Грани SIEM

Рассмотрены отдельные функции, возможности и способы применения первой отечественной SIEM-системы Security Capsule, которые не являются очевидными. Особое внимание авторы уделили функциональным возможностям SIEM Security Capsule, превосходящим заграничные аналоги, и существующим недостаткам применения зарубежных программных продуктов в инфраструктуре российских компаний. Из приведенных в статье данных можно сделать вывод, что на сегодняшний день Security Capsule не имеет аналогов среди российских продуктов данного класса по реализованному функционалу, архитектуре, а также по соотношению затрат на приобретение, внедрение, применение и по результативности в деле обеспечения уровня безопасности организаций.

Ключевые слова: SIEM, SIEM Analytics, SIEM-система, Security Capsule, особенности применения, первая отечественная SIEM, ГИС, ИСПДн, АСУ ТП, регистрация, корреляция, события ИБ

Сергей Александрович Графов,
эксперт

Артем Юрьевич Белявцев,
программист

Дмитрий Андреевич Воронов,
программист

Андрей Андреевич Трофимов,
программист

Данная статья является продолжением публикации [1], также при ее подготовке использовались материалы, размещенные на сайте проекта SIEM Analytics [2].

За последние годы, в связи с выходом нормативно-методических документов регуляторов, предъявляющих требования к системам регистрации событий в ЛВС, значительно повысился интерес к системам класса SIEM (*Security information and event management*).

Пока продолжаются дискуссии о назначении и функциях SIEM различных производителей, признаках SIEM, целесообразности и эффективности применения систем данного класса, компания ООО «Инновационные технологии в бизнесе» выпустила и успешно внедряет новую версию системы Security Capsule. В статье описываются отдельные функции, возможности и способы применения Security Capsule, не являющиеся очевидными и отражаемые авторами как «грани SIEM».

Security Capsule является незаменимым средством при выявлении инцидентов ИБ и их разборе. Ее внедрение позволяет оценить эффективность применения средств, используемых в конкретной системе защиты, корректность их настроек, выявить наиболее проблемные элементы инфо-телекоммуникационных систем и автоматизированных систем управления технологическими процессами (АСУ ТП).

Для администрирования системы предусмотрены группы пользователей с настраиваемыми правами доступа и функциональностью. На данном этапе завершается разработка коннекторов для сбора событий ИБ от специализированных источников, входящих в состав АСУ ТП.

Security Capsule, реализующая подсистему централизованной ре-

En SIEM profile

S. A. Grafov,
expert

A. Yu. Beliavtsev,
software developer

D. A. Voronov,
software developer

A. A. Trofimov,
software developer

This article describes unobvious features, capabilities and ways of utilization of the first domestic SIEM-system Security Capsule. Authors put special attention to the capabilities which outdo foreign analogues, and also to existing weakness of these analogues being utilized in Russian companies infrastructures. The article highlights that Security Capsule is a unique solution on the Russian market due to its functions, architecture, effectiveness and reasonable costs.

Keywords: SIEM, SIEM Analytics, Security Capsule, application features, first domestic SIEM-system, state departmental information systems, personal data information systems, APCS, registration, correlation, information security events

гистрации, учет и корреляции событий ИБ, соответствует требованиям следующих федеральных законов, нормативно-методических и организационных документов:

- Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 14 марта 2014 года № 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»;
- Руководящий документ Гостехкомиссии России от 30 марта 1992 года «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
- нормативно-методический документ Гостехкомиссии России от 30 августа 2002 года № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее – СТР-К);
- приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 18 мая 2007 года).

