УДК 004.056.5

РАЗРАБОТКА ПРАВИЛ КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ НА ОСНОВЕ НОРМАТИВНОГО ПЕРЕЧНЯ СОБЫТИЙ

Г.С. СМОТРУК[1,2], С.Н. ПЕТРОВ[1], Т.А. ПУЛКО[1]

1 – Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь,
2 – ООО «СофтЛайн Директ»

Поступила в редакцию 7 апреля 2026

Аннотация. Рассмотрены вопросы повышения эффективности мониторинга информационной безопасности организаций за счет разработки и применения адаптированных правил корреляции событий в системах класса SIEM. Проведен анализ нормативно установленного перечня типов и записей событий информационной безопасности, подлежащих регистрации, консолидации и хранению. Выполнено сопоставление указанных типов событий с конкретными записями журналов логирования различных компонентов информационной инфраструктуры. Разработан набор правил корреляции, ориентированных на выявление типовых угроз и инцидентов информационной безопасности. Результаты апробации разработанных правил корреляции показали снижение уровня ложноположительных срабатываний и повышение эффективности выявления нарушений информационной безопасности.

Ключевые слова: информационная безопасность, SIEM-система, корреляция событий, журналы событий, мониторинг информационной безопасности, киберинциденты, приказ ОАЦ от 25 июля 2023 г. № 130.

Введение

Современные организации функционируют в условиях активной цифровизации и широкого внедрения информационных технологий, что приводит к росту запроса на безопасность. Использование распределенных вычислительных сред, удаленного доступа и сетевых приложений увеличивает сложность информационной инфраструктуры и расширяет поверхность потенциальных атак. Одновременно наблюдается рост числа и сложности кибератак, применяющих многоэтапные сценарии проникновения и маскировку вредоносной активности под легитимные действия пользователей. Одним из основных источников информации о состоянии информационной безопасности являются журналы событий, формируемые различными компонентами информационной инфраструктуры: операционными системами, серверными приложениями, СУБД, сетевым оборудованием и средствами защиты информации. Однако анализ таких журналов по отдельности затруднен из-за большого объема данных, различий в форматах записей и отсутствия единого контекста событий. Для решения данной проблемы применяются системы класса SIEM (Security Information and Event Management), обеспечивающие централизованный сбор, нормализацию, хранение и анализ событий информационной безопасности. Одним из ключевых механизмов анализа событий в таких системах являются правила корреляции, позволяющие выявлять взаимосвязанные события и формировать уведомления о потенциальных инцидентах безопасности.

Актуальность исследования обусловлена также развитием нормативно-правового регулирования в сфере информационной безопасности Республики Беларусь. В частности, в результате принятия приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» (далее – Приказ) установлен обязательный перечень типов

и записей событий информационной безопасности, подлежащих регистрации, консолидации и хранению. Данный перечень определяет минимально необходимый набор событий, подлежащих сбору, и служит основой для построения процессов мониторинга, расследования и реагирования на инциденты информационной безопасности с использованием систем класса SIEM. Перечень служит исходной точкой для последующего сопоставления событий с конкретными источниками логирования и их идентификаторами, а также для разработки правил корреляции, направленных на выявление инцидентов информационной безопасности в SIEM-системах [1].

Несмотря на широкое распространение SIEM систем и наличие в них встроенных наборов правил корреляции, большинство таких правил ориентировано на типовые сценарии угроз и не учитывает особенности конкретной информационной инфраструктуры, а также требования национального законодательства. В результате использование стандартных правил корреляции может либо не обеспечивать достаточный уровень обнаружения инцидентов, либо приводить к значительному количеству ложноположительных срабатываний.

Целью исследования является разработка набора правил корреляции событий информационной безопасности для SIEM-системы (на примере платформы RuSIEM), обеспечивающих автоматизированное выявление значимых событий и инцидентов информационной безопасности на основе нормативно установленного перечня событий.

