I.E. Habarov, V.S. Oladko

The Program Complex Security Data Recorded by Means of Information Protection

Keywords: event log, threat, encryption.
In this paper the author analyzes the problem of data security breach of the events that are registered by means of information protection. Causes of security registration subsystems analyzed. The approach to data security, registered means of protection, based on a modification of SIEM proposed. A special feature is the addition of encryption and separating the components of the data collection and analysis of data recorded by means of protection. Program complex data security recorded means of protection designed. The client-server architecture and user interface are described.

И.Е. Хабаров, В.С. Оладько

ПРОГРАММНЫЙ КОМПЛЕКС ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ, РЕГИСТРИРУЕМЫХ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

В настоящее время для успешного функционирования любого предприятия необходимо обеспечивать безопасность бизнес-процессов и данных, обрабатываемых в информационной системе. Для решения данной проблемы существует большое количество готовых решений, направленных не только на активную и пассивную защиту информации, но и на выявление вторжений в систему, анализ событий и инцидентов происходящих в ней. Для этого вся информация, связанная с событиями и действиями, происходящими в системе, регистрируется средствами защиты информации и записывается в специальные журналы, которые используют в процессе управления инцидентами и при аудите информационной безопасности предприятия. При этом сами журналы регистрации событий также могут быть подвержены воздействиям злоумышленника с целью скрыть следы своего присутствия в системе. Следовательно, актуальны исследования, связанные с обеспечением защиты данных, регистрируемых подсистемами информационной безопасности предприятия.

Проблемы безопасности подсистем регистрации событий

Наиболее распространенными средствами защиты информации на предприятии являются программно-аппаратные. В процессе своей работы данные средства фиксируют и регистрируют информацию о происходящих событиях в специализированных журналах. К таким средствам относят:

антивирусные подсистемы;
межсетевые экраны;
системы обнаружения вторжения;
системы журналов операционных систем;
DLP-системы;
системы инвентаризации и др.

События, зарегистрированные в журналах данных средств, могут указывать на действие вредоносного программного обеспечения, различные аномалии в процессах или сетевом трафике, идентифицировать хосты, с которых была зафиксирована подо-

зрительная деятельность, а также объекты и ресурсы системы, на которые эта деятельность была направлена, и т.д.

Поскольку в журналах событий средств защиты информации регистрируется информация о событиях, аномалиях и инцидентах, происходящих в системе, то их следует регулярно просматривать и собирать записи для дальнейшего анализа. Анализируя информацию журналов регистрации, можно своевременно выявить вторжение в систему и минимизировать последствия и риски, связанные с атаками злоумышленника. При этом сами журналы и их данные также могут быть подвержены воздействиям злоумышленника и дестабилизирующих факторов случайного характера, которые могут привести к уничтожению журналов и искажению информации в них. Основные причины нарушения безопасности данных подсистем регистрации:

несанкционированное изменение, удаление записей о событиях в журналах событий;

несанкционированное удаление журналов регистрации событий;

несанкционированное копирование данных журналов регистрации;

ошибки при конфигурировании подсистем регистрации событий;

перехват данных при передаче и сборе информации с подсистем регистрации;

отказы и сбои в работе подсистем регистрации.

Таким образом, для предотвращения возможных угроз, связанных с нарушением безопасности подсистем регистрации, целесообразно использовать специализированные средства, обеспечивающие защиту данных регистрируемых средствами защиты информации, распределенными по ИС предприятия. Для решения данной задачи авторами был разработан программный комплекс, позволяющий осуществлять удаленный сбор данных регистрируемых различными средствами защиты ИС и обеспечивать их защищенную передачу и хранение.

Подход к обеспечению безопасности данных подсистем регистрации

Для обеспечения взаимодействия с подсистемами регистрации средств защиты, с целью последующей защиты их данных, при разработке программного комплекса в качестве основы была выбрана концепция функционирования системы управления журналами безопасности (SIEM), которая была подвергнута модификации. SIEM – система, имеющая привилегии в сборе и обрабатке информации о записях и состоянии журналов регистрации для последующего анализа. Информация, которая обрабатывается SIEM-системами, может собираться практически со всех средств, где существует регистрация поведения. Сбор данных у типовых SIEM-систем осуществляется с помощью специальных агентов, которые представляют собой программы, собирающие данные журналов и передающие их на выделенный сервер (рис. 1).

