

Архипов Алексей Витальевич

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Информационные системы

Значение мониторинга информационной безопасности для организаций с удаленными информационными ресурсами

Аннотация. В статье рассматривается значение мониторинга информационной безопасности для организаций, использующих удаленные информационные ресурсы: филиальные серверы, рабочие станции сотрудников, виртуальные машины, облачные компоненты и сетевое оборудование. Анализируются риски отсутствия единой наблюдаемости и требования к централизованному сбору и анализу событий. Показано, что мониторинг необходим не только для обнаружения атак, но и для контроля состояния ИТ-активов, расследования инцидентов и поддержания устойчивости работы организации. В качестве практической технологической основы рассматривается Wazuh.

Ключевые слова: мониторинг информационной безопасности, удаленные ресурсы, распределенная инфраструктура, SIEM, Wazuh, события безопасности, сбор журналов, обнаружение инцидентов.

Современная ИТ-инфраструктура организации выходит за пределы единой локальной сети. В нее входят удаленные подразделения, серверы в центрах обработки данных, облачные ресурсы, виртуальные машины и рабочие станции сотрудников, подключающиеся из разных сетей. Под удаленным информационным ресурсом в работе понимается ресурс организации, физически размещенный вне основной площадки либо доступ к которому осуществляется через внешние или межсегментные соединения. Такая архитектура повышает гибкость бизнеса, но усложняет получение единой картины состояния информационной безопасности [1; 2].

Актуальность проблемы подтверждается современными данными об угрозах. В исследовании Positive Technologies за вторую половину 2024 года и первые три квартала 2025 года отмечено использование незащищенных служб удаленного доступа как точки входа в инфраструктуру российских организаций [1]. Это не доказывает, что причиной каждого инцидента является отсутствие мониторинга, но показывает необходимость постоянного контроля удаленных точек доступа.

1. Особенности мониторинга удаленных ресурсов

ГОСТ Р 59547-2021 определяет мониторинг информационной безопасности как процесс постоянного наблюдения и анализа данных о событиях безопасности для выявления нарушений, угроз и уязвимостей. Стандарт предусматривает возможность охвата информационных систем, функционирующих в центрах обработки данных и облачной инфраструктуре [2]. Следовательно, удаленность ресурса не исключает централизованный мониторинг, а требует его технической и организационной организации.

Для распределенной инфраструктуры характерны различия в операционных системах, форматах журналов и способах подключения. Часть устройств позволяет установить агент, другая часть передает события через Syslog или API. Система мониторинга должна объединять неоднородные источники и связывать событие с конкретным активом, пользователем и временем.

2. Риски отсутствия единого мониторинга удаленных ресурсов

Первый риск связан с появлением «слепых зон». События на удаленном сервере или рабочей станции могут не попадать в единое пространство анализа. Второй риск — потеря контекста: последовательность «неудачные попытки входа — успешная аутентификация — повышение привилегий — изменение файла» может быть распределена между несколькими источниками и без корреляции восприниматься как набор несвязанных событий [5, с. 15; 6, с. 32].

Третий риск возникает при расследовании инцидента. Если журналы хранятся только локально, специалисту необходимо получать данные с каждого узла и восстанавливать хронологию. ГОСТ Р 59548-2022 устанавливает требования к регистрируемой информации и предусматривает фиксацию даты и времени,

идентификатора события, источника, результата операции и субъекта доступа [3]. Это формирует основу для централизованного анализа.

Мониторинг важен и для контроля доступности и целостности. Отсутствие событий от удаленного узла может означать не отсутствие угроз, а остановку агента, потерю связи или изменение конфигурации. Поэтому состояние канала мониторинга должно контролироваться отдельно.

3. Требования к системе мониторинга

Система мониторинга удаленных ресурсов должна обеспечивать полноту охвата и достаточность данных. ГОСТ Р 59547-2021 допускает агентный и безагентный сбор [2]. Для большинства организаций приоритетными источниками являются:

- события аутентификации и авторизации;
- события удаленного подключения и изменения параметров доступа;
- запуск процессов и привилегированные операции;
- изменения критических файлов и конфигураций;
- сведения об установленном программном обеспечении и уязвимостях;
- сообщения средств защиты и данные о работе контролируемых компонентов.

Существенным требованием является своевременность. Критические события должны поступать с минимальной задержкой, а инвентаризационные сведения могут передаваться периодически. При этом данные мониторинга необходимо защищать от изменения и несанкционированного доступа [2; 3].

