Развитие российских SIEM-систем: Security Capsule

Предпосылкой для публикации данной статьи явились приказы ФСТЭК России № 17 от 11.02.2013 и № 21 от 18.02.2013, а также обзоры SIEM-систем, опубликованные в ряде печатных и электронных средств массовой информации.

Традиционный обзор SIEM-систем в российской прессе предполагает описание и анализ функциональных возможностей некоторого количества продуктов зарубежныхразработчиков в силу того, что отечественные аналоги малоизвестны. В данной статье рассматривается опыт создания, сертификации и применения, пожалуй, первой отечественной сертифицированной SIEM-системы «Программно-аппаратный комплекс администратора безопасности».

А. Ф. Графов

Программно-аппаратный комплекс администратора безопасности (ПАКАБ) предназначен для регистрации и учета событий информационной безопасности в информационно-вычислительных сетях, разграничения доступа к информационным ресурсам и обеспечения контроля целостности файлов.

Пользователями комплекса являются:

- администраторы сети и информационных систем;
- администраторы безопасности;
- руководители подразделений по безопасности;
- разработчики систем информационной безопасности;
- разработчики информационных систем;
- руководители компаний.

Прототипом ПАКАБ является ПО «Автоматизированное рабочее место администратора безопасности» (АРМ АБ). Первые проекты по разработке и внедрению АРМ АБ были выполнены в период с 2003 по 2005 годы.

АРМ АБ был интегрирован в системы управления сетями связи и цифровые учрежденческо-производственные автоматические телефонные станции (УПАТС) оперативно-технологических (ОТС) и общетехнологических (ОбТС) видов связи, прежде всего, на полигонах железных дорог (МПС России и впоследствии ОАО «РЖД»). Необходимость создания специализированного программного средства мониторинга и анализа событий ИБ для систем управления сетями связи была вызвана следующими факторами:

- переходом на цифровые виды связи с коммутацией пакетов;
- необходимостью обеспечения безопасности информации, прежде всего от несанкционированного доступа (НДВ) и недекларированных возможностей (НДВ).

Данный период характеризовался отсутствием специалистов по информационной безопасности в связной отрасли и, как следствие, недопониманием актуальности этих вопросов для обеспечения надежной связи, а также большим количеством разнообразных неоднородных средств защиты от НСД.

Архитектура АРМ АБ основывалась на клиент-серверной технологии. Сбор, передача и обработка данных (событий информационной безопасности) были реализованы на основе применения протокола SNMP. Решение проблемы сбора и передачи данных о событиях ИБ потребовало доработки систем управления сетями связи и УПАТС. В работах участвовали специалисты служб связи и вычислительной техники ОАО «РЖД» (МПС России), ОАО «Дирекция по строительству сетей связи» – филиала ОАО «РЖД», а также лидеры отрасли, такие как ЗАО «Информтехника и Промсвязь» (Москва), ЗАО «Интелсет» (Санкт-Петербург), ОАО «Морион» (Пермь).

При помощи АРМ АБ были решены следующие основные задачи:

- сбор, передача, обработка и хранение данных о событиях информационной безопасности;
- анализ событий;
- принятие решения по событию;
- контроль действий эксплуатирующего персонала;
- обеспечена автоматизация мониторинга и анализа событий администраторов ОТС и ОбТС;

- разработка и предоставление отчетов о событиях ИБ;
- анализ статистики событий ИБ.

Сбор данных о событиях ИБ осуществлялся с установленных средств защиты от НСД (СЗИ от НСД), журналов ОС (OS Windows, Linux), прикладного ПО систем управления сетями связи.

Таким образом, можно сделать вывод о том, что в АРМ АБ впервые были реализованы основные функции SIEM-системы.

Программно-аппаратный комплекс администратора безопасности (ПАКАБ) и его коммерческая версия Security Capsule явились логическим продолжением развития SIEM-систем.

Security Capsule основывается на клиент-серверной технологии. Для сбора и обмена данными используются программные модули, реализующие SNMP- и Syslog-протоколы.

Security Capsule (ПАКАБ) имеет модульную архитектуру (рис. 1), включающую в себя:

- модуль серверной части;
- модуль мониторинга и администрирования;
- центральный модуль;
- клиентские модули;
- коннекторы.

