Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

# Самый безопасный SOC

№ 3 (212)/2011

**Jet Info**
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

**Редакция:**

Дмитриев В.Ю.
*vlad@jet.msk.su*

Некрасова Н.А.
*nekrasova@jet.msk.su*

Шедова Е.Л.
*eshedova@jet.msk.su*

**Верстка:**
Толоконникова Е.А.

**Корректура:**
Андрушко О.Ю.

**Над номером работали**:
Ежкова В.
Жевнерев М.
Ляпунов И.
Медведев А.
Рудацкий Е.
Силуянов В.
Симис Б.
Черных А.

**Издатель:**
Компания
«Инфосистемы Джет»

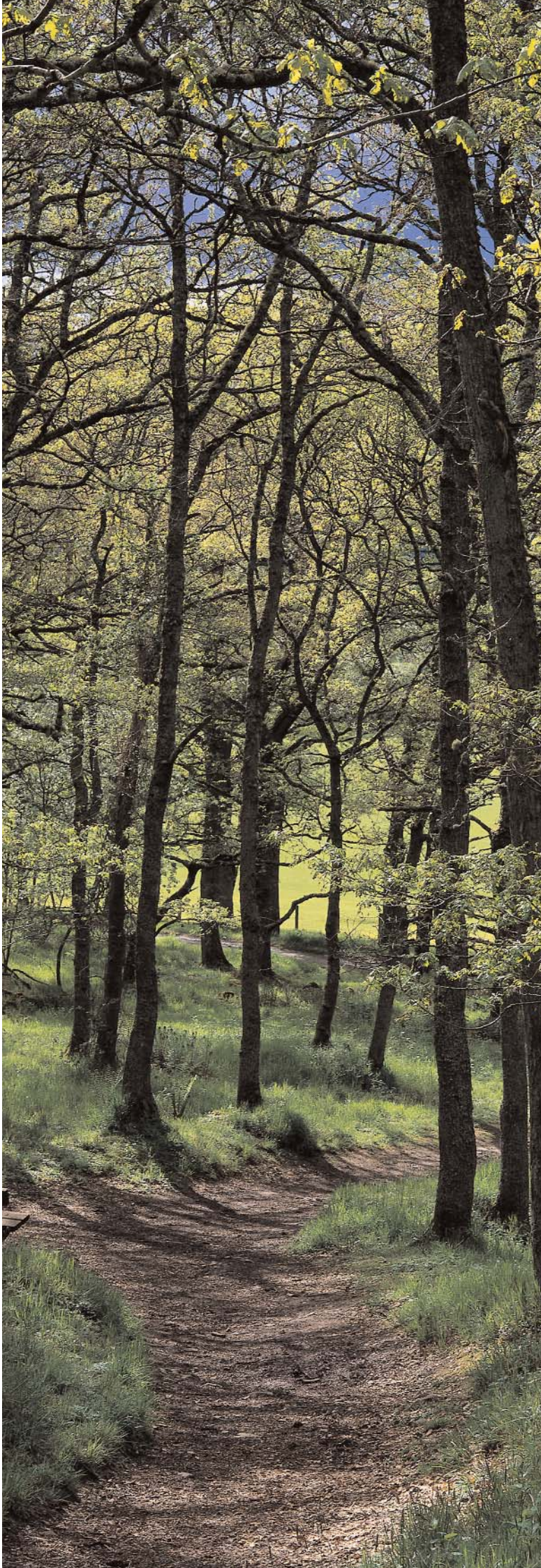
**Контакты:**
тел. (495) 411 76 01
*http://www.jetinfo.ru*

# От редакции

Век информационных технологий предъявляет особые требования к владельцам бизнеса. Как обеспечить достойный уровень информационной безопасности в компании? Какие элементы защиты обязательны, а какие нет? Как правильно и эффективно внедрить процесс управления ИБ? За последний год эти и другие вопросы стали волновать все больше руководителей подразделений, отвечающих за безопасность информационных ресурсов практически любой компании.

В этом номере мы познакомимся с основными трендами и практиками в области построения центров информационной безопасности (SOC, Security Operations Center) и внутренних процессов управления ИБ. Попытаемся максимально охватить полезный функционал продуктов по защите информации, расскажем о задачах, решаемых центром управления ИБ, узнаем о проблемах, актуальных для многих российских компаний, и вариантах их решения с помощью SOC.

