Секция «Математическое моделирование и информационные технологии»

Централизованный мониторинг событий аудита с целью выявления угроз безопасности

Азарычева Мария Андреевна
Аспирант
Ульяновский государственный университет, Ульяновск, Россия
E-mail: mar10537@yandex.ru

Системы управления событиями и обнаружения инцидентов – одни из важных составляющих информационной безопасности инфраструктуры автоматизированной системы [1-6]. Осуществление работы с событиями аудита операционной системы дает возможность администраторам безопасности своевременно реагировать на угрозы безопасности в информационно-телекоммуникационных системах. На сегодняшний день в ОС Astra Linux отсутствуют средства централизованного просмотра и анализа событий аудита, исходя из этого разработка модуля централизованного мониторинга событий аудита является актуальной задачей.

Для реализации процесса анализа поступающих событий аудита с контролируемых технических средств предлагается использование набора правил, формируемого администратором безопасности. Примеры правил представлены в контексте множеств $\{P_{11}, P_{12}, \dots P_{1n}\}$ и $\{P_{21}, P_{22}, \dots P_{2n}\}$. Где $\{P_{11}, P_{12}, \dots P_{1n}\}$ – правила поиска событий аудита, $\{P_{21}, P_{22}, \dots P_{2n}\}$ – правила поиска инцидентов. В рамках исследования приводятся примеры выявления следующих инцидентов: многочисленное количество неудачных попыток запуска утилиты ssh, неуспешное редактирование файлов /etc/passwd и /etc/passwd, несанкционированное изменение конфигурационного файла параметров ядра.

Для получения и последующего анализа данных в части аудита на всех станциях сети необходимо функционирование инструмента auditd с целью контроля ОС на базе заданных в конфигурационном файле правил аудита. При построении централизованной архитектуры, центральный узел осуществляет реализацию следующих функций: сбор, нормализацию каждого принятого события, отбрасывание излишних данных и анализ на основе правил, сформированных администратором безопасности. При срабатывании того или иного правила найденные события направляются в базу данных, обращаясь к которой администратор безопасности получает доступ к инцидентам и событиям на своем рабочем месте. Архитектура взаимосвязи источников регистрационной информации, центрального узла и рабочего места администратора безопасности отображена на рисунке 1. Анализ регистрационных данных аудита проводится в соответствии с алгоритмом, представленном на рисунке 2. События, относящиеся к аудиту, содержат в своем составе подстроку «msg=audit», позволяя отличить различные потоки событий друг от друга. В момент получения данных аудита инициализируется процесс формирования таблиц соответствия на основе идентификаторов, содержащихся в тексте сообщения. Формирование соответствующих таблиц позволяет объединить несколько событий одного идентификатора в одно единое, дополнив необходимыми данными. По завершении приема потока событий, происходит формирование потока сообщений аудита на основе сформированных таблиц, который затем проходит процедуру анализа согласно заведенным правилам выявления событий и инцидентов.

Аудит является одним из главных средств защиты ОС. Возможность его настройки за счет использования определенных инструментов, позволяет осуществить генерацию событий, связанных с безопасностью и своевременный их анализ с целью поиска инцидентов.

Источники и литература

1) ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. URL: https://docs.cntd.ru/document/1200068822 (дата обращения: 02.03.2024).
2) ГОСТ Р ИСО/МЭК 27002-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. URL: https://docs.cntd.ru/document/1200179669 (дата обращения: 02.03.2024).
3) ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 02.03.2024).
4) Приказ ФСТЭК России от 14 марта 2014 г. № 31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikazfstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 02.03.2024).
5) Приказ ФСТЭК России от 18 февраля 2013 г. № 21. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikazfstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 02.03.2024).
6) Федеральный Закон от 26 июля 2017 г. № 187-ФЗ. О безопасности критической информационной инфраструктуры Российской Федерации. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespecheniebezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 02.03.2024).

