УДК 004.056

В.А. Пиков[1]
М.В. Басангов[2]

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ. ПРИМЕНЕНИЕ SIEM-СИСТЕМ ДЛЯ АНАЛИЗА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СЛАЙС-ТЕХНОЛОГИИ В SIEM РОССИЙСКОГО ПРОИЗВОДСТВА

V.A. Pikov
M.V. Basangov

ACTUAL PROBLEMS OF INFORMATION SECURITY IN MODERN INFORMATION SYSTEMS. THE USE OF SIEM-SYSTEMS TO ANALYZE THE STATE OF INFORMATION SECURITY. THE PROSPECTS FOR USE OF SLICE-TECHNOLOGIES IN THE RUSSIAN PRODUCTION SIEM

Различные информационные системы (далее – ИС) активно входят в нашу жизнь, являясь важнейшими компонентами становления информационного общества в современной России. ИТ-инфраструктура государственных учреждений и коммерческих организаций весьма разнообразна. Одна из приоритетных задач таких систем – обеспечить максимально защищенную информационную поддержку процессов принятия управленческих решений с помощью электронных документов, имеющих юридическую силу. Остро стоит вопрос защиты информации в электронном документообороте. С развитием высоких технологий главной проблемой построения защиты стало не отсутствие информации, а ее обработка. Число активных источников, обеспечивающих поступление актуальной информации по текущему состоянию защищенности, непрерывно растет.

Анализ имеющихся ИС показал, что информационная безопасность в них обеспечивается реализацией множества требований по защите информации в виде совокупности программных и технических средств защиты информации и процессов ее обработки от доступа нелегитимных пользователей и процессов, а также множеством внедренных организационных мер. Наблюдается постоянный процесс адаптации и развития систем защиты к новым видам угроз. Растет с каждым днем и количество источников информации, из которых поступают данные по текущему состоянию защищенности. Ввиду сложности и, часто, распределенной структуры современной информационной системы, невозможно уследить за общей картиной происходящего в ней, а тем более – прогнозировать дальнейшие тренды [2, с. 9].

Важно своевременно реагировать на возникающие угрозы и предотвращать их появление. Необходим инструмент для анализа событий

[1] Доцент кафедры информационных технологий и естественно-научных дисциплин АНО ВО «Российский новый университет», начальник отдела программирования Управления (разработки и внедрения программно-аппаратных комплексов систем управления Военно-воздушных сил) Центрального научно-исследовательского института Военно-воздушных сил Министерства обороны Российской Федерации.

[2] Начальник службы – помощник начальника института по защите государственной тайны Центрального научно-исследовательского института Военно-воздушных сил Министерства обороны Российской Федерации.

информационной безопасности, разбора произошедших инцидентов.

Для решения этой проблемы около десяти лет назад появились системы Security Information and Event Management (SIEM) – системы управления событиями информационной безопасности. Системы SIEM занимаются сбором, анализом и визуализацией информации от сетевых устройств, различных устройств безопасности, приложений идентификации и управления учетными данными, доступом, инструментов поддержания политик безопасности и отслеживания уязвимостей, мониторинга операционных систем, систем управления базами данных и журналов приложений, а также сведений о внешних угрозах.

SIEM-системы, как и многие другие продукты, появились в результате эволюционного развития и последующего слияния систем SEM и SIM.

SEM (Security Event Management) – системы, действующие в режиме, приближенном к реальному времени. Для этого им требуется: автоматический мониторинг событий, их сбор, корреляция, генерация предупреждающих сообщений.

SIM (Security Information Management) – системы, анализирующие в свою очередь накопленную информацию со стороны статистики, различных отклонений от «нормального поведения» и т.д.

Когда же возможности SIM и SEM объединяются в рамках одного продукта, говорят о SIEM-системах. Исходя из этого, можно дать «литературный» перевод аббревиатуры SIEM – системы сбора и корреляции событий информационной безопасности.

Как правило, SIEM-система состоит из следующих компонентов:

• средство сбора данных (программные или аппаратные агенты сбора информации из различных источников);

• средства хранения собранной информации (сервер баз данных);

• средства обработки и анализа (сервер корреляции);

• средства управления и мониторинга системы, формирования уведомлений и отчетов [3, с. 23].