Сопоставление типов событий с журналами логирования и их идентификаторами

Для выполнения требований Приказа в организации реализована архитектура централизованного сбора и обработки событий информационной безопасности, учитывающая разнородность источников, их критичность и масштаб инфраструктуры. Практика показывает, что нормативно установленный перечень событий может быть собран только при сочетании встроенных механизмов журналирования операционных систем с расширенными средствами аудита, а также при использовании устойчивых каналов доставки и буферизации.

В инфраструктуре на рабочих станциях и части серверов семейства Windows базовым источником является журнал безопасности и системные журналы. Однако для значимой части задач мониторинга встроенного аудита недостаточно, поскольку он фиксирует факт события, но часто не содержит необходимых атрибутов (например, хеши исполняемых файлов, сведения о родительском процессе, детализированную сетевую активность процесса). Поэтому сбор событий в Windows строится в два слоя. Первый слой – расширенный аудит безопасности, включаемый и настраиваемый централизованно через групповые политики домена Active Directory. Он позволяет детализировать аудит процессов, прав доступа, задач планировщика, служб, изменений политик и других категорий. Настройка производится через Advanced Audit Policy Configuration, где включаются категории Process Creation, Logon/Logoff, Account Management, Policy Change, Object Access, Privilege Use и другие. Существенным моментом является включение опции отображения командной строки в событиях создания процессов (Audit Process Creation: Include command line in process creation events), что позволяет для события 4688 получить аргументы запуска и повысить детектируемость скриптовых атак, «живущих за счет встроенных средств» (например, PowerShell, wscript, rundll32) [2].

Второй слой – расширенный журнал событий Sysmon, устанавливаемый как служба и ведущий логирование в отдельный журнал Microsoft-Windows-Sysmon/Operational. Sysmon обеспечивает глубоко контекстные события, которые повышают качество последующей корреляции. Для запуска процессов фиксируются события Sysmon Event ID 1 (Process Create), содержащие командную строку, родительский процесс, путь к бинарному файлу, идентификаторы процесса и пользователя, а при соответствующей конфигурации – хеши. Сетевые соединения процессов регистрируются через Sysmon Event ID 3 (Network Connection), что позволяет связывать сетевую активность не только с хостом, но и с конкретным процессом-инициатором. Для контроля изменений в файловой системе применяется Sysmon Event ID 11 (FileCreate), а изменения в реестре, связанные с закреплением и модификацией конфигурации, фиксируются событиями Sysmon Event ID 12/13/14 (создание ключа, установка значения, переименование значения). Для выявления техник внедрения в процессы и скрытого выполнения полезны Sysmon Event ID 8 (CreateRemoteThread) и Sysmon Event ID 10 (Process Access). Для наблюдения за загрузкой драйверов используется Sysmon Event ID 6 (Driver Load), что актуально

при попытках обхода средств защиты и внедрения вредоносных драйверов. Конфигурация Sysmon определяется XML-политикой и может быть унифицирована на уровне организации: в ней задаются правила include/exclude для событий с фильтрацией по путям, образам процессов, командным строкам, сетевым назначениям и т.п. В результате Windows-источник обогощается деталями (базовые идентификаторы событий из Security/System покрывают нормативную часть, а Sysmon повышает наблюдаемость и точность детектирования на этапе корреляции).

Для операционных систем семейства Linux в качестве базовых источников используются журналы systemd-journal (journald), сообщения подсистемы syslog, а также механизм аудита ядра auditd. Journald и syslog закрывают значительную часть системных событий (запуск/остановка сервисов, сообщения ядра о подключении устройств, сетевые события, сообщения приложений), однако ключевой компонент для выполнения требований по контролю действий пользователей и процессов – auditd. Auditd работает на уровне ядра, фиксируя системные вызовы и формируя события аудита, которые могут использоваться как для расследований, так и для высокоточной корреляции. Практическое преимущество auditd состоит в том, что он позволяет описывать правила фиксации действий независимо от прикладного уровня, то есть регистрировать не «лог приложения», а факт обращения процесса к объекту или вызова системного интерфейса [3].

