Кольченко Александр Альбертович, студент
Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Kolchenko Alexander Albertovich

АЛГОРИТМ ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ СЕТИ ИНФОРМАЦИОННЫХ СИСТЕМ
ALGORITHM FOR DETECTING UNAUTHORIZED ACTIONS OF INFORMATION SYSTEM NETWORK ADMINISTRATORS

Аннотация. В статье рассматривается алгоритм выявления несанкционированных действий администраторов сети корпоративных информационных систем на основе многопараметрического мониторинга с применением системы Zabbix. Предложена модель индикаторов безопасности с весовыми коэффициентами и интегральным показателем подозрительности.

Abstract. The article describes an algorithm for detecting unauthorized actions of corporate information system network administrators using multi-parameter monitoring with Zabbix. A security indicator model with weighted coefficients and an integral suspicion index is proposed.

Ключевые слова: Информационная безопасность, администратор сети, мониторинг, несанкционированные действия, Zabbix, индикаторы безопасности.

Keywords: Information security, network administrator, monitoring, unauthorized actions, Zabbix, security indicators.

В современных корпоративных информационных системах (ИС) сетевые администраторы обладают широкими техническими полномочиями: им доступны все ресурсы системы, они знают об используемых средствах защиты и могут скрывать следы своей деятельности. Это делает угрозу со стороны привилегированных пользователей одной из наиболее сложно обнаруживаемых. Традиционные средства защиты, ориентированные на внешние угрозы, не обеспечивают эффективного контроля за действиями легитимных привилегированных пользователей. Специализированные коммерческие решения (SIEM, UEBA) требуют значительных затрат на внедрение и эксплуатацию, что ограничивает их применение.

Настоящая работа посвящена разработке алгоритма выявления несанкционированных действий администраторов сети на базе системы мониторинга Zabbix, которая обладает открытой лицензией, поддерживает сбор логов, пользовательские скрипты и развитый API для интеграции.

Формальная постановка задачи. Информационная система описывается множеством наблюдаемых событий $E = \{e_1, e_2, \ldots, e_n\}$, где каждое событие $e_i = (h, p, v, t)$ характеризуется узлом h, контролируемым параметром p, его значением v и временем регистрации t. На основе E формируется множество индикаторов безопасности $S = \{s_1, s_2, \ldots, s_n\}$, принимающих бинарные значения: $s_j = 1$ при выявлении признака подозрительной активности, $s_j = 0$ в противном случае.

Алгоритм выявления несанкционированных действий реализуется в режиме реального времени и включает следующие шаги.

Шаг 1. Непрерывный сбор данных мониторинга. С помощью агентов Zabbix, протоколов SNMP и пользовательских скриптов с интервалом 30 секунд собираются: состояние служб безопасности; контрольные суммы конфигурационных файлов; размер файлов журналов аудита; объём сетевого трафика; количество входов суперпользователя; количество учётных записей в системе.

Шаг 2. Вычисление индикаторов безопасности. Для каждого собранного параметра проверяется условие аномалии. Определены шесть классов индикаторов, охватывающих типовые сценарии несанкционированных действий администратора (таблица 1).

Таблица 1

Индикаторы безопасности и их весовые коэффициенты

№	Индикатор	Обозначение	Вес (w_iн)	Условие срабатывания
1	Отключение службы аудита/безопасности	s_sec	0,225	Служба auditd остановлена
2	Изменение конфигурации защиты	s_conf	0,2	Изменение MD5-хеша файла конфигурации
3	Очистка журналов аудита	s_log	0,2	Уменьшение размера файла журнала
4	Аномальный сетевой трафик	s_net	0,15	Превышение среднего трафика более чем на 3σ
5	Аномальное число входов суперпользователя	s_auth	0,125	Более 5 входов root за 30 секунд
6	Добавление новых пользователей	s_user	0,1	Увеличение числа записей в /etc/passwd

Шаг 3. Расчёт интегрального показателя подозрительности. Для дифференцированной оценки опасности зафиксированных признаков вводится интегральный показатель R:

$R = \Sigma w_i \cdot s_i$, i = 1..m,

где s_i – значение i-го индикатора; w_i – нормированный весовой коэффициент, отражающий критичность признака. Весовые коэффициенты (см. таблицу 1) назначаются методом экспертных оценок с учётом сценариев нарушений и нормируются так, чтобы $\Sigma w_i = 1$. Итоговая формула:

$R = 0{,}225 \cdot s\_sec + 0{,}2 \cdot s\_conf + 0{,}2 \cdot s\_log + 0{,}15 \cdot s\_net + 0{,}125 \cdot s\_auth + 0{,}1 \cdot s\_user$.

Шаг 4. Сравнение с пороговым значением. Если $R \geq R_{крит}$, считается, что зафиксирован инцидент информационной безопасности. Рекомендуемое значение $R_{крит} = 0{,}3$ обеспечивает баланс между чувствительностью системы и количеством ложных срабатываний. При необходимости порог корректируется по результатам эксплуатации.

Шаг 5. Регистрация инцидента и запуск механизма реагирования. При превышении порогового значения в журнале событий Zabbix формируется инцидент безопасности наивысшей степени серьёзности. Одновременно запускаются настроенные действия: отправка уведомлений ответственному за информационную безопасность по электронной почте или в мессенджер, а также выполнение удалённых команд на контролируемом узле. При необходимости инцидент передаётся в интегрированную SIEM-систему.

Программная реализация алгоритма включает два компонента: скрипт настройки Zabbix-агента (язык Bash), автоматически добавляющий пользовательские параметры UserParameter в конфигурационный файл агента, и XML-шаблон Zabbix-сервера, реализующий логику сбора данных, вычисления индикаторов и формирования тревожных событий. Разделение ответственности между агентом и сервером минимизирует вычислительную нагрузку на контролируемом узле и централизует логику обнаружения аномалий на стороне сервера.

Оценка эффективности алгоритма проводилась методом экспертных оценок. Было выделено 10 типов несанкционированных действий администратора; первые четыре выявляются стандартными средствами Zabbix, остальные шесть – только разработанным алгоритмом. Сумма нормированных весовых коэффициентов действий, выявляемых стандартными средствами, составила $P_1 = 0{,}228$, тогда как алгоритм обеспечивает выявление всей совокупности действий ($P_2 = 1{,}0$). Эффективность разработанного алгоритма:

$Э = P_2 / P_1 = 1 / 0{,}228 \approx 4{,}4$.

Таким образом, применение разработанного алгоритма увеличивает вероятность выявления несанкционированных действий администратора сети более чем в 4 раза по сравнению со стандартными средствами мониторинга Zabbix, не требуя приобретения дополнительного специализированного программного обеспечения

Список литературы:

1. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2009.
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008.
3. Пузанков А.М. Системы поведенческого анализа (UEBA) // Общетеоретические и отраслевые проблемы науки: сб. статей. – Волгоград, 2019. – С. 70–73.
4. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы // Вестник ПНИПУ. – 2016. – № 19. – С. 111–124.
5. Официальный сайт Zabbix [Электронный ресурс]. – URL: https://www.zabbix.com/documentation/3.4/ru/manual (дата обращения: 15.05.2026)