Анализ типовой архитектуры SIEM и литературных источников [1–4] показывает, что большинство SIEM присуще следующие недостатки:

1) данные, собранные с подсистем регистрации агентами передаются на сервер в открытом виде, что позволяет злоумышленнику перехватить их и(или) осуществить подмену;

2) база данных, центр управления и агенты сбора информации часто расположены на едином сервере, что делает систему уязвимой в случае сбоев и отказов программно-аппаратной части и(или) атаки злоумышленника;

3) требуют большого количества вычислительных ресурсов и создают высокую нагрузку на сеть, что повышает затраты и затрудняет для применение подобных систем на небольших предприятиях.

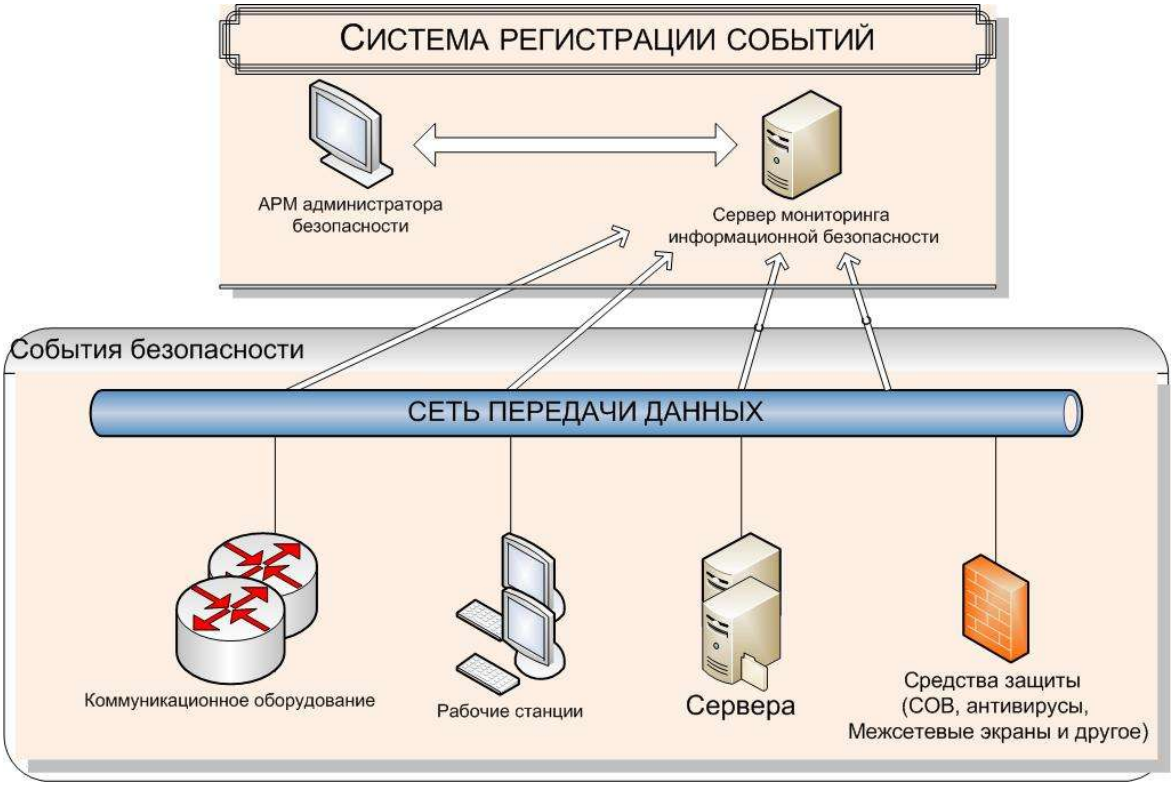

Рис 1. Компоненты SIEM-системы

Среди выделенных недостатков наибольшее значение с точки зрения информационной безопасности имеют первый и второй недостатки. Поскольку именно открытое хранение информации и передача сериализованных данных и отчетов от агентов на сервер предоставляют злоумышленнику возможность перехватить данные в сети, проанализировать и восстановить их, составив полную картину обо всех средствах обеспечения информационной безопасности на предприятии, функциональных подсистемах, событиях и отчетах об ошибках. Эти данные злоумышленник может использовать при проведении атак или для сокрытия своего присутствия и действий в системе. Поэтому для устранения выделенных недостатков предлагается модифицировать архитектуру SIEM посредством создания зашифрованного канала передачи регистрируемых данных из журналов событий средств защиты ИС, а также разделения и переноса центра управления от средств сбора информации с подсистем регистрации (рис. 2).