Security Capsule не только соответствует по качеству лучшим иностранным образцам, но и превосходит их по ряду параметров:

1) является специализированным средством защиты информации, в состав которого входит стандартный набор конвекторов к сертифицированным СЗИ от НСД, криптографических средств защиты;

2) интегрирована с основными автоматизированными системами уровня предприятия и производства в области ТЭК (многолетний опыт интеграции с системами энергосбытовой, энергетической отраслей и др.);

3) стоимость ее приобретения и внедрения на порядок меньше аналогичных западных образцов (например, системы ArcSight);

4) неограниченная масштабируемость и аналитические возможности;

5) оперативность технической поддержки и обновлений системы;

6) ориентирована прежде всего на соответствие отечественным техническим регламентам и стандартам в области ИБ.

На сегодняшний день Security Capsule не имеет аналогов среди российских продуктов данного класса по реализованному функционалу, архитектуре, а также по соотношению затрат на приобретение, внедрение, применение и по результативности в деле обеспечения уровня безопасности организаций.

Security Capsule может использоваться для мониторинга и корреляции событий ИБ государственных информационных систем (ГИС), информационных систем персональных данных (ИСПДн), АСУТП, а также других систем, для которых требуется ведение мониторинга и анализ происходящих в них событий.

Security Capsule прошла испытания и экспертизу в системе сертификации ФСТЭК России на соответствие требованиям ТУ и отсутствие НДВ по 4 уровню (Сертификат соответствия в системе сертификации ФСТЭК России № 3649 от 9 ноября 2016 года).

Security Capsule зарегистрирована в едином реестре Минкомсвязи России российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети Интернет приказом министерства от 14 июня 2016 года (Свидетельство о государственной регистрации программы для ЭВМ № 2016613392).

Правильность архитектурных решений и качество системы подтверждены также положительным семилетним опытом внедрения, эксплуатации и испытаний на пилотных зонах в крупнейших предприятиях и организациях энергетической отрасли, нефтедобывающей компании, ПАО «Газпром межрегионгаз», энергосбытовой отрасли, фондах ОМС, ГК «Роснефть» и др. Функциональность и качество системы оценивались согласно типовой методике оценки более чем по 150 параметрам и требованиям.

Кроме основных функций необходимо перечислить так называемые грани SIEM (дополнительные функции и возможности системы), такие как:

1) оценка эффективности применяемых средств защиты, систем защиты информации;

2) оценка полноты и корректности настроек средств и механизмов защиты, включая механизмы защиты, встроенные в операционные системы, системы управления базами данных, коммуникационное оборудование, прикладное ПО;

3) оценка соответствия состояния ИБ требованиям регуляторов, политик ИБ компании (организации, предприятия, учреждения);

4) использование данных о событиях ИБ при разборе инцидентов, интеграция SIEM с системами разбора инцидентов;

5) применение системы для сбора событий не только ИБ-, но технологической информации, например, с АСУ ТП.

Все эти возможности реализованы в системе Security Capsule.

Система представляет собой программный комплекс в защищенном исполнении, в котором воплощены следующие механизмы защиты:

- идентификация и аутентификация пользователей (администратора и операторов) [ИАФ.1];
- управление доступом [УПД.1], [УПД.6];
- контроль целостности компонентов Системы [ОЦЛ.1];
- регистрация событий в системе [РСБ.2], [РСБ.3], [РСБ.5], [РСБ.8].

При работе с Системой обеспечиваются следующие возможности:

- настройка системы в составе целевой информационной системы и/или системы защиты заказчика;
- реализация агентского и безагентского методов сбора событий ИБ;
- организация сбора и передачи информации о событиях ИБ по нижеперечисленным протоколам и методам:
  - UDP (*User Datagram Protocol*) – протокол пользовательских датаграмм;
  - TCP/IP (*Transmission Control Protocol/Internet Protocol*);
  - SMTP (*Simple Mail Transfer Protocol*) – простой протокол передачи почты;
  - SQL Queries – запросы в БД;
  - WMI (*Windows Management Instrumentation*) – инструментарий управления ОС Windows, удаленный безагентовый сбор для Windows;
  - WEB GET/POST – методы передачи данных, GET- и POST-запросы (например, SDEE);
  - SMB (*Server Message Block*) – сетевой протокол прикладного уровня;
  - Syslog (*system log* – системный журнал) – стандарт отправки и регистрации сообщений о происходящих в системе событиях;
  - SNMP (*Simple Network Management Protocol*) – простой протокол сетевого управления;
- сбор событий от неоднородных, территориально распределенных источников событий;
- гарантированный сбор, обработка и доставка информации о событиях ИБ при агентском методе сбора;
- встроенный «мастер» настройки модулей;
- нормализация событий;
- агрегация событий;
- корреляция событий;
- разбор инцидентов ИБ;
- управление учетными записями пользователей системы;
- хранение информации о событиях ИБ, фильтрация данных по заданным критериям;
- организация ролевого метода и разграничение доступа пользователей к объектам доступа;
- определение состава и содержания информации о событиях безопасности от различных источников;
- формирование отчетов о событиях ИБ;
- ранжирование событий;
- отправка сообщения о событиях ИБ в реальном масштабе времени и по расписанию;
- отправка сообщений о событиях различного уровня значимости на адреса электронной почты;
- отправка отчетов о событиях ИБ по расписанию;
- отправка отчетов о событиях ИБ в зашифрованном виде;
- просмотр и анализ результатов регистрации и реагирование на них (регистрационные журналы с регламентированным доступом);
- контроль работоспособности компонентов системы;
- восстановление работоспособности системы после сбоев и отказов;
- геоинформационная привязка источников событий и архитектуры системы.

Важно: *Не поставляются средства обратной связи на источники целевой системы, однако такая возможность предусмотрена и активируется по требованию заказчика.*

Далее перечислим достоинства и недостатки агентского и безагентского методов сбора событий информационной безопасности.

1. *Безагентский метод сбора* характерен для большинства известных систем данного класса и показал достаточную эффективность. Как правило, применяется там, где недопустимо применение агентского метода сбора.

Положительные факторы метода:

а) возможность сбора данных без установки дополнительного ПО на конечную рабочую станцию;

б) простота управления для администратора безопасности из единой точки – консоли администратора, отсутствие каких-либо дополнительных настроек при установке;

в) развитый набор стандартных средств, например ОС Windows;

г) сбор данных из файлов.

Особенности реализации метода:

1) необходимость создания учетных записей пользователей с различными правами доступа;

2) отсутствие шифрования при передаче данных;

3) отсутствие возможности гарантированной доставки (то есть возможно удаление логов событий до их передачи в систему);

4) многомерное увеличение нагрузки на центральный узел обработки системы, так как весь исполняющийся код выполняется на стороне узла;

5) отсутствие возможности нормализации трафика до операции передачи данных на обработку;

6) невозможность работы в периметре закрытой сети (невозможность инициализации соединения в границы такой сети).

2. Преимущества *агентского метода сбора* относительно безагентского:

а) не требует создания дополнительных учетных записей для обеспечения работы клиента;

б) применение шифрования при передаче данных;

в) обеспечение сжатия данных;

г) нормализация трафика;

д) отправка сообщений о событиях ИБ в заданные промежутки времени;

е) гарантированная доставка сообщений (в случае отказа, происхо-

дит сохранение в локальную базу, а затем – отправка при возобновлении соединения);

ж) первичная обработка данных происходит на стороне клиента, за счет чего увеличивается производительность центрального узла (нагрузка на клиента – минимальная);

з) реализована возможность создания профилей защиты для каждого клиента, а также работа по менеджменту этих клиентов (объединение в группы, формирование профиля защиты на группу), что позволяет осуществлять фильтрацию данных еще при первичной обработке событий, до момента ее передачи на сервер (профили защиты позволяют реализовать механизмы «черных» и (или) «белых» списков;

и) возможность работы в рамках закрытой сети;

к) удаленная установка и удаление ПО агента;

л) возможность локальной установки клиента (со съемного носителя информации);

м) возможность установки агента с помощью Active Directory;

н) работа со специализированными средствами защиты информации – написанными библиотеками или предоставляемыми DLL (например, Dallas Lock, eToken);

о) возможность проведения дополнительного аудита (например, контроль внешних носителей без системы DLP);

п) упорядочивание источников.