Правила auditd могут задаваться как в виде набора директив в файлах /etc/audit/rules.d/.rules с последующей компиляцией через augenrules, так и напрямую через auditctl. В правилах определяются системные вызовы (например, execve, openat, chmod, chown, setuid), фильтры по архитектуре (b64/b32), по пользователю (uid/auid), по успешности выполнения и по путям к объектам (watch rules). Для контроля запуска процессов применяется правило аудита системного вызова execve, позволяющее фиксировать выполнение бинарных файлов и параметров запуска с привязкой к пользователю и терминалу. Типичным примером является правило вида -a always, exit -F arch=b64 -S execve -k exec_log, где метка (key) используется для последующей фильтрации и маршрутизации событий при отправке в систему мониторинга. Для контроля изменений критичных файлов (например, /etc/passwd, /etc/shadow, /etc/sudoers, конфигураций сетевых сервисов) используются watch-правила: -w /etc/passwd -p wa -k identity, фиксирующие операции записи и изменения атрибутов. Для контроля действий планировщика могут быть выделены правила на файлы /etc/crontab, каталоги /etc/cron и пользовательские crontab-файлы. Для отслеживания применения привилегий важны события, связанные с sudo (как журналы /var/log/auth.log или /var/log/secure, так и аудит системных вызовов setuid/setgid), а также системные события изменения ролей и контекстов безопасности, если используется SELinux (avc: denied) или AppArmor [9].

Auditd формирует события нескольких типов, наиболее часто используемых для задач мониторинга: EXECVE и SYSCALL для запуска процессов и системных вызовов, USER_LOGIN/USER_LOGOUT/ USER_AUTH для событий аутентификации, USER_ADD/USER_DEL/ USER_MOD для управления учетными записями, SERVICE_START/ SERVICE_STOP для жизненного цикла сервисов. В дополнение к auditd важны сообщения ядра и systemd о подключении устройств (USB и другая периферия), а также сетевые события подсистемы фильтрации пакетов. В зависимости от реализации это могут быть сообщения iptables, nftables, firewalld и записи подсистемы netfilter, которые используются для фиксации разрешенных/заблокированных соединений и попыток доступа к нестандартным портам. Для обеспечения непрерывности логирования в Linux применяется ротация журналов (logrotate), управление размером и временем хранения journald, а также буферизация на уровне транспортных сервисов (rsyslog/syslog-ng) при временной недоступности центрального коллектора.

Разработка правил корреляции

В соответствии с изложенными принципами в рамках практической реализации разработан перечень правил корреляции событий информационной безопасности, реализующих требования нормативно установленного набора типов и записей событий. Правила разработаны для применения в SIEM-системе RuSIEM и ориентированы на выявление значимых аномалий и инцидентов информационной безопасности в условиях функционирования реальной информационной инфраструктуры организации. Представленные правила охватывают

ключевые категории источников событий и классы информационных активов, включая операционные системы, системы управления базами данных, телекоммуникационное оборудование, средства защиты информации и прикладное программное обеспечение. Каждое правило построено на анализе формализованных полей нормализованных событий и использует логические, строковые и агрегирующие механизмы корреляции, поддерживаемые SIEM-системой. Список разарботанных правил включает правила:

– выявления незапланированного отключения операционной системы;

– контроля событий остановки и аварийного завершения системных служб и демонов;

– обнаружения фактов использования недоверенных съемных машинных носителей информации;

– выявления фактов подключения запрещенных периферийных устройств и каналов передачи данных;

– детектирования попыток установки и запуска недоверенного программного обеспечения с признаками обхода ограничений привилегий;

– обнаружения признаков компрометации учетных записей пользователей;

– детектирования аномального использования привилегированных учетных записей пользователей;

– контроля операций создания, удаления и модификации учетных записей пользователей;