Таким образом, разработанный программный комплекс базируется на модифицированной архитектуре SIEM и обеспечивает:

сбор данных журналов событий из различных источников;

шифрование сериализованных данных, которые поступают от клиентов на сервер для обработки и анализа;

хранение собранной информации в зашифрованном виде базе данных;

анализ информации о событиях и инцидентах;

выдача отчетов.

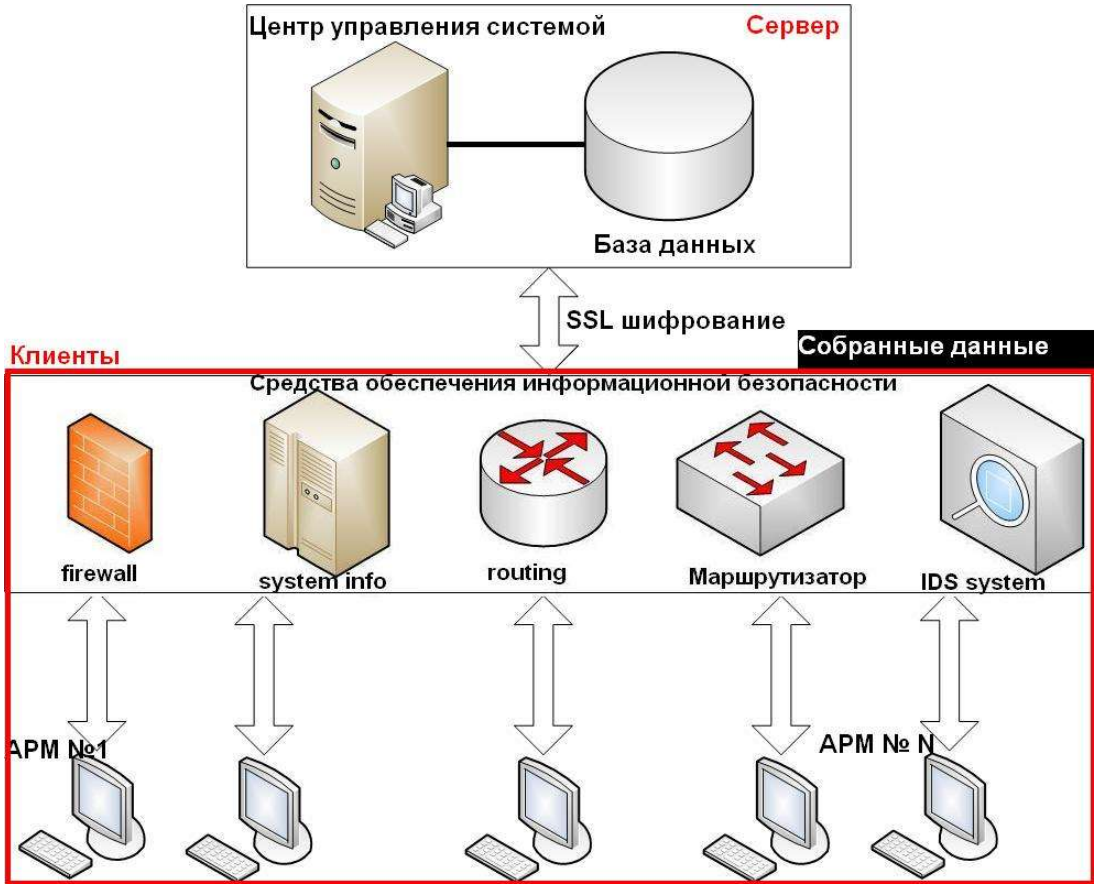

Рис. 2. Предлагаемая модификация SIEM

Архитектура программного комплекса

Разработанный программный комплекс обеспечения безопасности данных, регистрируемых средствами защиты информации, имеет клиент-серверную архитектуру (рис. 3).

Сервер осуществляет управление процессом сбора и защиты данных с подсистем регистрации, обеспечивает контроль над установкой SSL-соединения и передачей данных от клиентов в зашифрованном виде. Принимает множественные сообщения от установленных на компьютерах ИС клиентов, при этом команды управления и просмотра передаются автоматически без вмешательства пользователя. Также со стороны сервера можно просматривать базу данных событий, собранных с подсистем регистрации.