Особенности реализации метода:

1) необходимость установки стороннего ПО, что не всегда допускается политикой ИБ компании;

2) необходимость интеграции в программную среду.

В Security Capsule реализованы модули агентского сбора, основанные на опыте эксплуатации предыдущих версий системы, требованиях заказчиков, политиках ИБ крупных организаций.

Дополнительные модули прошли апробирование в структурах ГК «Россети», Росграницы, АО «Газпром межрегионгаз», ГК «Интер РАО», ПАО «НК «Роснефть» и др.

Данные модули устанавливаются и активируются как на ПК пользователей, так и на серверах, и запускаются как службы. При возникновении события администратор получает сигнал (сообщение) о факте возникновения события и описание последнего. Перечень модулей агентского метода приведен в табл. 1. Следует иметь в виду, что представленные в ней состав модулей и их функции могут быть дополнены, расширены или изменены.

Таблица 1. ***Перечень модулей агентского метода***

№ п/п	Наименование модуля	Функция	Инициатор
1	Контроль событий AD	Функция предназначена для сравнения текущего состояния AD с эталонным. Применяется для выявления несогласованных учетных данных, несанкционированного изменения прав, изменения роли (группы) и т. д.	Рекомендовано ПАО «Интер РАО» и др.
2	Контроль событий реестра	Данная функция применяется, например, с целью выявления несанкционированной установки ПО, изменения ОС, оборудования. В частности, используется для контроля ветвей реестра, которые могут быть несанкционированно модифицированы при включении персонального компьютера в бот-сеть	Рекомендовано для контроля АО КБ «Газпромбанк», АО «Газпром межрегионгаз»
3	Контроль событий eToken	Функция сравнивает перечень зарегистрированных в организации носителей ключевой информации с активными носителями. При появлении незарегистрированного носителя инициируется событие. Актуальна, например, для финансовых систем при проведении платежей. Может быть увязана с учетными данными пользователей ПК	Рекомендовано ПАО «Интер РАО» и др.
4	«Белый»/ «черный» список ПО	Функция сравнения эталонного перечня разрешенного ПО с пользовательским и системным ПО. Позволяет контролировать, например, отсутствие средств разработки (модификации) кода, месенджеры и т. д.	Рекомендовано к реализации ГК «Россети», МРСК

Система построена с применением клиент-серверной технологии, имеет модульную иерархическую архитектуру.

Основные понятия системы:

а) *неоднородные данные* – представляют собой события, для которых не заданы правила разбора (все события по умолчанию отображаются в этом разделе);

б) *нормализация* – механизм разбора неоднородных данных с целью их приведения к удобному для обработки виду;

в) *корреляция* – механизм корреляции позволяет находить взаимосвязи между различными данными и обладает возможностью прогнозирования событий ИБ;

г) *агрегирование* – механизм, позволяющий группировать однотипные события вместе, что позволяет минимизировать количество повторяющихся строк;

д) *тип данных* – ключевое понятие системы, которое позволяет определять типы данных, объединяющих информацию, характеризующую события (в базовой поставке представлено более 50 типов данных);

е) *хранение* – хранение данных о событиях ИБ реализовано средствами MySQL. По требованию заказчика система может быть настроена для работы с СУБД PostgreSQL, MS SQL.

Обработка данных осуществляется в трех режимах:

1) в реальном масштабе времени;

2) архивная обработка, анализ;

3) прогнозирование инцидентов.

Типовая схема размещения логических элементов системы (модулей сбора, обработки, корреляции и хранения) приведена на рисунке.