**С уважением, Ваш JI**



## СОДЕРЖАНИЕ

**Новости** ..... 5

**Тема номера** ..... 9

**Самый безопасный SOC** (Медведев Артем, руководитель направления Security Operations Center компании «Инфосистемы Джет»)

- Предпосылки создания Центра оперативного управления ИБ ..... 9
- Практика SOC в России ..... 10
- Центр оперативного управления ИБ ..... 10
- Централизация оперативного управления ИБ ..... 11
- Мониторинг состояния ИБ ..... 12
- Управление инцидентами ИБ ..... 13
- Контроль соответствий ..... 13
- Построение Security Operations Center, SOC ..... 13
- Использование Центра оперативного управления ИБ для решения задач бизнеса ..... 13
- Выгоды, получаемые компанией, при внедрении SOC ..... 14
- Компоненты Центра Оперативного управления ИБ ..... 15
- MaxPatrol - система контроля состояния ИБ ..... 15
- Управление инцидентами ИБ ..... 18
- Управление событиями и инцидентами ИБ ..... 19
- ArcSight ESM ..... 20
- RSA enVision ..... 24
- Symantec Security Information Manager ..... 27
- Контроль действий пользователей баз данных и приложений ..... 29
- IBM Guardium ..... 30
- Imperva ..... 33
- Прикладные аспекты СОК ..... 35
- SOC и защита персональных данных ..... 35
- SOC и PCI DSS ..... 36
- SOC и внутренние задачи ..... 37
- В Заключение ..... 37

**Экспертное мнение** ..... 38

**Собеседник** ..... 43

**MaxPatrol: Универсальное решение может быть индивидуальным**
(Борис Симис, директор по развитию компании Positive Technologies)

**Наши проекты** ..... 45

**Приведение системы информационной безопасности ОАО Банк ЗЕНИТ в соответствие с требованиями стандарта PCI DSS**

## Компания «Инфосистемы Джет» развернула автоматизированную систему активации и обеспечения сервисов для компании «Дальсвязь»

Компании «Дальсвязь» и «Инфосистемы Джет» сообщили о завершении проекта по внедрению системы активации и обеспечения сервисов (САОС) в Приморском филиале оператора связи. Система автоматизирует бизнес-процессы обработки заявок на дополнительные услуги, поступающие от абонентов провайдера. Ранее такие операции как регистрация карточки клиента, подключение, отключение, заморозка счета выполнялись программным обеспечением, разработанным разрозненно внутри филиалов компании, частично осуществлялись вручную. Использование САОС позволило автоматизировать работу операторов, значительно сократить время реагирования на запросы пользователей и, как следствие, разгрузить персонал, обслуживающий предоставляемые сервисы.

В настоящий момент компания «Дальсвязь» делает акцент на предоставлении услуг на базе технологии MEN (Metro Ethernet Networks — городские сети Ethernet). Провайдер работает по трем основным направлениям — высокоскоростной доступ в Интернет, голосовая телефонная связь посредством IP-телефонии, цифровое телевизионное вещание (IP-телевидение). Компания «Дальсвязь» проводит внутреннюю политику по оптимизации бизнес-процессов, включающую внедрение промышленных решений автоматизации. Результатом чего должна стать минимизация затрат на расширение штата операторов, количества ошибок конфигурирования, времени, затрачиваемого от момента подачи заявления абонентом до получения им услуги. По итогам проведенного конкурса было выбрано решение на базе промышленной платформы Kabira Provision and Service Activation (KPSA), разработанное компанией «Инфосистемы Джет». Решение в полной мере соответствует функциональным задачам и является оптимальным по стоимости.

Специалисты компании «Инфосистемы Джет» прописали и реализовали логику процессов таким образом, чтобы совместно могли функционировать все бизнес-системы компании «Дальсвязь». Взяв за основу промышленную платформу Kabira Provision and Service Activation (KPSA), специалисты интегратора спроектировали и внедрили систему «под ключ», способную работать с заявкой клиента от момента ее регистрации до конечного результата — выполненной операции по услуге.