4. Мониторинг как основа управления инцидентами

Мониторинг не заменяет средства предотвращения атак, а формирует обратную связь между состоянием инфраструктуры и действиями специалистов. Процесс можно представить как последовательность: сбор данных — нормализация — анализ — выявление отклонения — оценка — реагирование — ретроспективный анализ. Такой подход соответствует концепции «непрерывный мониторинг», в которой актуальные сведения используются для оценки риска и своевременного управления защитными мерами.

Для распределенной инфраструктуры особенно важна корреляция. Единичное

событие редко дает достаточный контекст, тогда как взаимосвязанные события от нескольких узлов могут указывать на единый сценарий атаки. Исследования построения SOC и интеграции SIEM подтверждают значение централизованного сбора, предобработки и сопоставления событий [5, с. 13; 6, с. 21]. Накопленные данные используются и после завершения инцидента: они позволяют восстановить последовательность действий, определить затронутые активы и уточнить правила обнаружения.

5. Применение Wazuh для удаленных ресурсов

В рамках разрабатываемой системы практической основой централизованного мониторинга может выступать Wazuh. Официальная архитектура платформы включает агенты на контролируемых узлах и центральные компоненты Wazuh server, Wazuh indexer и Wazuh dashboard. Агент собирает данные на конечной точке и передает их серверу для анализа, после чего результаты индексируются и визуализируются [7].

Wazuh поддерживает установку агентов на Windows, Linux и macOS, а также на виртуальные машины, контейнеры и облачные экземпляры. Для устройств, где установка агента невозможна, предусмотрен безагентский прием журналов. Платформа также поддерживает контроль целостности файлов, инвентаризацию и выявление уязвимостей. Это позволяет в одном контуре объединять сведения о состоянии удаленных активов и событиях безопасности.

При этом техническая платформа не заменяет проектирование правил мониторинга. Перечень критических событий должен соответствовать архитектуре организации, способам удаленного доступа и значимости конкретных ресурсов. Для субъектов критической информационной инфраструктуры российское законодательство предусматривает мероприятия по обнаружению и противодействию компьютерным атакам [4].

6. Практические принципы построения мониторинга

При внедрении мониторинга целесообразно последовательно определить перечень активов и их критичность, состав источников и событий, организовать защищенную передачу и централизованное хранение, а затем настроить корреляцию

и порядок реагирования. Отсутствие данных от критического ресурса следует фиксировать как отдельное событие, требующее проверки.

Полученные результаты позволяют сформулировать следующие положения:

1. Удаленные ресурсы расширяют область контроля организации и повышают требования к наблюдаемости инфраструктуры.

2. Централизованный мониторинг уменьшает вероятность формирования неучтенных зон за счет объединения событий от различных площадок и типов устройств.

3. Мониторинг необходим для обнаружения подозрительной активности, инвентаризации, контроля конфигураций и расследования инцидентов.

4. Wazuh может использоваться как технологическая основа такого контура благодаря поддержке конечных точек и функций контроля состояния активов.

Таким образом, для организаций с удаленными информационными ресурсами мониторинг является механизмом непрерывной обратной связи о состоянии ИТ-инфраструктуры. Его практическая ценность заключается в переводе разрозненных журналов и технических признаков в единое пространство анализа. Российские стандарты связывают мониторинг с постоянным наблюдением, сбором, обработкой и анализом событий, а средства класса SIEM позволяют реализовать эти принципы на распределенных объектах.

Литература

1. Positive Technologies. CODE RED 2026: Актуальные киберугрозы для российских организаций / [Электронный ресурс] / URL: <https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/> (дата обращения: 24.09.2026).

2. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения / [Электронный ресурс] / URL: <https://docs.cntd.ru/document/1200180385?ysclid=mv137cerf876088399>.

3. ГОСТ Р 59548-2022. Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации / [Электронный ресурс] /

URL: <https://docs.cntd.ru/document/1200182791?ysclid=mv134hg39a862827299>.

4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) / [Электронный ресурс] / URL: <https://www.consultant.ru/cons/cgi/online>. (дата обращения: 24.09.2026).

5. Мунтян М.М., Сидоркина И.Г. Способ интеграции вспомогательного модуля с SIEM-системами // Вестник Чувашского университета. 2024. № 4. С. 60–74.

6. Миханько А.Д., Машкина И.В. Метод определения типичных временных характеристик событий безопасности на основе статистических данных для задач корреляционного анализа // Проблемы информационной безопасности. Компьютерные системы. 2026. № 2. С. 32–48.

7. Wazuh Documentation. Architecture / [Электронный ресурс] / URL: <https://documentation.wazuh.com/current/getting-started/architecture.html> (дата обращения: 24.09.2026).