксированных Event ID в ходе реализации сценария атаки или пользовательской активности, а также 0 в случае, если запись о наступлении данного события отсутствует.

Набор для обучения моделей формируется следующим образом: в качестве столбцов используются уникальные идентификаторы событий Event ID, в качестве строк – наборы значений признаков исследуемых объектов (уникальные сессии, соответствующие проводимым сценарием, поле fields.session).

Также необходимо преобразовать название категорий и субкатегорий в числовые значения. Преобразование осуществляется по следующим правилам.

Поле fields.category переводится в целевую переменную target, которая имеет значение 1, соответствующее «ATTACK», и 0, соответствующее «USER_ACTION».

Из fields.sub_category формируется поле sub_category_encoded в соответствии со словарем: {'ACCOUNT_MANIPULATION_(T1098)': 0, 'CREDENTIAL_BRUTEFORCE_(T1110)': 1, 'BITS_JOBS_(T1197)': 2, 'SYSTEM_BINARY_PROXY_EXECUTION_(T1218)': 3, 'OFFICE': 4, 'WEB': 5, 'MAIL': 6, 'FTP': 7}.

Общий вид обработанного датасета приведен на рис. 1.

На следующем этапе для решения задачи по обнаружению признаков компьютерных атак необходима разработка классификатора, который с учетом значений набора признаков объекта сможет отнести исследуемые события к одной из двух категорий: компьютерная атака или легитимное действие пользователя.

	fields.session	0	1	6	12	14	15	16	18	20	...	16384	16394	16962	16977	16983	50036	50103	51046	sub_category_encoded	target
0	20250412144135	1	4	18	2	2	0	2	2	4	...	2	2	2	2	2	2	2	2	5	0
1	20250412144551	0	3	19	2	2	0	2	2	4	...	0	1	2	2	2	2	2	2	4	0
2	20250412145345	1	4	17	2	2	0	2	2	4	...	2	2	2	2	2	2	2	2	5	0
3	20250412145802	0	3	17	2	2	0	2	2	4	...	0	1	2	2	2	2	2	2	4	0
4	20250412150131	2	4	17	2	2	0	2	2	4	...	2	3	2	2	2	2	2	2	5	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
9995	20250428232302	1	3	9	1	1	0	1	1	2	...	3	0	1	1	1	0	0	1	5	0
9996	20250519131652	0	1	8	1	1	0	1	1	2	...	0	1	1	0	1	1	0	1	0	1
9997	20250518004124	0	2	0	0	1	0	2	1	0	...	0	1	1	0	3	1	1	1	2	1
9998	20250405154854	0	3	8	2	1	2	2	1	2	...	1	1	1	1	1	0	2	0	3	1
9999	20250331135527	0	1	10	3	0	0	1	1	2	...	2	1	1	1	2	1	1	0	0	1

10000 rows × 123 columns

Рис. 1. **Наборы признаков в преобразованном датасете**

Ввиду значительного объема признаков в рассматриваемом датасете и сложности его ручной обработки необходимо применение автоматизированных методов обработки данных. Для решения данной задачи целесообразно использование методов машинного обучения.

В машинном обучении задача классификации представляет собой задачу по разделению множества объектов на группы, называемые классами, на основе анализа их формального описания.

К числу распространенных методов решения задачи классификации [16] относятся:

1. Линейные классификаторы:

– LogisticRegression – логистическая регрессия (для бинарной и многоклассовой классификации);

2. Методы опорных векторов (SVM):

– Support Vector Classification (SVC) – метод опорных векторов для классификации;

3. Деревья и ансамбли деревьев:

– DecisionTreeClassifier – дерево решений;

– RandomForestClassifier – случайный лес (ансамбль деревьев);

– GradientBoostingClassifier – градиентный бустинг;

4. Байесовские методы:

– GaussianNB – наивный Байесовский классификатор для нормально распределённых признаков;

5. Методы ближайших соседей:

– KNeighborsClassifier (KNN) – k-ближайших соседей.

6. Нейронные сети:

– MLPClassifier (MLP) – многослойный перцептрон (простая нейросеть);

7. Дискриминантный анализ:

– LinearDiscriminantAnalysis (LDA) – линейный дискриминантный анализ.