Каждый клиент устанавливается отдельно и отвечает за свой персональный компьютер ИС, при организации передачи собранных данных клиент предоставляет серверу такие идентификационные данные, как «Имя Компьютера», и сертификат. Каждый клиент представляет собой совокупность функциональных модулей сбора и передачи данных. Каждый отдельный модуль сбора данных отвечает за свой тип средства защиты, модуль антивирусной системы – за журналы антивируса, модули IDS – за сбор данных с журналов систем обнаружения вторжений и т.п. С целью более эффективного потребления ресурсов модули сбора не взаимодействуют друг с другом и работают в отдельных потоках. Модуль передачи подготавливает и сериализует собранные данные и инициирует запрос на передачу.

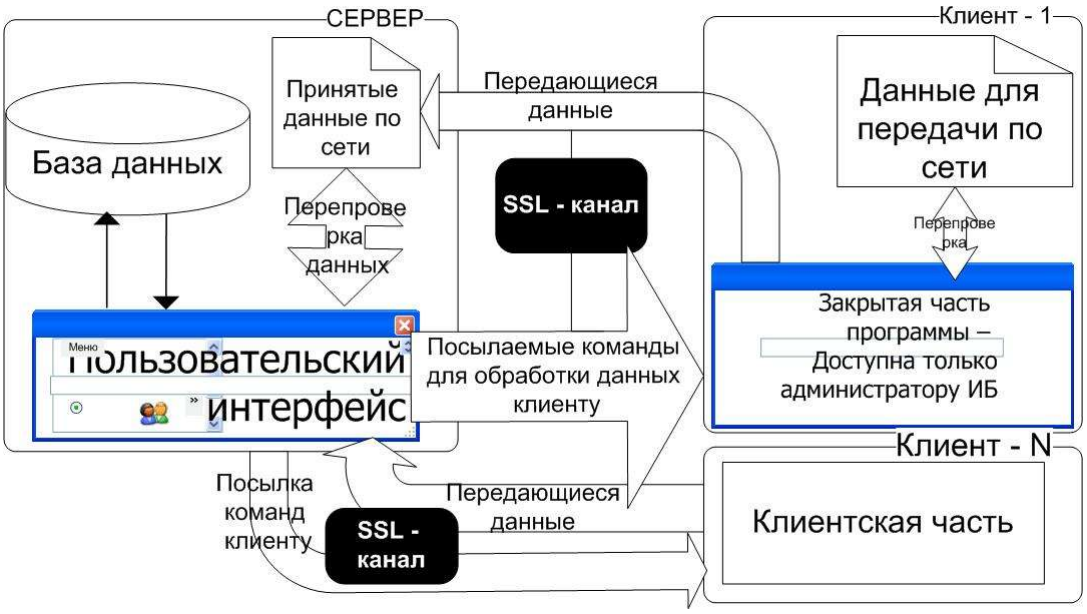

Рис. 3. Архитектура разработанного программного комплекса обеспечения безопасности данных, регистрируемых средствами защиты информации

База данных представляет собой совокупность табличных данных, содержащих информацию о собранных событиях из журналов средств защиты, которая используется сервером для подробного анализа инцидентов безопасности.

Пользовательский интерфейс (рис. 4) имеет графический вид и предназначен для взаимодействия пользователя с программным комплексом и позволяет конфигурировать параметры распределенного сбора данных, выводить отчет о работе и результаты анализа инцидентов на основании информации собранной с журналов событий.