Общая концепция SIEM подразумевает реализацию разнесенной территориальной системы, где все модули внутри нее независимы друг от друга и являются автономными объектами, за исключением головного сервера, через который происходит синхронизация модулей нижнего уровня.

Каждый объект из общей схемы работает как процессинговая машина. Далее перечислим имеющиеся в системе типы модулей.

1. *Сборщик («Воронка»)* – программный модуль, который позволяет собирать на себя данные с различных источников в сети. Является

как пассивным, так и активным участником сбора и получения данных. Каждый сборщик может удалено устанавливаться через головной модуль посредством графического интерфейса консоли.

2. *Нормализатор* – программный модуль, позволяющий преобразовывать данные из неоднородного формата в формат SIEM-системы (приведение к структуре данных). Каждый нормализатор может удаленно устанавливаться через головной модуль посредством графического интерфейса консоли. Конфигурирование модуля возможно любым из доступных способов.

3. *Коррелятор* – программный модуль, который занимается корреляцией событий в режиме реального времени. Является одним из ключевых элементов системы. Может быть установлен только в единичном экземпляре в одном периметре. Установка производится через головной модуль посредством графического интерфейса. Поддерживает различные комбинации настроек.

4. *База данных* – программный комплекс из СУБД MySQL, а также модуля агрегации и записи в базу данных. Представляет собой единую систему. Программный комплекс устанавливается в единичном экземпляре в рамках одного периметра.

5. *Головной модуль* – основной модуль для системной поддержки и обеспечения работы всех служб. Отвечает за служебные действия по реконфигурированию, удаленные установки, работу с API по отправке данных из системы и пр. Ставится в единичном экземпляре для всех периметров сети.

Система представляет собой территориально распределенный комплекс, который поддерживает любую комбинацию в рамках одного периметра сети. Данная реализация «сервера серверов» работает по технологиям репликации, а также приоретизированной отправки сообщений между нижним и верхним уровнем. Внутри системы поддерживается автоматическое построение сети, автобалансировщик нагрузки, перераспределение трафика по резервным каналам и пр.

Отказоустойчивость реализуется на модулях следующим образом:

а) *локальное хранилище* – в случае потери соединения до ближайшей точки, а также при отсутствии запасного канала в карте сети, данные будут сохраняться в локальное хранилище SQLlite (данная функция настраивается);

б) *переподключение* – в случае потери соединения с ближайшей точкой система автоматически будет пытаться переподключиться к предыдущей точке, или же, в случае если имеется запасной канал, – к этой же точке для восстановления работоспособности;

в) *автобалансировщик* – между сборщиками и нормализаторами встроена система автоматического перераспределения нагрузки: в случае, когда в пределах периметра имеется несколько нормализаторов, система автоматически будет перераспределять потоки на менее нагруженный сервер для балансировки средней нагрузки;

г) *автоматическое поднятие службы* – в случае отказа в обслуживании или выхода из строя система автоматически «поднимется» на машине;

д) *восстановление контрольной точки* – в случае сбоя службы или модифицирования клиента, который приводит к невозможности работы модуля, неэталонная копия автоматически удаляется из компьютера, а взамен нее скачивается и запускается эталонная версия с успешным конфигурационным файлом с головного сервера;

е) *проверка контрольной суммы* – конечная контрольная сумма каждого модуля проходит периодическую проверку с целью контроля целостности.

Система дополнительно поддерживает следующий функционал:

1) компрессия данных между модулями для уменьшения нагрузки на трафик сети;

2) шифрование данных при передаче между модулями (настраиваемый параметр);

3) возможность отправки данных с агентов (централизованно устанавливаемый компонент) по расписанию (актуален для работы с малым каналом связи).