– выявления неудавшихся и отмененных действий пользователей и процессов;

– контроля создания и изменения заданий автозапуска и планировщика задач;

– контроля установки, удаления, перезапуска и ошибок запуска служб и сервисов;

– детектирования изменений системной конфигурации, сетевых настроек и средств межсетевого экранирования;

– обнаружения фактов удаления журналов и следов аудита в операционных система;

– контроля изменений и попыток изменения настроек средств защиты операционных систем;

– выявления несанкционированных сетевых соединений и удаленного доступа;

– детектирования массового архивирования и вывода данных в операционных системах;

– контроля сессий и аутентификации пользователей в системах управления базами данных;

– обнаружения попыток аутентификации в СУБД с использованием незарегистрированных учетных записей;

– детектирования подозрительных административных действий пользователей в системах управления базами данных;

– контроля операций назначения и отзыва привилегий пользователей в системах управления базами данных;

– контроля запуска и остановки телекоммуникационного оборудования;

– контроля изменений системной конфигурации телекоммуникационного оборудования;

– выявления подозрительных операций с локальными учетными записями на сетевых устройствах;

– обнаружения фактов удаления журналов и следов аудита в операционных системах;

– контроля изменений и попыток изменения настроек средств защиты операционных систем.

Ниже продемонстрировано правило выявления фактов подключения и отключения устройств ввода/вывода к сетевым устройствам. Подключение USB-устройств, модемов и накопителей к сетевым устройствам может использоваться для обхода политики безопасности, загрузки конфигураций или вывода данных (достаточно распростарненный случай). Корреляция фиксирует все операции подключения и отключения устройств ввода/вывода.

Huawei: %DEV/5/DEV_ADD, %DEV/5/DEV_REMOVE.

Check Point: USB device inserted/removed.

FortiGate: logid=0100040000.

Cisco: syslog USB insert/remove.

Логика работы правила корреляции:

```
(
  device.vendor in {"Huawei","Check Point","Fortinet","Cisco"}
```

```
AND
(
  event.type contains "DEV_ADD"
  OR event.type contains "DEV_REMOVE"
  OR event.type contains "USB"
```

Обобщенная модель корреляции событий информационной безопасности представлена в табл. 1.

Табл. 1. **Обобщенная модель корреляции событий информационной безопасности**

Категория события	Источник	Признаки события	Условия корреляции	Выявляемый инцидент
Аутентификация пользователей	Windows Security Log / Linux auth.log	Множественные ошибки входа	>5 неудачных попыток входа за короткий интервал времени	Подбор пароля (Brute Force)
Аутентификация пользователей	Windows / Linux	Успешный вход после серии ошибок	Успешная аутентификация после множества неудачных попыток	Компрометация учетной записи
Управление учетными записями	Active Directory / Linux user management	Создание новой учетной записи	Создание пользователя вне рабочего времени	Несанкционированное создание учетной записи
Управление учетными записями	Active Directory	Добавление пользователя в группу администраторов	Добавление в привилегированную группу	Эскалация привилегий
Использование привилегий	Windows Security Log / Linux sudo	Использование административных прав	Частые вызовы привилегированных команд	Подозрительная административная активность
Запуск процессов	Windows Process Events / Linux auditd	Запуск системных утилит	Запуск инструментов администрирования обычным пользователем	Возможная подготовка атаки
Изменение системных настроек	Windows Security Policy / Linux configuration logs	Изменение политики безопасности	Изменение параметров аудита или политики безопасности	Попытка сокрытия активности
Доступ к файлам	Windows Object Access / Linux file audit	Массовое чтение или копирование файлов	Большое количество операций чтения за короткое время	Возможная утечка данных
Сетевые соединения	Firewall / IDS / Netflow	Подключения к подозрительным адресам	Повторяющиеся соединения с неизвестными внешними узлами	Командный сервер (C2)
Сетевые соединения	Firewall logs	Массовые соединения на разные порты	Сканирование портов	Сетевая разведка
Аппаратные события	Windows Device Events / Linux udev	Подключение внешних устройств	Подключение USB в защищенной зоне	Потенциальная утечка данных
Завершение процессов	Windows / Linux	Принудительное завершение системных служб	Остановка служб безопасности	Отключение средств защиты

