Применение отечественных технологий для мониторинга информационной безопасности в условиях импортозамещения

En **Utilization of Domestic Technologies for Monitoring Information Security in the Context of Import Substitution**

A. V. Dorofeev,
General Director
ad@cnpo.ru
Echelon Training Center

A. S. Markov,
PhD (Eng., Grand Doctor), Full Professor
a.markov@bmstu.ru
Bauman Moscow State Technical University

The purpose of the paper is to illustrate the possibility of ensuring the technological independence of the country in solving the problems of IS monitoring. The normative and methodological bases of IS monitoring are considered. Definitions of modern and promising technologies used in IS monitoring are given. Global trends and evolution of monitoring centers are shown. The pragmatic moments of the choosing a monitoring center are noted. The conclusion about the demand for monitoring centers for small and medium businesses is made. Solutions, which allow to realize an IS monitoring center according to the «nothing more» principle in the medium-sized organizations, are shown. The advantages of the proposed solutions are noted.

Keywords: cyber security, situation center, SIEM, threat analysis, incident management, vulnerability management, threat hunting, firewall, NTA

УДК 004.056

Цель работы состоит в иллюстрировании возможности обеспечения технологической независимости страны при решении задач мониторинга информационной безопасности. Рассмотрены нормативно-методические основы мониторинга информационной безопасности. Представлена классификация центров мониторинга информационной безопасности. Даны определения современных и перспективных технологий, используемых при мониторинге информационной безопасности. Показаны мировые тенденции и эволюция центров мониторинга. Отмечены прагматические моменты выбора центра мониторинга. Сделан вывод о востребованности центров мониторинга для малого и среднего бизнеса. Показаны технологические решения, позволяющие реализовать центр мониторинга информационной безопасности по принципу «ничего лишнего» в организациях среднего размера. Отмечены преимущества предложенных решений. Сделан вывод о возможности решения проблемы технологического суверенитета страны.

Ключевые слова: кибербезопасность, ситуационный центр, мониторинг событий, анализ угроз, управление инцидентами, управление уязвимостями, поиск угроз, межсетевое экранирование, глубокий анализ трафика

Александр Владимирович Дорофеев,
генеральный директор
ad@cnpo.ru
АО «Эшелон Технологии»

Алексей Сергеевич Марков,
доктор технических наук, профессор
a.markov@bmstu.ru
МГТУ им. Н. Э. Баумана

Введение

Внимание к теме мониторинга информационной безопасности (ИБ) обусловлено рядом причин. В первую очередь, это предопределено колоссальным объемом событий безопасности в сети, которые необходимо отслеживать, анализировать, а также реагировать на таковые в случае подозрения на исходящую от них опасность [1]. При этом отмечается рост числа событий безопасности, относящихся к маскируемым и сложным в идентификации целенаправленным атакам. Во-вторых, область мониторинга ИБ находится в сфере государственного регулирования, что выражается, например, в следующем:

- сформирована и активно развивается Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА);

- деятельность по мониторингу ИБ подлежит лицензированию, а также формируется система аккредитации центров мониторинга ГосСОПКА;
- требования по безопасности информации к защищаемым информационным системам обязательно включают меры в части мониторинга ИБ.

Реализационные вопросы мониторинга ИБ в настоящее время рассматриваются не только с точки зрения ухода с российского рынка поставщиков высокотехнологических решений, платформ и комплектующих, но и с точки зрения их возможной избыточности, к примеру, востребованности вообще или затратности относительно результативности решаемых организацией задач.

Хотя сейчас активно обсуждаются решения по построению больших центров мониторинга ИБ, где прямо или косвенно задействованы сотни и тысячи специалистов [2, 3], задачи мониторинга актуальны практически для любой организации, представляющей крупный и средний бизнес-сегменты. Это делает актуальным появление решений, не требовательных к аппаратным мощностям и, разумеется, функционирующих в отечественных защищенных операционных средах. Демонстрация одного из подобных решений и составляет цель статьи. В ее начале мы кратко вспомним нормативные требования, терминологические аспекты мониторинга ИБ, коснемся задач и классификаций центров мониторинга, а также современных тенденций.