Иллюстрации

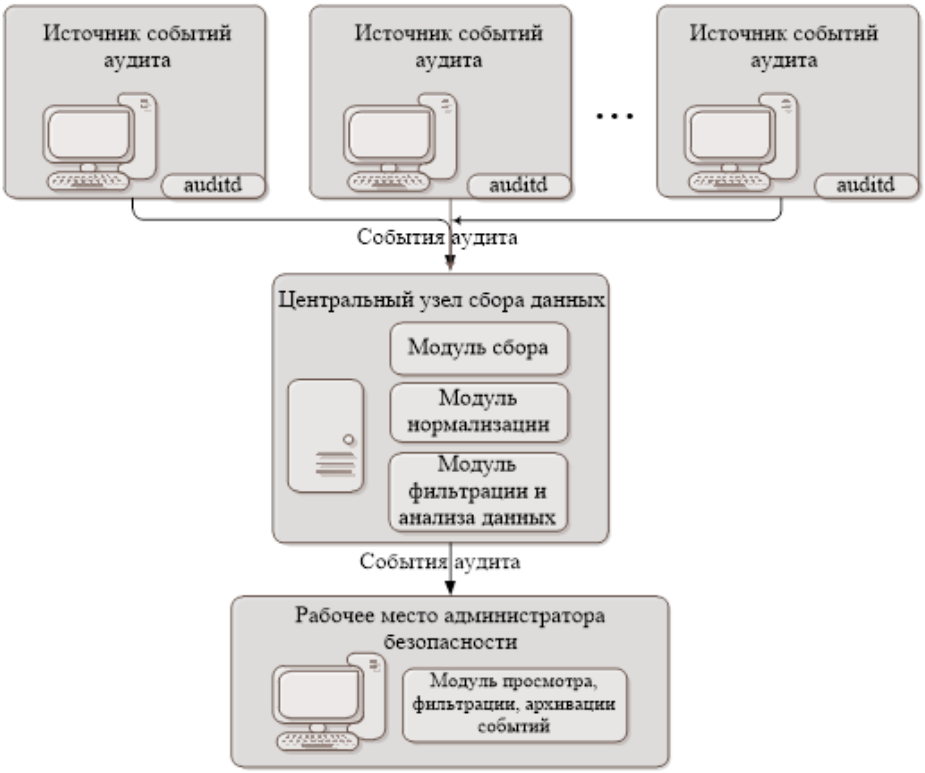

Рис. : Архитектура взаимосвязи источников событий, центрального узла сбора и рабочего места администратора безопасности

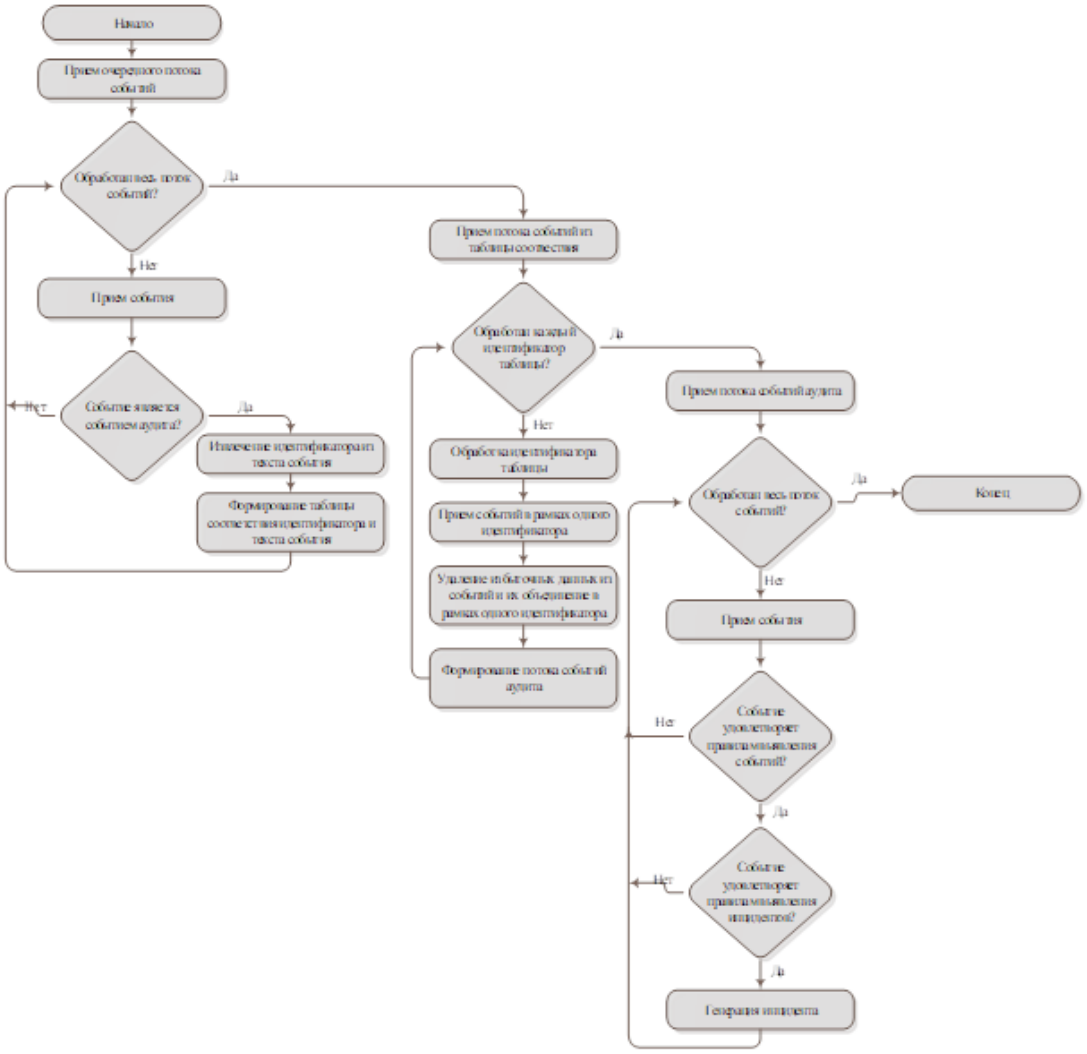

Рис. : Блок-схема алгоритма работы сервиса анализа событий аудита на основе правило-ориентированного метода