Стандартный набор коннекторов включает в себя коннекторы к следующим источникам событий:

- контроль состояния Active Directory;

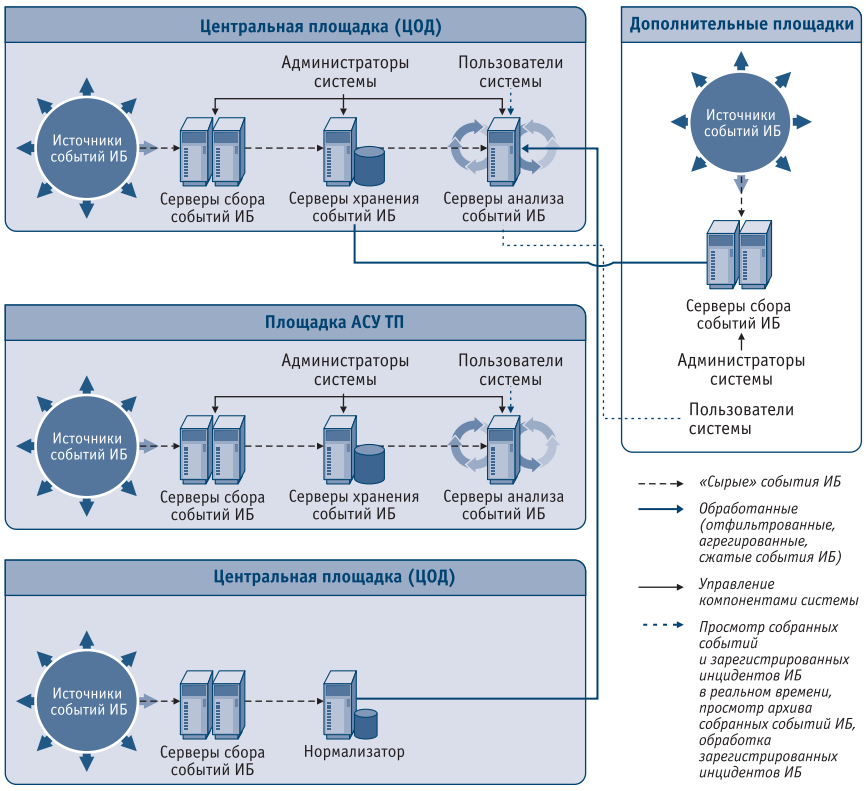

Рисунок. ***Типовая схема размещения логических элементов системы***

- контроль подключаемых съемных носителей (eToken, Rutoken);
- контроль подключённых клиентов;
- контроль запущенных процессов;
- контроль системного реестра;
- модуль работы с сообщениями SysLog;
- модуль работы с сообщениями протокола SNMP Trap;
- модуль работы с сообщениями протокола SMTP;
- модуль работы с событиями Active Directory ОС семейства Windows;
- сообщения, получаемые по протоколам Syslog и SNMP trap;
- события, получаемые от СЗИ от НСД Dallas Lock;
- события, получаемые от СЗИ от НСД Zlock;
- события, получаемые от СЗИ от НСД DeviceLock;
- события, получаемые от СЗИ от НСД «Блокхост»;
- события, получаемые от АВС Dr.Web;
- события, получаемые от линейки продуктов АВС «Kaspersky»;
- события, получаемые от МЭ и СОВ Cisco, Cisco ASA;
- события, получаемые от СУБД Oracle;
- события, получаемые от МЭ Check Point;
- события, получаемые от СКЗИ S-Terra;
- события, получаемые от IDM «Аванпост»;
- события, получаемые от SIEM ArcSight;
- события, получаемые от DLP Secure Tower;
- по отдельному запросу поставляются коннекторы для сбора событий от источников, производимых компаниями Siemens, General Electric, ABB, Alstom.

Security Capsule, в отличие от аналогичных SIEM, например ArcSight, имеет ряд существенных архитектурных отличий и преимуществ, определяемых логикой работы системы.