Нормативно-методическая база мониторинга

В нашей стране активное развитие систем, центров и групп мониторинга ИБ связывают с Указом Президента от 15 января 2013 года РФ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и Федеральным законом от 26 июля 2017 года 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», ознаменовавшими реализацию государственной системы мониторинга (ГосСОПКА), собирающей данные о киберинцидентах от объектов КИИ РФ [4–6]. Кроме того, с 1 сентября 2022 года взаимодействовать с ГосСОПКА обязаны операторы ИСПДн. Построение ГосСОПКА регламентировано рядом известных приказов ФСБ России. УК РФ и КоАП дополнены соответствующими статьями на случаи саботажа и нарушений.

С 2018 года в стране активно функционирует государственный центр мониторинга – Национальный координационный центр по компьютерным инцидентам (НКЦКИ). В настоящее время формируются требования по аккредитации центров мониторингов ГосСОПКА согласно Указу Президента РФ от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Как лицензионный вид деятельности оказание услуг по мониторингу ИБ средств и систем информатизации существует с 2017 года (на основании Постановления Правительства РФ от 15 июня 2016 года № 541 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности»). Авторам публикации посчастливилось стать первыми в стране, получившими данный вид лицензии на организацию! В настоящее время в реестре ФСТЭК России числятся уже 240 организаций, имеющих право на предоставление указанного сервиса.

Что касается требований к подсистемам мониторинга информационных систем (ИС), то они определены в той или иной степени во всех приказах ФСТЭК России по различным защищаемым информационным системам: ГИС, АСУ ТП, ИСПДн, КИИ РФ и др. (в части подсистем «РСБ», «АУД»). Добавим, что мониторинг является базовой функцией любой подсистемы безопасности ИС, представленной в качестве контрмеры ИБ во многих популярных международных документах, например, FISMA, PCI DSS, GDPR, HIPAA, SOX, FERPA.

В плане импортозамещения напомним, что к концу 2024 года Указом Президента РФ № 250 запрещено использовать средства защиты информации, произведенные в недружественных странах. В реальности иностранные средства защиты информации сейчас не сертифицируются по ряду причин, что и вовсе делает их применение нелегитимным. Кроме того, на значимых объектах КИИ РФ любое программное обеспечение должно быть российским и включенным в Единый реестр отечественного программного обеспечения или ЕАЭС. Заметим, что здесь остается «серая зона» – компоненты open source, однако ограничения на их применение будут расширяться с развитием доверенных российских репозиториев в текущем году.

Центры мониторинга информационной безопасности

Как отмечалось нами ранее, в современной информационно-коммуникационной сети происходит гигантское количество событий, потенциально коррелированных с обеспечением безопасности, а оперативным центром их обнаружения, анализа и реагирования с целью выявления, расследования и устранения инцидентов безопасности является особое подразделение организации, именуемое *центром мониторинга ИБ* (Security Operations Center). Из определения видно, что его технологическим ядром является система управления событиями и ИБ: SIEM (Security Information and Event Management) [7–11]. Сделаем ремарку относительно так называемых *групп реагирования на компьютерные инциденты*, таких как CERT/CSIRT, представляющих собой организационные структуры, ориентированные на решение стратегических государственных или корпоративных задач ситуационного анализа и реагирования в области кибербезопасности и строящие работу, в том числе, на базе центров мониторинга ИБ [12]. Есть сообщества и объединения, например, CERT FIRST и Trusted Introducer. Примерами групп реагирования в нашей стране являются НКЦКИ и ФинЦЕРТ.

Современные центры мониторинга ИБ различают следующим образом:

- по операционной модели:
  - внутренние или внешние, а также гибридные;
  - централизованные (в том числе иерархические) и децентрализованные;
  - национальные, ведомственные, корпоративные;
- по масштабу (сколько сотрудников задействовано, сколько систем контролируется);
- по уровню зрелости (какие реализуются процессы и технологии, помимо SIEM);
- по форме реализации: стационарные, мобильные, виртуальные.

Как правило, при построении центра мониторинга ИБ первым вопросом является выбор его операционной модели, а именно: делать его собственным или передать сторонней организации, оказывающей соответствующие услуги. Понятно, что передача чувствительных данных внешней стороне вызывает много сомнений, но, с другой стороны, есть ряд узкопрофессиональных задач, которые целесообразно передать на аутсорсинг: например, компьютерная криминалистика или слепое тестирование на проникновение. Согласно Gartner, к 2025 году 90 % центров мониторинга в развитых странах будут использовать гибридную модель, передавая на аутсорсинг не менее 50 % операционной нагрузки. Собственно, выбор модели и решаемые задачи определяют масштаб центра мониторинга, то есть количество сотрудников, задействованных в его работе (тысяча, сотни, десятки, пара человек, совместитель).

