

АНАЛИЗ ФУНКЦИЙ МОНИТОРИНГА И УПРАВЛЕНИЯ ПЕРИМЕТРАЛЬНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: Целью исследования – определить эффективность представленных возможностей для просмотра и управления периметральной системой защиты информации. В статье рассмотрены основные функции, программного обеспечения вендора, способствующие значительному упрощению работы сотрудников и повышению их результатов для сохранения данных компании в современном мире. **Научная новизна** заключается в изучении и анализе возможностей современных систем для охраны компании от новых угроз. **В результате** определено, что вендоры на сегодняшний день находятся в постоянном улучшении своего программного продукта, позволяя сохранять данные своих заказчиков под замком.

Ключевые слова: Security Management Server, сервер управления шлюзами, технические задачи, операции контроля.

Annotation: the purpose of the study is to determine the effectiveness of the presented capabilities for viewing and managing the perimeter information security system. The article discusses the main functions of the vendor's software that significantly simplify the work of employees and improve their results for saving company data in the modern world. Scientific novelty consists in studying and analyzing the capabilities of modern systems to protect the

company from new threats. As a result, it is determined that vendors are currently constantly improving their software product, allowing them to keep their customers' data under lock and key.

Keywords: Security Management Server, gateway management server, technical tasks, control operations.

Security Management Server (SMS) - сервер управления шлюзами предназначена для централизованного управления несколькими шлюзами, а также для автоматизации процесса мониторинга оборудования ПСЗИ, что предусматривает решение следующих технических задач:

- получение объективных и актуальных данных о состоянии оборудования для оперативно-технического управления;
- Внесение изменение в политику безопасности на межсетевом экране;
- текущий анализ работоспособности технического состояния оборудования;
- снижение вероятности недоступности сети в целом и уменьшение времени простоя оборудования;
- просмотр нагрузки оборудования;
- просмотр статуса VPN-туннелей между различными площадками ОГ;
- просмотр логов трафика взаимодействий между различными площадками;
- просмотр списка пользователей, которые подключаются к оборудованию;
- просмотр о последней установленной политики на оборудование;
- выгрузка логов трафика за определенный период.

Security Management Server (SMS) представляет собой комплекс программно-аппаратных средств, построенных по принципу интегрированного управления.

SMS осуществляет следующие операции:

- производит постоянную защиту рабочих станций пользователей на основе политики безопасности;
- контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа субъектов к указанным ресурсам;
- обеспечены механизмы обнаружения и защиты от вторжений (IDS/IPS);
- идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору доступа;
- оповещение администраторов безопасности информации о критичных событиях ИБ;

Сервер управления шлюзами обеспечивает автоматическую защиту информации на основании установленных правил.

Все предоставленные системой функции для мониторинга и управления позволяют эффективно оперативно и легко получать необходимую информацию о состоянии системы, быстро устранять и предотвращать новые угрозы для компании в современном мире технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. <https://habr.com/ru/company/tssolution/blog/323606/>
2. SmartView Tracker R77 Administration Guide. — 2-е изд. — Check Point Software Technologies Ltd. 2014 г.. —36 с.
3. Gaia R77 Versions Administration Guide - 2-е изд. - Check Point Software Technologies Ltd. - 2016 г.. —266 с.