SIEM-системы могут использовать следующие источники информации:

• Access Control, Authentication. Применяются для мониторинга контроля доступа к информационным системам и использования привилегий.

• DLP-системы. Сведения о попытках инсайдерских утечек, нарушении прав доступа.

• IDS/IPS-системы. Несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам.

• Антивирусные приложения. Генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде.

• Журналы событий серверов и рабочих станций. Применяются для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности.

• Межсетевые экраны. Сведения об атаках, вредоносном ПО.

• Сетевое активное оборудование. Используется для контроля доступа, учета сетевого трафика.

• Сканеры уязвимостей. Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры.

• Системы инвентаризации и Software Asset Management (SAM). Поставляют данные для контроля активов в ИТ-инфраструктуре.

• Системы веб-фильтрации. Предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов.

На данный момент на рынке России лидируют следующие системы управления информационной безопасностью:

• IBM QRadar SIEM;
• HP ArcSight;
• Tibco Loglogic;
• McAfee NitroSecurity;
• Symantec SSIM;
• RSA Envision;
• Splunk;
• LogRhythm;
• «НПО «Эшелон» КОМРАД;
• OSSIM.

Все вышеперечисленные системы, обладая встроенной логикой и имея возможность задавать правила обработки вручную, являются, по сути, «вещью в себе». Так или иначе в них реализованы триггеры, счетчики, наборы условий и соответствующие сценарии поведения. Опыт практического использования современных ИС показывает, что необходимо отдельное автоматизированное рабочее место (далее – АРМ) администратора информационной безопасности (далее – АРМ АИБ). Для мгновенного понимания состояния системы важен вывод текущего состояния в режиме информационного стенда (табло), на который выводится графическая интерпретация «ядра» проблемы. В настоящий момент не существует SIEM-системы, способной к

подобному комплексированию, систематизации и представлению разнородного информационного массива, который ежесекундно генерирует программные или аппаратные агенты сбора информации.

Только создание – на волне повсеместного импортозамещения – российского программного продукта (SIEM-системы) на основе Системной теории авторефлексии с применением явления переноса проблемно-понятийных представлений для построения «Ориентированного организованного пространства проблемно-понятийных представлений» (далее – слайс-технологии), позволит избежать недостатков импортных аналогов [1–2].

Вышеупомянутая система имеет 30-летнюю историю, в частности – она является методологической и технологической основой объектов загоризонтной локации. В настоящий момент авторефлексивный системный анализ широко применяется в различных направлениях фундаментальных, прикладных, природоведческих и гуманитарных наук. Интересным представляется применение системы при работе с разнородными потоками информации, ситуационном анализе и прогнозировании: выявлении сути проблемы, определении потенциала, траекторий и горизонта развития, выявлении нетривиальных эффектов.

С помощью слайс-технологии можно формализовать процесс трансдисциплинарного исследования путем агрегирования в авторефлексивном пространстве результатов слайс-анализа отдельных дисциплинарных задач и последующего переноса представлений. Временные процессы, происходящие в различных местах информационной системы, в авторефлексивном пространстве представляются пучками некоторых траекторий, среди которых требуется найти оптимальную, в соответствии с принципом максимума (принцип Понтрягина Л.С.). Отображение «Образа безопасности системы» на информационном стенде АРМ АИБ в виде динамической геометрической фигуры (на плоскости и в пространстве) будет являться наиважнейшим элементом мониторинга ключевых показателей состояния защищенности ИС, а определение траекторий развития системы – средством прогнозирования.

Литература

1. Нагих В.Н., Нагих М.В., Карпухин А.И. Слайс-технология: методологические основы. – М. : Издательство «Полиграфический центр ИНЭК», 2015. – 40 с.

2. Грибунин В.Г. Комплексная система защиты информации на предприятии. – М. : Академия, 2009.

3. ГОСТ 50.922-96. Стандартизированные термины и определения в области защиты информации.

4. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

5. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информатизацию. Общие положения.