В отношении потенциала центров мониторинга имеется ряд корпоративных взглядов, касающихся интуитивной привязки такого центра к модели зрелости COBIT, к средствам автоматизации или используемым инновационным технологиям [2, 3, 13, 14]. На взгляд авторов, имеет смысл, в первую очередь, принять во внимание целевые факторы ИБ, в данном случае – степень сложности атак (рис. 1). Такое представление позволяет использовать модель угроз организации с целью приоритизации организационных и технических мер ИБ.

В академической литературе выделяют следующие логические составляющие центра мониторинга: *персонал* (ответственное лицо и команда), *процессы* (документы, процедуры), *технологии* (и средства их реализующие) и др. [2].

Персонал обычно включает руководителей центра мониторинга и службы ИБ, аналитиков ИБ, архитектора ИБ. В крупных центрах мониторинга выделяют аналитиков нескольких линий. Например, аналитик 1-й линии анализирует оповещения о событиях ИБ, формирует карточку инцидента, конфигурирует инструментарий мониторинга. Аналитик 2-й линии анализирует срабатывания, подтвержденные аналитиком 1-й линии, проводит атрибуцию атаки, ее вектор и поверхность. Аналитик 3-й линии детально расследует критические неприятности и т. д. К области персонала также относят режимы работы центра: 7/24, 5/8 и т. д.

Что касается *процессов*, то обычно они связаны с основными функциональными задачами центра мониторинга ИБ, такими как:

- мониторинг источников событий;
- анализ угроз (Cyber Threat Intelligence);
- управление инцидентами (Incident Management);
- реагирование на инциденты (Incident Response);
- управление уязвимостями (Vulnerability Management);
- поиск угроз (Threat Hunting).

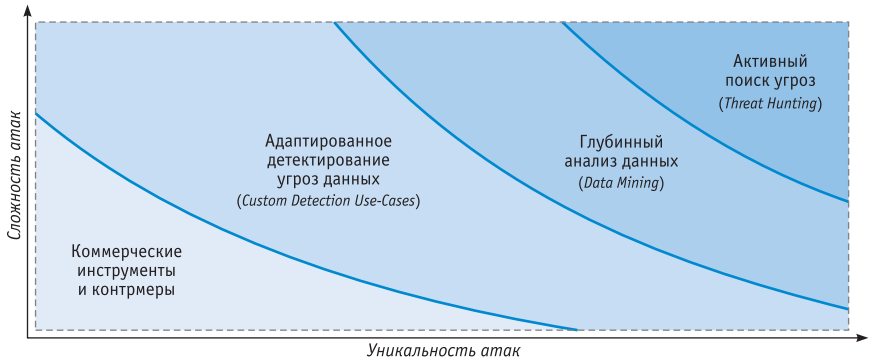
Отметим, что все указанные процессы стандартизированы и подкреплены «лучшими практиками», к примеру:

- ISO/IEC 27002:2022 регламентирует функции 1, 2, 4, 5 как контрмеры (controls 8.6, 5.7, 5.6, 8.8 и др.);
- ГОСТ Р 59709 и ISO/IEC 27035 дают дефиниции функциям 1, 3, 4;
- документ NIST SP 800-53 Rev. 5 (2020) регламентирует функцию 6 как контрмеру (control RA-10).

Ряд подзадач мониторинга описаны в ГОСТ Р 59547, ГОСТ Р 59548, ГОСТ Р 59710, ГОСТ Р 59711 и др. При необходимости важно следовать методическим документам НКЦКИ, также полезно посмотреть NIST SP 800-61, ENISA CSIRT Setting Up Guide и ISACA Incident Management and Response.

Итак, под *мониторингом информационной безопасности* обычно понимают процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений, угроз и уязвимостей. При этом, согласно ГОСТ, событие представляет собой зафиксированное состояние информационной системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств защиты информации, или ситуацию, которая может быть значимой для ИБ.

Анализ или разведка угроз, по NIST, имеет целью получение информации об угрозе: вектор, поверхность, тактические задачи (тактики) и приемы злоумышленников (техники атаки). Данная информация агрегируется, преобразовывается, анализируется, интерпретируется и «обогащается», чтобы обеспечить необходимый контекст для принятия решений.