Проведенный анализ журналов операционных систем, сетевого оборудования и средств защиты информации позволил выделить основные категории событий, имеющих наибольшее значение для задач мониторинга информационной безопасности. К ним относятся события аутентификации пользователей, управление учетными записями, использование привилегий, запуск процессов, доступ к данным и сетевые соединения. Несмотря на различия в форматах журналов и идентификаторах событий различных операционных систем, большинство событий могут быть приведены к унифицированным логическим типам. Это позволяет формировать универсальные правила корреляции, основанные на семантике событий, а не на конкретных

идентификаторах журналов. Разработанная обобщенная модель корреляции связывает категории событий, источники журналов и условия их совместного анализа, что позволяет выявлять типовые сценарии нарушений информационной безопасности, включая подбор паролей, компрометацию учетных записей, эскалацию привилегий, подготовку атак, утечку данных и взаимодействие с командными серверами злоумышленников.

Заключение

Исследование подтвердило важность системного подхода к разработке правил корреляции событий информационной безопасности в SIEM-системах. В отличие от типовых наборов правил, ориентированных на универсальные сценарии угроз, предложенный подход основан на учете нормативных требований и особенностей функционирования конкретной информационной инфраструктуры. Сформирована методика сопоставления нормативно установленных в соответствии с Приказом типов событий информационной безопасности с записями журналов различных источников, что обеспечивает корректную интерпретацию событий на уровне системы мониторинга безопасности. Разработан набор правил корреляции, позволяющий выявлять сложные сценарии атак и нарушений политики безопасности. Апробация разработанных правил показала их высокую эффективность при эксплуатации в реальной информационной инфраструктуре. Применение предложенных правил позволило повысить снизить количество ложноположительных срабатываний и улучшить процессы реагирования на события информационной безопасности. Полученные результаты могут быть использованы при проектировании и модернизации систем мониторинга безопасности, а также при разработке нормативно ориентированных механизмов обнаружения инцидентов информационной безопасности.

DEVELOPMENT OF RULES FOR CORRELATION OF INFORMATION SECURITY EVENTS IN SIEM SYSTEMS BASED ON A NORMATIVE LIST OF EVENTS

H.S. SMATRUK, S.N. PETROV, T.A. PULKO

Abstract. The issues of increasing the effectiveness of monitoring the information security of organizations through the development and application of adapted rules for event correlation in SIEM class systems are considered. The analysis of the normatively established list of types and records of information security events subject to registration, consolidation and storage is carried out. The specified types of events were compared with specific log entries of various components of the information infrastructure. A set of correlation rules has been developed aimed at identifying typical threats and incidents of information security. The results of testing the developed correlation rules showed a decrease in the level of false positive positives and an increase in the effectiveness of detecting information security violations.

Keywords: information security, SIEM system, event correlation, event logs, information security monitoring, cyber incidents, OAC Order No. 130 dated July 25, 2023.

Список литературы

1. О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 : приказ Оператив.-аналит. центра при Президенте Респ. Беларусь, 25 июля 2023 г., № 130 // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=12551&p0=T62305425 (дата обращения: 06.04.2026).
2. Таненбаум Э. Современные операционные системы / Э. Таненбаум, Х. Бос. – 4-е изд. – СПб.: Питер, 2015. – 1120 с.
3. Столлингс У. Операционные системы. Внутренняя структура и принципы проектирования / У. Столлингс. – 9-е изд. – М.: Вильямс, 2019. – 944 с.
4. Робачевский А. М. Операционная система UNIX / А. М. Робачевский. – СПб.: БХВ-Петербург, 2016. – 640 с.