Для решения задач классификации необходимо ввести метрики, по которым будут оцениваться полученные модели.

В рамках настоящего исследования для оценки качества полученных моделей используется F-мера, которая гармонично учитывает как ложноположительные, так и ложноотрицательные значения классификатора, что имеет важное значение в рамках решения задачи по обнаружению признаков компьютерных атак [17].

Дополнительно для оценки качества моделей может использоваться кросс-валидация – это метод оценки обобщающей способности модели, при котором исходная выборка данных разбивается на несколько частей, а обучение и тестирование проводится многократно на разных подмножествах.

Кросс-валидация используется для оценки устойчивости модели – проверки, насколько хорошо алгоритм работает на разных подвыборках. Использование данного метода снижает зависимость от «неудачного» разбиения выборки, при котором классы в обучающей и тестовой выборке не сбалансированы.

Обучение классификаторов и оценка результатов

В качестве инструмента для обучения моделей машинного обучения в рамках настоящего исследования использовался язык программирования Python и библиотека для анализа данных Scikit-learn.

Для обучения классификаторов создан словарь с параметрами по умолчанию. Оценка качества классификации проведена отдельно для тренировочной и тестовой выборки. Дополнительно для F-меры, как основной метрики, проведена кросс-валидация, чтобы получить максимально достоверный результат.

Результаты обучения классификаторов приведены на рисю 2, 3.

Model	Train Accuracy	Test Accuracy	Train Precision	Test Precision	Train Recall	Test Recall	Train F1	Test F1
Random Forest	1.0000	0.9965	1.0000	0.9965	1.0000	0.9965	1.0000	0.9965
Gradient Boosting	0.9990	0.9960	0.9990	0.9960	0.9990	0.9960	0.9990	0.9960
MLP	0.9995	0.9950	0.9995	0.9950	0.9995	0.9950	0.9995	0.9950
Decision Tree	1.0000	0.9935	1.0000	0.9935	1.0000	0.9935	1.0000	0.9935
Logistic Regression	0.9975	0.9925	0.9975	0.9925	0.9975	0.9925	0.9975	0.9925
LDA	0.9940	0.9900	0.9940	0.9900	0.9940	0.9900	0.9940	0.9900
KNN	0.9945	0.9880	0.9945	0.9881	0.9945	0.9880	0.9945	0.9880
SVC	0.9710	0.9680	0.9712	0.9682	0.9710	0.9680	0.9710	0.9680
Gaussian NB	0.9260	0.9195	0.9288	0.9217	0.9260	0.9195	0.9260	0.9193

Рис. 2. **Результаты обучения классификаторов**

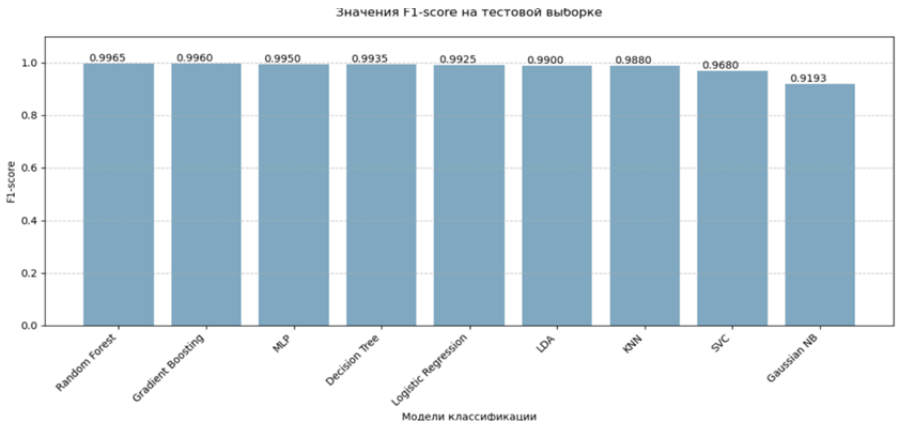

Рис. 3. **Результаты обучения классификаторов**

Как видно из представленных графиков, лучшие результаты из рассмотренных алгоритмов на заданном наборе данных показал алгоритм классификации «случайный лес» (Random Forest).

Интерпретация результатов и программная реализация

Для оценки результатов работы модели составлена и проанализирована матрица ошибок, приведенная на рис. 4.