Источник: www.ncsc.gov.uk/collection/building-a-security-operations-centre

Рис. 1. ***Матрица возможностей центра мониторинга***

Управление инцидентами представляет собой комплекс мероприятий и процедур, направленных на обнаружение, регистрацию, анализ инцидентов ИБ, а также реагирование на таковые, и на совершенствование системы защиты по результатам разбора инцидентов.

Реагирование на инциденты – собственно, часть управления инцидентами, зачастую, выделяемая по причине принятия конкретного решения. По сути, это действие или совокупность действий, осуществляемых в отношении зарегистрированного инцидента. Показатель реагирования (время реакции на инцидент) – базовый показатель центра мониторинга.

Управление уязвимостями – процесс, включающий процедуры инвентаризации и категорирования ресурсов, выявления уязвимостей, оценки опасности уязвимостей, их анализа и исправления, а также проверки эффективности исправления. На практике указанная операция включает в себя регулярное сканирование на наличие известных уязвимостей и их устранение. Недавно появился проект документа ФСТЭК России «Руководство по управлению уязвимостями программного обеспечения и программно-аппаратных средств в органе (организации)».

Если названные выше функции носят в целом реактивный характер (событие – угроза – инцидент – команда), то *поиск угроз* – это процесс проактивного обнаружения угроз, которые не выявлены средствами защиты информации, работающими по заданным правилам. Как правило, специалисты используют методы проверки гипотез, ситуационного анализа, расследования по индикаторам компрометации и атак (IOC, IOA) и пр.

Что касается третьей логической составляющей центра мониторинга – *технологий и средств*, то уже упоминалось, что основой центра мониторинга ИБ является SIEM-система, в простейшем случае выполняющая функции сбора и анализа событий (преобразование, унификация, нормализация, фильтрация), уведомления и принятия (согласно правилам) решения об инциденте, собственно реакции системы, а также хранения данных для постанализа и оценки соответствия (рис. 2). В реальности конкретные SIEM-решения имеют множество дополнительных смежных функций.

Другими устоявшимися (и упомянутыми в приказах ФСТЭК России) технологиями являются системы обнаружения вторжений (IDS/IPS), межсетевые экраны, средства антивирусной защиты (AV) и средства анализа защищенности (VA/VM). К относительно новым технологиям автоматизации процессов центра мониторинга, но принципиально направленным на выявление нетривиальных атак (например, APT-атак), могут быть отнесены следующие:

- EDR (*Endpoint Detection & Response*[1]) – класс решений для обнаружения и изучения вредоносной активности на конечных точках путем непрерывного наблюдения и анализа подозрительной корреляции событий;
- TIP (*Threat Intelligence Platform*) – автоматизируют цикл работ с потоками данных об угрозах («фидами»);
- IRP (*Incident Response Platform*) – используются для автоматизации действий по реагированию на инциденты на основе сценариев реагирования («плейбуков») и сбору дополнительной информации по инцидентам;
- SOAR (*Security Orchestration, Automation and Response*) – представляют собой результат развития IRP в направлении интеграции и управления средствами защиты информации;
- NTA (*Network Traffic Analysis*) – предназначены для автоматизации перехвата и анализа безопасности сетевого трафика, главным образом, в оффлайн-режиме с целью обнаружения признаков проведения сложных и целенаправленных APT-атак, не выявленных техническими средствами обнаружения.

Следует сказать, что мир не стоит на месте, и можно ожидать ряд околомаркетинговых приемов, направленных на освещение оригинальных свойств новых технологий мониторинга, которые либо выделяют отдельно, либо интегрируют в конкретные корпоративные решения класса SIEM [15–21]. На рис. 3 представлен пример эволюции центров мониторинга, как его видят ведущие разработчики [13].

Подобные тенденции прослеживаются у видных игроков на рынке, представляющих крупные центры мониторинга (нисколько не умаляя их действительно грандиозных возможностей), такие как Solar JSOC, BI.ZONE, IZ.SOC, Angara CRC, JET CSIRT, и ориентированных на определенный целевой сегмент: крупный бизнес или государственные корпорации. Однако имеется ряд исследований, которые демонстрируют не столько корпоративные тренды по построению комплексных центров будущего, сколько реальные потребности компаний в центрах мониторинга.