В качестве аппаратной базы для работы САОС спроектирован и внедрен вычислительный комплекс отказоустойчивой конфигурации на серверах Sun компании Oracle. Таким образом, САОС представляет собой бесконфликтное решение, органично интегрированное в мультивендорный ИТ-ландшафт заказчика.

Для наиболее эффективной работы системы активации и обработки сервисов специалисты компании «Инфосистемы Джет» доработали стандартный модуль хранения данных платформы KPSA, который значительно упрощает и оптимизирует работу с системами хранения данных. Кроме того, был создан удобный интерфейс для работы с бэк-офисом для управления настройками системы: редактирование и просмотр заявок, а также системных справочников — их состояний, истории изменений.

«Мы получили надежную производительную систему с высокой скоростью выполнения операций, что позволяет нам эффективно управлять конфигурацией массовых услуг, обеспечивающих прирост абонентской базы без изменения количества специалистов подразделений активации, — резюмирует **Олег Орлов, заместитель директора департамента эксплуатации телекоммуникаций.** — Применение данного решения работает на перспективу — позволяет нам вводить новые виды услуг едино-

образно и одновременно во всех филиалах с минимальными рисками реализации соответствующих проектов».

«Благодаря возможностям платформы — гибкой настройке процессов и продуктовых каталогов — нам удалось автоматизировать все необходимые бизнес-процессы и провести интеграцию с внешними системами в самые короткие сроки. Кроме того, для полной реализации бизнес-требований заказчика мы разработали два специализированных модуля, — комментирует **Андрей Яшин, директор по работе с ГК «Связьинвест» компании «Инфосистемы Джет».** — Этот проект позволил нам применить накопленный ранее опыт по созданию специализированных решений для телеком-операторов».

## Компания «Инфосистемы Джет» получила специализацию по Oracle Exadata

Компания «Инфосистемы Джет» прошла обучение по Oracle Exadata и получила специализацию в рамках программы OPN Specialized. Oracle подтверждает, что интегратор выполнил сертификационные требования и в настоящее время обладает всеми необходимыми ресурсами для развития экспертизы по направлению Oracle Exadata.

«Oracle Exadata вызывает интерес у наших заказчиков, и мы планируем развивать это направление, в том числе в регионах нашего присутствия, — отмечает **Игорь Григорьев, Директор по работе с решениями Oracle компании «Инфосистемы Джет».** — Расширение экспертизы по решениям Oracle Exadata позволит существующим и потенциальным заказчикам нашей компании получить оперативный доступ к нашим услугам, а нам — вести работу в демо-центрах более эффективно».

## В Киеве открыт демо-центр по Oracle Exadata

**Компания «Инфосистемы Джет» и Представительство Oracle в Украине открыли демо-центр по Oracle Exadata Database Machine в Киеве.**

Полный интегрированный высокопроизводительный программно-аппаратный комплекс Oracle Exadata Database Machine оптимизирован и готов к работе. Oracle Platinum Partner, компания «Инфосистемы Джет» первой в Украине приглашает клиентов «вживую» протестировать свои приложения на самой быстрой в мире машине баз данных Oracle.

Программно-аппаратный комплекс нового поколения Oracle Exadata Database Machine состоит из кластера серверов БД, системы хранения данных, СУБД Oracle Database 11g. Кроме того, комплекс включает интеллектуальное программное обеспечение Oracle Exadata Storage Server, которое способствует ускоренной обработке запросов с меньшей загрузкой широких каналов InfiniBand благодаря обработке и фильтрации запросов в непосредственной близости к данным.

«Мы приглашаем в наш центр в Киеве прежде всего компании, которые имеют дело со значительными объемами данных или нуждаются в консолидации приложений, а также в ускорении работы OLTP или DSS приложений, — отметил **Владимир Резник, генеральный директор компании «Инфосистемы Джет – Украина».** – Уже сегодня они могут протестировать программно-аппаратный комплекс нового поколения Oracle Exadata Database Machine на собственных реальных данных и для решения своих бизнес-задач».