Всего рассматривалось 2 000 объектов. Как видно из указанной матрицы, классификатор верно отнес к классу 1 (компьютерные атаки) 1 026 объектов, к классу 0 (легитимные действия пользователей) – 968 объектов. Классификатор ошибочно отнес к классу компьютерных атак четыре легитимных действия пользователей, а также две кибератаки классифицировал как легитимное действие.

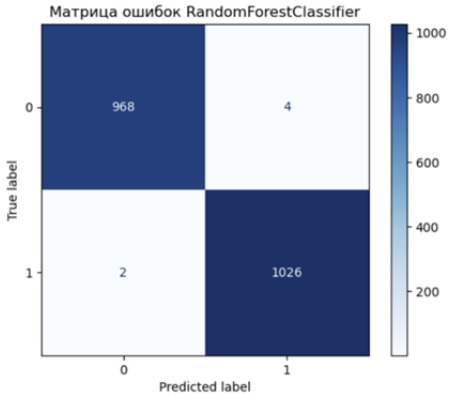

Рис. 4. **Матрица ошибок для разработанной модели**

Важным свойством алгоритма классификации является вычисление весов признаков [18], благодаря которым происходит дальнейшее отнесение объектов к тому или иному классу.

В рамках исследования признаки соответствуют идентификаторам событий операционной системы, что имеет важное значение для аналитиков в области информационной безопасности, поскольку каждое событие документировано и позволяет выявлять дополнительные характерные поведенческие признаки, присущие компьютерной атаке в ходе ее реализации.

Десять самых важных с точки зрения классификатора признаков, полученных в рамках исследования, приведены на рис. 5, 6.

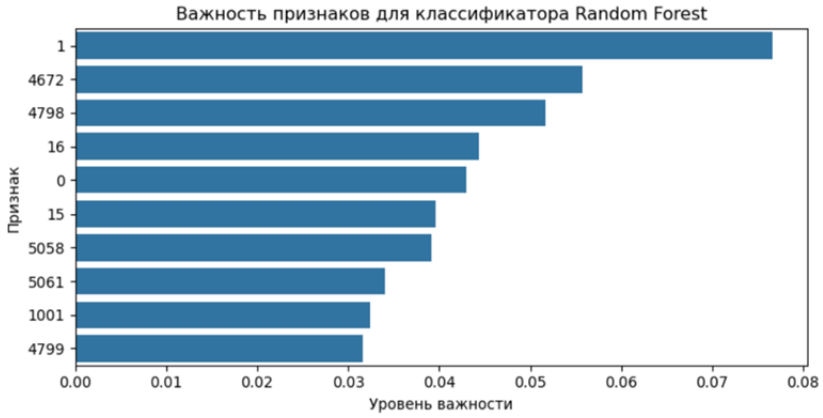

Рис. 5. **Важность признаков при классификации**

Feature	1	4672	4798	16	0	15	5058	5061	1001	4799
Importance	0.076633	0.055712	0.051627	0.044346	0.042954	0.03964	0.039084	0.034054	0.032464	0.031585

Рис. 6. **Важность признаков при классификации**

Итог работы классификатора составил 99,65 %, что является высоким результатам, который можно использовать в практической деятельности по выявлению признаков компьютерных атак. Разработанный на базе классификатора программный продукт прошел апробацию специалистами центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и используется в качестве одного из инструментов при расследовании компьютерных инцидентов. Получена справка о внедрении.

Заключение

В рамках настоящей работы предложен подход к составлению формальной модели компьютерных атак с помощью системных событий операционной системы.

Подготовлен датасет, включающий наборы признаков действий, соответствующих идентификаторам событий операционной системы. В качестве целевого признака введен тип действия: компьютерная атака или легитимная работа пользователя.

К полученному датасету последовательно применены алгоритмы машинного обучения: деревья решений, К-ближайших соседей, наивный Байесовский классификатор, опорных векторов, случайный лес, линейный дискриминантный анализ, многослойный перцептрон, логистическая регрессия.

Проведен сравнительный анализ полученных классификаторов согласно установленным метрикам и интерпретация полученных результатов. Итоговый результат работы классификатора составил 99,65 %.

Высокая точность обнаружения атак позволяет использовать предложенную формальную модель в рамках практической деятельности по выявлению кибератак.