Прагматический взгляд на центр мониторинга

Опрос, проведенный авторами, показал, что большая часть компаний главным фактором, учитываемым

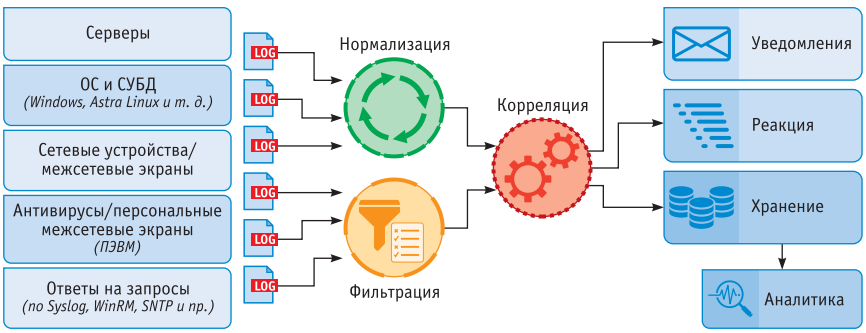


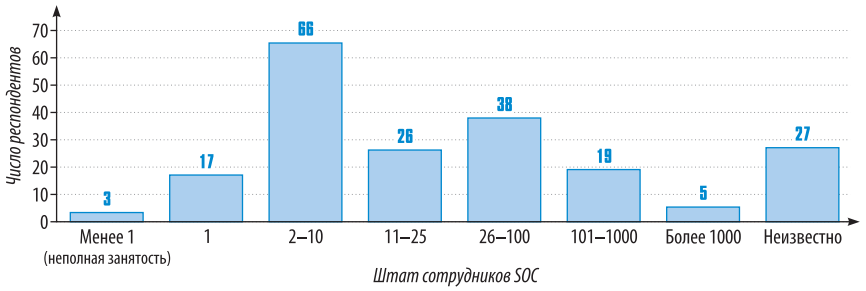
Рис. 2. ***Принцип работы SIEM***

[1] *Термин введен в 2013 году Антоном Чувакиным.*

Мониторинг доступности	Реактивный мониторинг		Проактивный мониторинг	Автоматизированный проактивный мониторинг	
Network Alerts	▯ Anti-virus ▯ IDS ▯ Firewall	▯ Vulnerability Management ▯ Statefull Inspection ▯ Anti-spam ▯ IPS	▯ DLP ▯ Advanced Persistent ▯ Threats ▯ SIEM ▯ SecOps	▯ GABS ▯ Cloud Security ▯ UEBA ▯ TIP ▯ Sandboxing ▯ CERT ▯ BYOD	▯ Big Data (Data Lake) ▯ CWPP/CSPM ▯ Next-Gen SIEM ▯ SOAR ▯ Deception ▯ EDR ▯ Cloud Native SIEM
Network Operation Center	**NSOC/SOC V1**	**SOC V2**	**SOC V3**	**NG SOC**	**CyberSOC**
Правительство Военные	Правительство Военные Крупные корпорации Банки	Правительство Военные Крупные корпорации	Правительство Военные Предприятия Банки Фармацевтика	Правительство Военные Банки Все предприятия	Все предприятия Интернет вещей Умные дома/автомобили
NOC	**Internal SOC**	**SOC**	**SOC as Managed Security Services**	**Hybrid SOC**	**SOC and Network Detection & Response**
▯ Network Device Management ▯ Malicious Code Analysis	▯ Virus Alerts ▯ Intrusion Detection and Response	▯ Compliance ▯ Incident Response	▯ Regulator Compliance ▯ Log Monitoring ▯ Malware Analysis	▯ Reverse Engineering ▯ AI/ML Models ▯ Threat Intelligence	▯ Threat Hunting ▯ Automation ▯ Orchestration ▯ Playbooks ▯ Analytics ▯ External Risk Scoring

Источник: ISACA Journal, 2021, V. 5

Рис. 3. ***Эволюция центров мониторинга***



Источник: SANS 2022 SOC Survey

Рис. 4. ***Потребности в центре мониторинга, исходя из его масштаба (персонала)***