Ядро системы образуют модули серверной и клиентской частей, поставляющиеся в виде дистрибутива (рис. 2). Основным преимуществом Security Capsule по сравнению с зарубежными аналогами является наличие возможности обрабатывать события от следующих источников:

- СЗИ от НСД;
- e Token;
- антивирусные программы;
- журналы ОС Windows и Linux;
- межсетевые экраны;
- маршрутизирующее оборудование;
- СУБД SQL, Oracle;
- прикладные информационные системы.

При необходимости обработки данных от нестандартных для Security Capsule источников разрабатывается коннектор под требуемый источник, что не влечет за собой значительных временных ифинансовых затрат, а также изменения технологии функционирования ИС. Идея

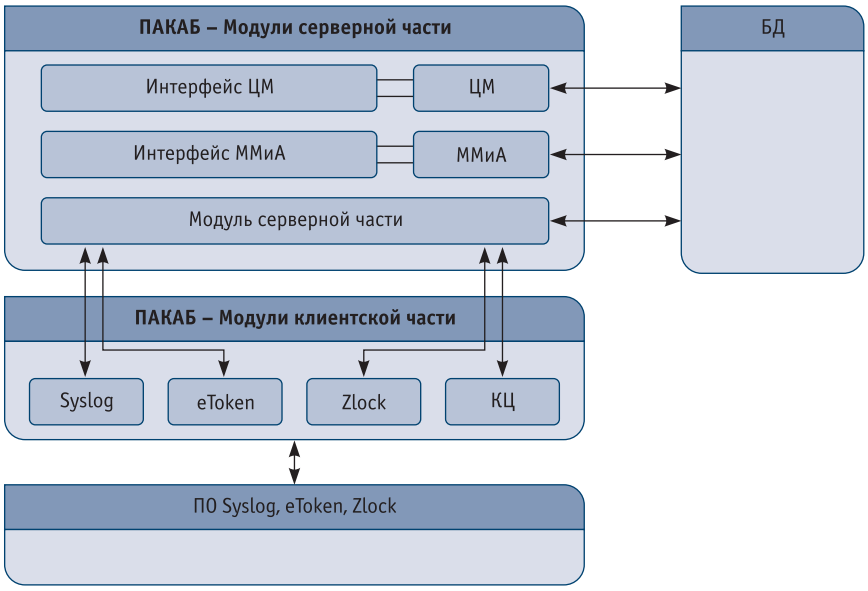

Рис. 1. ***Архитектура Security Capsule***

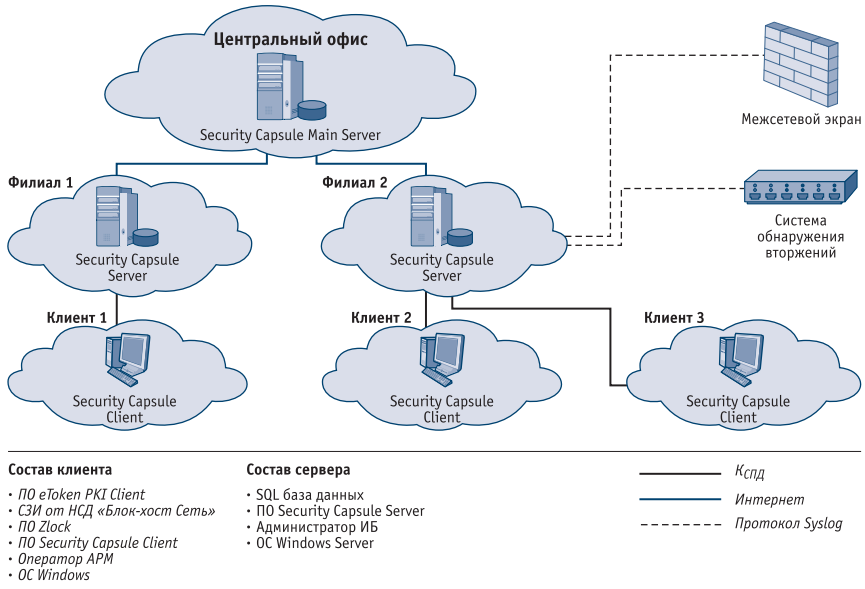

Рис. 2. ***Ядро системы***

не нова. Данный подход широко используется известными производителями информационных систем, например Oracle.