Список источников

1. Mallick M.A.I., Nath R. Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments // World Scientific News. 2024. Т. 190. № 1. P. 1–69. URL: https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf (дата обращения: 07.02.2026).

2. Грибачёв А.С., Кальщиков В.В., Ручай А.Н. Методы, алгоритмы и базы данных обнаружения компьютерных инцидентов. // Вестник УрФО. Безопасность в информационной сфере. 2024. Т. 1. № 51. С. 45–52. DOI: DOI: 10.14529/secur240106.

3. A detailed analysis of benchmark datasets for network intrusion detection system / M. Ghurab [et al.] // Asian Journal of Research in Computer Science. 2021. V. 7. № 4. P. 14–33. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834787 (дата обращения: 08.02.2026).

4. Enhancing network security via machine learning: opportunities and challenges / M. Amrollahi [et al.] // Handbook of big data privacy. 2020. P. 165–189. DOI: 10.1007/978-3-030-38557-6_8

5. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3 (55). С. 90–100. DOI:10.21681/2311-3456-2023-3-90-100

6. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4 (56). С. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93

7. Коцыняк М.А., Лаута О.С., Иванов Д.А. Математическая модель таргетированной компьютерной атаки // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 73–81. DOI: 10.24411/2409-5419-2018-10261

8. Имитационное моделирование многозначных компьютерных атак / О.И. Шелухин [и др.] // I-methods. 2023. Т. 15. № 4. С. 6.

9. Шабуров А.С., Никитин А.С. Модель обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2019. № 29. С. 104–117.

10. Структурно-функциональная модель имитации компьютерных атак на автоматизированные системы / В.А. Минаев [и др.] // Вестник Российского нового университета. Сер.: Сложные системы: модели, анализ и управление. 2020. № 1. С. 3–16.

11. Захарченко Р.И., Королев И.Д. Модель функционирования автоматизированной информационной системы в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 69–78.

12. Dwyer J., Truta T.M. Finding anomalies in windows event logs using standard deviation // 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. IEEE, 2013. P. 563–570.

13. Smiliotopoulos C., Barmpatsalou K., Kambourakis G. Revisiting the detection of lateral movement through Sysmon // Applied Sciences. 2022. Т. 12. №. 15. P. 7746.

14. Павлычев А.В., Стародубов М.И., Галимов А.Д. Модель функционирования вредоносного программного обеспечения на основе анализа системных журналов операционной системы Microsoft Windows // Прикаспийский журнал: управление и высокие технологии. 2022. Т. 66. № 4. С. 24–31.

15. Формирование размеченного набора данных на основе смоделированных компьютерных атак / А.В. Павлычев [и др.] // Безопасность информационных технологий. 2025. Т. 32. № 4. С. 1–18. DOI: 10.26583/bit.2025.4.01

16. A review of classification problems and algorithms in renewable energy applications / M. Pérez-Ortiz [et al.] // Energies. 2016. Т. 9. № 8. P. 607. DOI: 10.3390/en9080607

17. Naidu G., Zuva T., Sibanda E.M. A review of evaluation metrics in machine learning algorithms // Computer science on-line conference. Cham: Springer International Publishing. 2023. P. 15–25. DOI: 10.1007/978-3-031-35314-7_2

18. Ayua S.I. Random forest ensemble machine learning model for early detection and prediction of weight category // Journal of Data Science and Intelligent Systems. 2024. Т. 2. № 4. P. 233–240. DOI: 10.47852/bonviewJDSIS32021149

References

1. Mallick M.A.I., Nath R. Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments // World Scientific News. 2024. Т. 190. № 1. P. 1–69. URL: https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf (data obrashcheniya: 07.02.2026).

2. Gribachyov A.S., Kal'shchikov V.V., Ruchaj A.N. Metody, algoritmy i bazy dannyh obnaruzheniya komp'yuternyh incidentov. // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2024. Т. 1. № 51. S. 45–52. DOI: DOI: 10.14529/secur240106.

3. A detailed analysis of benchmark datasets for network intrusion detection system / M. Ghurab [et al.] // Asian Journal of Research in Computer Science. 2021. V. 7. № 4. P. 14–33. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834787 (data obrashcheniya: 08.02.2026).