при построении центра, считают *финансовые затраты*, каковые должны быть обоснованы на основе *риск-ориентированного подхода*. Подавляющее большинство компаний интересуют готовые «строительные» компоненты, на которых возможно построение гибридного центра. Значительная доля российских госкорпораций предпочитает ограничиться минимальными обязательными компонентами, подпадающими под контроль регулятора. По оценкам компании Deepwatch[2], подобная картина наблюдается и за рубежом. Согласно ее исследованиям, большинство заказчиков услуг по мониторингу ИБ выступает против новых и захватывающих технологий в пользу зрелых и стабильных средств защиты: например, 85 % респондентов вообще высказались за упрощенные традиционные методы реагирования на инциденты, а около половины не предполагают круглосуточный график работы центра мониторинга. Аналогичные выводы сделаны в исследовании потребностей рынка мониторинга ИБ, проведенном компанией SANS[3]. К примеру, на рис. 4 проиллюстрирована популярность небольших центров, обслуживаемых двумя-тремя сотрудниками. Можно, конечно, поиронизировать, что в условиях турбулентности ИТ-кадров в нашей стране привлечение штата высокопрофессиональных специалистов разного профиля к работе многофункционального центра мониторинга требует железной аргументации. Можно также отметить ряд проблемных вопросов, указывающих в итоге на экономию капиталовложений [22, 23].

Именно исходя из подобного анализа предлагается относительно простой вариант построения центра мониторинга информационной безопасности на базе продуктов компании НПО «Эшелон».

Линейка продуктов НПО «Эшелон» для построения центров мониторинга

На рис. 5 показаны технологические решения компании НПО «Эшелон», позволяющие построить центр мониторинга ИБ по *принципу «ничего лишнего»* в организациях среднего размера.

Как видно из рис. 5, основными компонентами центра являются следующие средства защиты информации:

- межсетевой экран/шлюз/система обнаружения вторжений «Рубикон»;
- SIEM-система KOMRAD Enterprise SIEM;
- средство анализа защищенности «Сканер-ВС 6.0»;
- NTA-анализатор трафика eSensor.

Текущие решения в целом покрывают ключевые функции центров мониторинга ИБ за исключением средств антивирусного контроля и EDR. Состав линейки средств защиты информации был продиктован следующими критериями:

- ориентация на российский рынок (отечественные платформы, интеграция с российскими продуктами);
- надежные характеристики для средних сетей;
- минимальные требования к вычислительным ресурсам;
- быстродействие;

[2] *https://www.deepwatch.com/state-of-the-modern-soc/.*
[3] *https://www.sans.org/white-papers/sans-2022-soc-survey/.*

- обеспеченность сертификатами соответствия по безопасности информации.

Если на рис. 5 проиллюстрировано соответствие предлагаемого варианта общепринятым технологиям, применяемым в центрах мониторинга, то в таблице показано соответствие приведенных выше компонентов требованиям регуляторов.

Кратко проинформируем читателей об основных характеристиках указанных средств защиты информации.

1. Программно-аппаратный комплекс (ПАК) «Рубикон»[4] выполняет функции маршрутизатора, межсетевого экрана, системы обнаружения и предотвращения вторжений.

Отличительные возможности:

- высокая надежность;
- сигнатурный анализ сетевого трафика;
- наличие специальных защищенных исполнений и исполнения однонаправленного шлюза (рис. 6);
- поддержка мандатных меток Astra Linux.

2. KOMRAD Enterprise SIEM[5] – SIEM-система, выполняющая централизованный сбор событий ИБ, выявление инцидентов ИБ и реагирования на таковые, а также отправление данных о событиях и инцидентах ИБ во внешние системы (например, ГосСОПКА).

Отличительные возможности:

- низкие требования к вычислительным ресурсам (ОЗУ – 4 GB, CPU – 2 ядра, SSD – 100 GB).

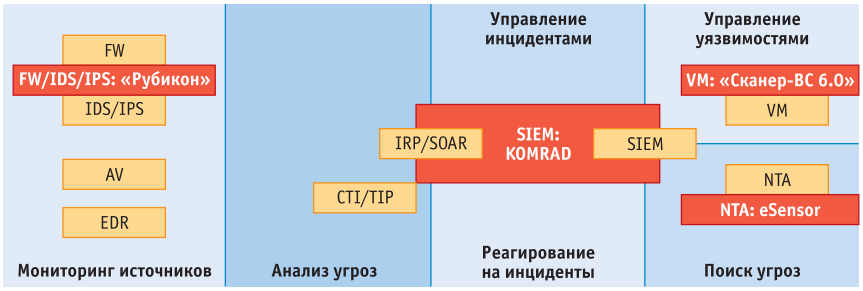


Рис. 5. ***Технологии, решения и средства автоматизации мониторинга***

- высокая производительность;
- оперативное оповещение об инциденте;
- возможность подключения любого источника событий;
- широкий спектр поддерживаемых источников событий «из коробки»;
- возможность передачи инцидентов в систему ГосСОПКА;
- возможность автоматического реагирования на инциденты;
- гибкость при создании фильтров и директив корреляции;
- дистрибутив под Astra Linux.