1. Прежде всего, Security Capsule имеет большой стандартный сертифицированный набор коннекторов, входящих в базовую конфигурацию, что позволяет разворачивать систему, не прибегая к необходимости разработки коннекторов, тестирования работоспособности коннекторов и ядра системы. При этом состав коннекторов может быть дополнен в зависимости от требований, предъявляемых к системе. В отличие от зарубежных аналогов, требующих разработки коннекторов с использованием средств разработки. Данный недостаток аналогов не позволяет убедительно утверждать о возможности реализации требуемых функций и механизмов, значительно увеличивает и усложняет процесс по сути внедрения и эксплуатации SIEM. Важным фактором является необходимость подтверждения соответствия в системе сертификации ФСТЭК России, например, через инспекционный контроль. Не требуется штата для обслуживания, настройки и сопровождения системы.

2. Security Capsule имеет сформированную базу данных, реализованную средствами СУБД MySQL. БД начинает заполняться данными о событиях безопасности сразу после установки, настройки и активации Security Capsule. Модель базы данных может быть изменена в соответствии с требованиями к системе.

3. Security Capsule построена с использованием клиент-серверной архитектуры. Установка и настройка клиентов реализуется удаленно. Клиенты осуществляют мониторинг и сбор событий ИБ, которые могут передаваться в режиме реального времени на сервер системы или, с целью уменьшения передаваемого трафика, по расписанию. При этом передаваемые данные защищаются криптографическими методами.

4. Не требуется штат программистов, способных разрабатывать модули и компоненты системы, включая коннекторы к источникам.

Серверный компонент имеет иерархическую структуру. Таким образом, мониторинг событий может осуществляться локально в территориально удаленных подразделениях, филиалах, дочерних и зависимых организациях. Первичная обработка событий ИБ осуществляется на локальных серверах; на центральный сервер передается либо полный состав событий ИБ, либо сформированный перечень критических событий и результаты анализа.

Перейдем к анализу событий. Последние подразделяются на события, относящиеся к ИБ ОС, к сетевым устройствам, к СЗИ от НСД, к СУБД и к прикладным системам. Каждому контролируемому событию или группе событий на этапе настройки системы присваивается определенный статус.

Сбор событий может быть непрерывным, дискретным с привязкой к системе единого времени, во временном интервале. События от различных источников могут быть сопоставлены по ряду критериев. Кроме того, они могут быть отсортированы, ранжированы и отфильтрованы по нескольким признакам. Администратор системы имеет возможность управлять правилами обработки событий.

Отдельно обрабатываются события, связанные с контролем учетных записей пользователей, включая создание, изменение, удаление, контроль прав доступа. Также обработке подлежат события, связанные с установкой/удалением общесистемного и прикладного ПО, средств защиты с использованием механизма контроля системного реестра.

Пользователи системы должны иметь опыт работы с ОС семейства Microsoft Windows 7 и последующих версий, Microsoft Windows Server 2008/2012 с поддержкой программной платформы Microsoft .NET Frame work 4.5.2, навыки установки базы данных MySQL.

Для установки, настройки и функционирования системы необходимо реализовать требования к программной среде (они приведены в табл. 2) и программно-техническим средствам.

Минимальные и рекомендуемые требования к программно-техническим средствам системы при ее функционировании в ЛВС (до 50 источников для сбора событий) приведены в табл. 3.

Данная конфигурация позволяет обрабатывать события со скоростью не менее 5000 EPS. Система может быть развернута на серверах в среде виртуализации.

Оптимальные требования к программно-техническим средствам для развертывания системы в макси-

мальной конфигурации приведены в табл. 4.

Проведение тестов на быстродействие требует качественно организованного подхода к получению данных. Для получения высокоточных результатов тестирования необходимо выделить следующие их группы:

- протокол взаимодействия;
- длина сообщения (количество байтов для обработки);
- качество написанного регулярного сообщения (быстродействие, учет бэктрекинга и т. д.);
- учет производительности аппаратного компонента.