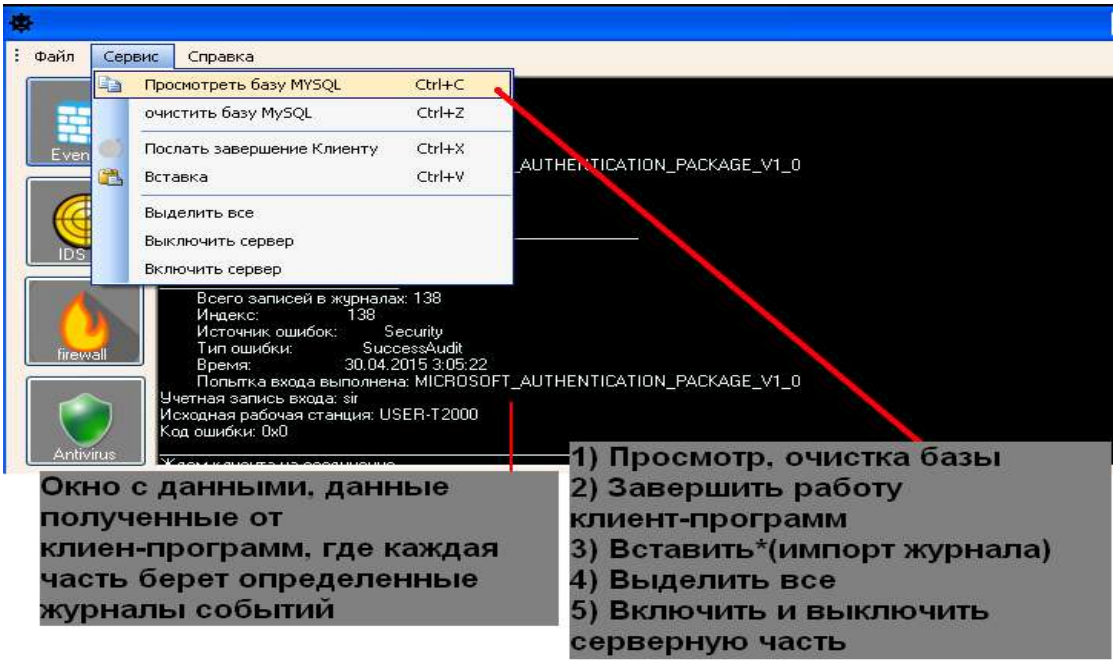

Рис. 4. Пользовательский интерфейс разработанного программного комплекса

На данной стадии разработки момент, прототип программного комплекса, работает с подсистемами регистрации таких средств защиты, как межсетевой экран, журналы событий ОС Windows и Linux, система обнаружения вторжений Snort, антивирус Comodo Antivirus. В дальнейшем планируются расширение функциональных возможностей программного комплекса и добавление взаимодействия с новыми средствами защиты.

Заключение

Разработанный программный комплекс можно применять для сбора и обеспечения защиты данных журналов регистрации средств защиты информации на малых предприятиях, а также в учебном процессе при обучении студентов по направлению информационная безопасность при проведении лабораторных работ в качестве стенда-макета.

СПИСОК ЛИТЕРАТУРЫ:

1. Новикова Е.С., Котенко И.В. Механизмы визуализации в SIEM-системах // Системы высокой доступности. 2012. Т. 8. № 2. С. 91–99.
2. Miller D., Harris S., Harpe A., VanDyke S. Security Information and Event Management (SIEM) Implementation // McGraw-Hill. 2010. P. 410.
3. Канаев А.Н. Мониторинг событий и обнаружение инцидентов информационной безопасности с использованием SIEM-систем // Международный студенческий научный вестник. 2015, № 3. С. 122–123.
4. Графов А.Ф. Развитие Российских SIEM-систем: Security Capsule//Защита информации. Inside 2013, № 5. С. 2–4.
5. Шелестова О. Что такое SIEM?//SecurityLab. URL: http://www.securitylab.ru/analytics/430777.php (дата обращения 10.08.2015).

REFERENCE:

1. Novikova Ye.S., Kotenko I.V. Mekhanizmy vizualizatsii v Siyem - sistemakh // Sistemy vysokoy dostupnosti. 2012. T. 8. № 2. S. 91–99.
2. Miller D., Kharris S., Arp A., VanDyke S. Informatsionnaya bezopasnost' i upravleniye sobytiyami (SIEM) osushchestvleniye // McGraw-Hill. 2010. P. 410.
3. Kanayev A.N. Monitoring sobytiy i obnaruzheniye intsidentov informatsionnoy bezopasnosti s ispol'zovaniyem SIEM - sistem // Mezhdunarodnyy studencheskiy nauchnyy vestnik. 2015, № 3. S. 122-123.
4. Grafov A.F. Razvitiye Rossiyskikh SIEM-sistem: Bezopasnost' Kapsula // Zashchita informatsii. Inside. 2013, № 5. S. 2–4.
5. Shelestova O. Chto takoye SIEM? // SecurityLab.URL: http://www.securitylab.ru/analytics/430777.php (data obrashcheniya 10.08.2015).