К слову, загрузка такой сложной системы, как SIEM, здесь выполняется за 5 минут.

3. Сканер-ВС 6.0 – скоростной сканер, реализованный по технологии, исключающей выполнение скриптов.

Перечень основных функций продукта:

- исследование сети: сканирование сетевых узлов и сервисов, идентификация операционной системы и приложений, трассировка сетевых маршрутов для построения топологии сети

Рис. 6. ***Примеры вариантов исполнения ПАК «Рубикон»***

- инвентаризация: исследование активного подключения к исследуемому узлу для сбора информации
- поиск уязвимостей: выявление уязвимостей ПО
- подбор паролей: проверка стойкости паролей сетевых сервисов
- аудит: проверка настроек ПО на соответствие требованиям безопасности

Отличительные особенности:

- высокая скорость поиска уязвимостей;
- широкий спектр поддерживаемых систем для сканирования (ОС семейств Windows и Linux, прикладное ПО);
- интеграция с SIEM-системами;
- дистрибутив под Astra Linux.

Таблица. ***Технические средства, определяемые регуляторами***

Средство защиты информации	Требования ФСБ России по средствам мониторинга ИБ	Требования ФСТЭК России по средствам мониторинга ИБ
KOMRAD Enterprise SIEM *(SIEM-система)*	• Средства взаимодействия персонала • Средства взаимодействия с главным центром ГосСОПКА • Средства учета и обработки инцидентов • Средства инвентаризации информационных систем • Средства анализа событий безопасности	• Средства управления информацией об угрозах безопасности информации Средства управления событиями безопасности информации • Средства управления инцидентами информационной безопасности
«Сканер-ВС»/«Инспектор» *(средство анализа защищенности и аттестации)*	• Средства выявления уязвимостей • Средства инвентаризации информационных систем	Средство контроля (анализа) защищенности информационных систем
«Рубикон» *(межсетевой экран и система обнаружения вторжений)*	Средства анализа событий безопасности	Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности
eSensor *(NTA-анализатор трафика)*	Средства анализа событий безопасности	-

[4] *https://npo-echelon.ru/production/65/11342.*
[5] *https://npo-echelon.ru/production/65/11793.*

4. eSensor – NTA-система глубокого анализа сетевого трафика, позволяющая записывать сетевой трафик, проводить его сигнатурный и эвристический анализ, осуществлять поисковые запросы по данным анализа и др.

Основные функции:

- сигнатурный анализ сетевого трафика;
- эвристический анализ сетевого трафика;
- запись трафика;
- поиск и фильтрация данных трафика;
- передача событий в SIEM;
- функционирование под Astra Linux.

Таким образом, вышеуказанное наглядно свидетельствует о том, что построение центра мониторинга ИБ возможно в экосистеме решений компании «Эшелон».

Выводы

Развитие и внедрение центров мониторинга является объективной динамикой отрасли ИБ, а насущный интерес в стране к внедрению таких структур диктуется требованиями регуляторов.

Согласно корпоративным отчетам, современное усовершенствование центров мониторинга ИБ идет в целом по пути наращивания функционала, однако анализ спроса и потребностей рынка ИБ показывает актуальность компактных собираемых или готовых отечественных изделий. Именно подобный подход рассмотрен в данной статье на примере комплексирования изделий НПО «Эшелон».

К достоинству линейки продуктов НПО «Эшелон» следует отнести то, что изначально, уже при разработке, она была ориентирована именно на отечественный рынок, поэтому оптимизирована под российские платформы и средства защиты информации. Несмотря на направленность в сторону ниши центров мониторинга организаций среднего размера, указанные продукты нацелены на высокий уровень доверия и обработку информации, отнесенной к сведениям, составляющим государственную тайну, а созданные на их основе проекты при необходимости легко масштабируются и интегрируются с иными системами.