Security Capsule имеет иерархическую структуру. С целью снижения нагрузки на сеть передачи данных первичная обработка событий осуществляется на серверах Security Capsule. В зависимости от степени важности и критичности информация о событиях ИБ передается на серверы более высокого уровня. С целью снижения трафика информация на серверы более высокого уровня передается по расписанию, как правило, во время наименьшей нагрузки на СПД. Критические события передаются в режиме реального времени.

Важнейшим модулем системы является модуль обработки и отображения информации о событиях, формирования отчетов. Администраторы системы имеет возможность самостоятельно, в соответствии с требованиями политики информационной безопасности, определять перечень контролируемых событий, выбирая из базового набора, требуемый. Уровень критичности контролируемых событий администратор может устанавливать в соответствии с политикой безопасности.

Данный модуль обладает функцией контроля за реакцией на собы-

НОВОСТИ

тия, с возможностью персонального контроля за действиями администраторов.

ПАКАБ обладает сертификатом ФСТЭК Росси № 2705 от 07.09.2012. Средствами ПАКАБ (Security Capsule) реализуется подсистема мониторинга и анализа событий (требование приказов ФСТЭК России № 17 от 11.02.2013 и № 21 от 18.02.2013), включая следующие функции:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- генерирование временных меток и (или) синхронизация системного времени в информационной системе;
- защиту информации о событиях безопасности.

ПАКАБ (Security Capsule) имеет более чем успешную трехлетнюю историю внедрения и эксплуатации как в ЛВС, так и в неоднородных территориально распределенных информационных системах, построенных на различных платформах, например ОС Windows, Linux, Oracle. Заказчиками комплекса в разные годы являлись предприятия и организации ОАО «РЖД», компании ОАО «Интер РАО ЕС», компании ОАО «Газпром», медицинские учреждения Ханты-Мансийского автономного округа (ХМАО). Количество инсталляций превысило показатель в 6000 для клиентских мест. Комплекс интегрирован не только в СЗ конфиденциальной информации и ИСПДн, но и в прикладные информационные системы.

ПАКАБ (Security Capsule) – постоянно развивающаяся система, учитывающая опыт внедрения и эксплуатации комплекса. В ближайшее время состав комплекса дополнится сертифицированными модулями криптографии и дополнительными коннекторами. По мере развития набор коннекторов постоянно расширяется. Разработчики системы создали развитую систему технической поддержки. Обучение основам работы с комплексом организовано в рамках курсов повышения квалификации БГТУ, ГУСЭ. Углубленное изучение архитектуры, эксплуатации и сопровождения организовано как на базе ООО «Инновационные технологии в бизнесе» (www.itb.spb.ru), так и на территории заказчиков при внедрении и дальнейшее эксплуатации.

ПАКАБ (Security Capsule) поставляется в комплекте, включающем в себя сервер, дистрибутивы с серверным программным обеспечением, а также клиентское ПО. Стоимость поставки, установки и настройки зависит от состава и архитектуры ИС. Более подробную информацию можно получить у разработчика и поставщика комплекса.

Таким образом, по своим функциональным возможностям ПАКАБ (Security Capsule) является полноценной SIEM-системой, обладающей следующими преимуществами:

- наличием сертификата ФСТЭК России в Системе сертификации средств защиты информации;
- соответствием в полном объеме требованиям ФЗ № 152 «О персональных данных» от 27.07.2006, Постановлению Правительства РФ от 01.11.2012 № 1119, Приказам ФСТЭК России № 17 от 11.02.2013 и № 21 от 18.02.2013;
- наличием расширенного набора коннекторов, позволяющих подключать различные средства защиты информации, сертифицированные ФСТЭК России;
- возможностью расширения базового набора коннекторов;
- простотой установки, настройки и эксплуатации;
- невысокой стоимостью владения по сравнению с аналогичными системами.