4. Enhancing network security via machine learning: opportunities and challenges / M. Amrollahi [et al.] // Handbook of big data privacy. 2020. P. 165–189. DOI: 10.1007/978-3-030-38557-6_8

5. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 1. Predposylki i skhema // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 90–100. DOI:10.21681/2311-3456-2023-3-90-100

6. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 2. Algoritm, model' i eksperiment // Voprosy kiberbezopasnosti. 2023. № 4 (56). S. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93

7. Kocynyak M.A., Lauta O.S., Ivanov D.A. Matematicheskaya model' targetirovannoj komp'yuternoj ataki // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2019. T. 11. № 2. S. 73–81. DOI: 10.24411/2409-5419-2018-10261

8. Imitacionnoe modelirovanie mnogoznachnyh komp'yuternyh atak / O.I. Sheluhin [i dr.] // I-methods. 2023. T. 15. № 4. S. 6.

9. Shaburov A.S., Nikitin A.S. Model' obnaruzheniya komp'yuternyh atak na ob"ekty kriticheskoj informacionnoj infrastruktury // Vestnik Permskogo nacional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya. 2019. № 29. S. 104–117.

10. Strukturno-funkcional'naya model' imitacii komp'yuternyh atak na avtomatizirovannye sistemy / V.A. Minaev [i dr.] // Vestnik Rossijskogo novogo universiteta. Ser.: Slozhnye sistemy: modeli, analiz i upravlenie. 2020. № 1. S. 3–16.

11. Zaharchenko R.I., Korolev I.D. Model' funkcionirovaniya avtomatizirovannoj informacionnoj sistemy v kiberprostranstve // Voprosy kiberbezopasnosti. 2019. № 6 (34). S. 69–78.

12. Dwyer J., Truta T.M. Finding anomalies in windows event logs using standard deviation // 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. IEEE, 2013. P. 563–570.

13. Smiliotopoulos C., Barmpatsalou K., Kambourakis G. Revisiting the detection of lateral movement through Sysmon // Applied Sciences. 2022. T. 12. №. 15. P. 7746.

14. Pavlychev A.V., Starodubov M.I., Galimov A.D. Model' funkcionirovaniya vredonosnogo programmnogo obespecheniya na osnove analiza sistemnyh zhurnalov operacionnoj sistemy Microsoft Windows // Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. 2022. T. 66. № 4. S. 24–31.

15. Formirovanie razmechennogo nabora dannyh na osnove smodelirovannyh komp'yuternyh atak / A.V. Pavlychev [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2025. T. 32. № 4. S. 1–18. DOI: 10.26583/bit.2025.4.01

16. A review of classification problems and algorithms in renewable energy applications / M. Pérez-Ortiz [et al.] // Energies. 2016. T. 9. № 8. P. 607. DOI: 10.3390/en9080607

17. Naidu G., Zuva T., Sibanda E.M. A review of evaluation metrics in machine learning algorithms // Computer science on-line conference. Cham: Springer International Publishing. 2023. P. 15–25. DOI: 10.1007/978-3-031-35314-7_2

18. Ayua S.I. Random forest ensemble machine learning model for early detection and prediction of weight category // Journal of Data Science and Intelligent Systems. 2024. T. 2. № 4. P. 233–240. DOI: 10.47852/bonviewJDSIS32021149

Информация о статье:
Статья поступила в редакцию: 13.02.2026; одобрена после рецензирования: 06.03.2026;
принята к публикации: 10.03.2026

Information about the article:
The article was submitted to the editorial office: 13.02.2026; approved after review: 06.03.2026;
accepted for publication: 10.03.2026

Информация об авторах:
Павлычев Алексей Викторович, директор центра информационной безопасности, доцент департамента информационной безопасности института математики и компьютерных технологий Дальневосточный федеральный университет (690922, г. Владивосток, о. Русский, п. Аякс, д. 10), e-mail: pavlychev.av@dvfu.ru, SPIN-код: 9934-0684

Information about authors:
Pavlychev Aleksey V., director of the information security center, associate professor of the information security department at the institute of mathematics and computer technology of Far Eastern Federal University (690922, Vladivostok, Ajax Bay, 10), e-mail: pavlychev.av@dvfu.ru, SPIN: 9934-0684