Разумеется, что подход авторов не претендует на уникальность: многие отечественные разработчики средств защиты информации могут предложить дополнения или вариации рассмотренной реализации центра мониторинга ИБ, что только поспособствует становлению технологической независимости и технологического суверенитета страны. ■

ЛИТЕРАТУРА

1. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под. ред. Д. П. Зегжды. – М.: Горячая линия – Телеком. – 2021. – 560 с.*
2. *Knerler K., Parker I., Zimmerman C. 11 Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation. 2022. 2nd ed. 767 p.*
3. *Muniz J. Modern Security Operations Center. Addison-Wesley Professional. 2021. 752 p.*
4. *Марков А. С. Технические решения по реализации подсистем ГосСОПКА // В кн.: Управление информационной безопасностью в современном обществе. Сб. научных трудов V Международной научно-практической конференции. – 2017. – С. 85–96.*
5. *Месенгисер Я. Я., Малахов М. А., Милославская Н. Г. Центры управления сетевой безопасностью как силы ГОССОПКА // Безопасность информационных технологий. – 2022. – Т. 29, № 1. – С. 94–107.*
6. *Петренко А. С., Петренко С. А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. – 2016. – № 6 (72). – С. 28–30.*
7. *Зварич С. Г., Краснов С. Г., Рычков М. А., Ященко А. В. Анализ развития систем мониторинга информационной безопасности // Вестник Ярославского высшего военного училища противовоздушной обороны. – 2022. – № 3 (18). – С. 91–95.*
8. *Клянчин А. И., Марков А. С., Фадин А. А., Илюхин М. В. SIEM-технология как основа построения защищенных систем // В сб.: Информатизация и информационная безопасность правоохранительных органов – XXII Всероссийская научная конференция. – 2013. – С. 270–273.*
9. *Лаврова Д. С., Полтавцева М. А., Печенкин А. И., Зегжда Д. П. SIEM-система для обнаружения и анализа инцидентов безопасности в интернете вещей // Методы и технические средства обеспечения безопасности информации. – 2016. – № 25. – С. 35–36.*
10. *Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. – 2013. – № 4 (52). – С. 80–81.*
11. *Петренко С. А., Цирлов В. Л. Импортозамещение решений IDS И SIEM // Защита информации. Инсайд. – 2017. – № 5 (77). – С. 46–51.*
12. *Зотова А. В., Петренко С. А. Модели перспективных облачных CERT/CSIRT // Защита информации. Инсайд. – 2013. – № 5 (53). – С. 38–44.*
13. *Kaliyaperumal L. N. The evolution of security operations and strategies for building an effective SOC // ISACA Journal. 2021. V. 5. P. 1–9.*
14. *Khan N. A. Next gen security operations center: from concept to reality: the comprehensive guide to building, managing and transforming your organization's security operations center (SOC). First Edition // IP Specialist. 2023. 370 p.*
15. *Богданов В. В., Домуховский Н. А., Савин М. В. SOAR: автоматизация работы с инцидентами информационной безопасности // Защита информации. Инсайд. – 2021. – № 3 (99). – С. 13–17.*
16. *Корнеев Н. В., Меркулов В. Д. Концепция интеллектуального обнаружения угроз в вертикально интегрированных иерархиях центров безопасности // Информационные технологии. Проблемы и решения. – 2020. – № 2 (11). – С. 134–139.*
17. *Мещеряков Р. В., Исхаков С. Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. – 2022. – № 5 (51). – С. 82–99. – DOI: 10.21681/2311-3456-2022-5-82-99.*
18. *Лукацкий А. В. Концепция активной кибероборонs для железнодорожного транспорта // Автоматика, связь, информатика. – 2018. – № 1. – С. 24–26.*
19. *Ajmal A. B., Shah M. A., Maple C., Asghar M. N., Islam S. U. Offensive security: towards proactive threat hunting via adversary emulation // IEEE Access. 2021. V. 9. P. 126023–126033.*
20. *Barabanov A., Dergunov D., Makrushin D., Teplov A. Automatic detection of access control vulnerabilities via api specification processing // Voprosy kiberbezopasnosti. 2022. № 1 (47). P. 49–65. – DOI: 10.21681/2311-3456-2022-1-49-65.*
21. *Poltavtseva M., Zegzhda D., Alexandrova E., Shelupanov A., Bragin D. Key concepts of systemological approach to CPS adaptive information security monitoring // Symmetry. 2021. № 13 (2425). P. 1–16. – DOI: 10.3390/sym13122425.*
22. *Афанасьева С. В., Кузьмина У. В. Основные проблемы при работе с центрами мониторинга информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. – 2023. – № 1 (47). – С. 51–58. – DOI: 10.14529/secur230105.*
23. *Стрельников Р. В. SOC. Начинает и проигрывает // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. – 2021. – № 1. – С. 26–30.*