Таблица 2. ***Требования к программной среде***

№ п/п	Программные средства	Примечание
1	ОС семейства Microsoft Windows 7 и последующие версии, Microsoft Windows Server 2008/2012	Операционная система
2	.NET Framework 4.5.2	Свободно распространяемое ПО устанавливается на всех ПЭВМ. Данное ПО является библиотекой плагинов для запуска и функционирования программ, написанных в среде «.NET»
3	MySQL Database Server 5.5	Свободно распространяемое ПО устанавливается на ПЭВМ, используемой в качестве сервера, который применяется как хранилище данных

Таблица 3. ***Минимальные и рекомендуемые требования к программно-техническим средствам системы***

№ п/п	Элемент	Минимальные требования	Рекомендуемые требования
1	Процессор	Intel X86/64 с частотой 1 ГГц или аналог	Intel X86 или X64 с частотой 1,2 ГГц и более или аналог
2	ОЗУ	2 Гб	8 Гб или более
3	Внешняя память для установки	200 Мб	200 Мб
4	Видеокарта	SVGA	
5	Монитор с разрешением экрана	800*600 dpi	1920*1080 dpi и более
6	Устройство чтения/записи компакт дисков и DVD		
7	Карта сетевая с поддержкой стандартов IEEE 802.3 10BaseT, IEEE 802.3u 100BaseTX		

Таблица 4. ***Оптимальные требования к программно-техническим средствам системы***

Назначение сервера	Количество	Системные требования	
Сервер анализа событий ИБ	1 шт.	Процессор	8 ядер
		ОЗУ (Гб)	64
		Диск (ТБ)	1
		ОС	Windows 2008 и выше
Сервер сбора событий ИБ	1 шт.	Процессор	4 ядра
		ОЗУ (Гб)	16
		Диск (ТБ)	1
		ОС	Windows 2008 и выше
Сервер хранения данных (БД MySQL)	1 шт.	Процессор	8 ядер
		ОЗУ (Гб)	64
		Диск (ТБ)	1
		ОС	*nix/Windows 2008 и выше
Система хранения данных для событий ИБ в течение одного года	1 шт.	Полезная ёмкость	Зависит от количества хранимых в архиве событий

Сформировав указанные первичные требования, необходимо произвести корректировку следующих вторичных показателей:

- первичная обработка данных на клиенте;
- распределенность системы для обработки;
- архитектура СПД и пропускная способность каналов;
- нормализация приходящих событий.

Оценив все перечисленные выше показатели, можно говорить уже о фактическом представлении показателя EPS (количества событий в секунду).

На наш взгляд, предоставляемые в массовом доступе данные о производительности далеко не в полной мере соответствуют объективным показателям. Обычно производители умалчивают о том, какие из перечисленных выше показателей были использованы при подсчете реального количества EPS в конечной обрабатываемой системе.

Тестирование проводится в двух режимах: при стрессовой и периодической нагрузке.

Стрессовый режим представляет собой тест по увеличению приходящих сообщений, например Syslog, до нахождения верхнего предела стабильной работы системы. Например, тест начинается при скорости 500 EPS с постепенным увеличением объема передаваемых сообщений, пока не определяется верхний предел скорости обработки данного ПК.

Периодическая нагрузка – это тест, моделирующий работу реального прототипа сервера (то есть с меняющимся уровнем загрузки, простоями и т. д.). Данный тест позволяет более качественно проверить нагрузку, максимально приближенную к реальному работающему прототипу.

Более подробно испытания системы будут рассмотрены в последующих публикациях.

ЛИТЕРАТУРА

1. Графов А. Ф. Развитие российских SIEM-систем: Security Capsule // Защита информации. Инсайд. – 2013. – № 5. – С. 84–86 .

2. Сайт проекта SIEM Analytics [Электронный ресурс]. – Режим доступа: http://siem.su, http://siem.guru.