Уникальная архитектура Oracle Exadata обеспечивает более высокую скорость передачи данных, снимая традиционные ограничения систем хранения информации. Линейная масштабируемость и высокая надежность Oracle Exadata являются критически важными для успешной поддержки бизнес-операций.

«Цель наших инноваций и разработок — создавать значимые преимущества для бизнеса заказчиков, причем с каждым годом расширять и дополнять их, — подчеркнул **Эдуард Попович, глава Представительства Oracle в Украине.** — Совместно разработанные программно-аппаратные комплексы Oracle созданы, чтобы работать вместе. Они дают лучшую производительность, безопасность, управляемость, и, главное, снижают затраты. Мы полностью поддерживаем инициативу партнера, ведь демо-центр в Киеве даст возможность украинским компаниям оценить эти преимущества на практике».

Комплекс наиболее востребован компаниями в телекоммуникационном, государственном, финансовом, розничном и производственном секторах. Демо-центр позволит существующим и потенциальным клиентам поработать с Oracle Exadata. Опытные консультанты партнера и Oracle окажут помощь в оценке и выборе оптимальной конфигурации полной системы (приложение и база данных). Пять экспертов компании «Инфосистемы Джет», в том числе непосредственно в Украине, получили сертификаты по результатам обучения по Oracle Exadata.

С открытием демо-центра в Киеве спектр возможных задач для тестирования Oracle Exadata будет расширен за счет одновременного задействования двух демо-центров партнера — киевского и ранее открытого московского. Проверить эффективность

комплекса будет возможно теперь не только при колоссальных нагрузках, но и для территориально-распределенных решений.

## Компания «Инфосистемы Джет» провела комплексный ИТ-аудит в СЗРЦ Банка ВТБ

**Компания «Инфосистемы Джет» сообщает об успешном завершении обследования ИТ-инфраструктуры, системы управления ИТ-сервисами и документационного обеспечения деятельности Дирекции сопровождения информационных технологий (ДСИТ) Северо-Западного регионального центра ОАО Банк ВТБ (СЗРЦ Банка ВТБ).** В результате проекта была дана разносторонняя оценка текущего состояния ИТ-системы Центра и разработаны рекомендации по ее модернизации.

В марте 2011 года ОАО «Банк ВТБ Северо-Запад» был реорганизован — присоединен к Банку ВТБ. На базе головного офиса ВТБ Северо-Запад создан Северо-Западный региональный центр. Одним из важнейших направлений при присоединении банка была интеграция ИТ-системы, доработка и настройка ИТ-процессов для дальнейшего развития будущего Центра в соответствии со стратегическими планами группы ВТБ. Прежде чем наметить пути развития ИТ-системы, было принято решение провести независимый аудит ВТБ Северо-Запад. Для этой цели была приглашена компания «Инфосистемы Джет», имеющая опыт комплексных аудитов разного масштаба на крупных предприятиях различных секторов экономики, в том числе в банках.

Проект длился шесть месяцев и включил в себя обследование ИТ-инфраструктуры (общая архитектура, серверные комплексы, системы хранения данных, системы резервного копирования, сети передачи данных, инженерные подсистемы основного и резервных ЦОД), обследование практики управления ИТ-сервисами и документационного обеспечения деятельности ДСИТ. Проведение аудита осуществлялось с применением хорошо зарекомендовавших себя методик и технологий (в том числе собственных), отработанных на практике экспертами компании «Инфосистемы Джет».

Обследование ИТ-инфраструктуры проводилось в тесном сотрудничестве со специалистами заказчика и носило масштабный характер, поскольку инфраструктура банка включает несколько центров обработки данных и сотни единиц оборудования. Проанализировав текущую ситуацию и имеющиеся у заказчика планы развития, эксперты компании «Инфосистемы Джет» предложили способы модернизации ИТ-инфраструктуры в соответствии с требованиями по доступности, сформулированными заказчиком, а также показателями надежности и производительности, основанными на лучших практиках по организации ИТ. Заказчику были представлены возможные пути оптимизации ИТ-парка с точки зрения снижения эксплуатационных затрат, в первую очередь — за счет консолидации и виртуализации вычислительных ресурсов и ресурсов системы хранения данных.

В рамках обследования системы управления ИТ были выбраны процессы, наиболее важные для решения текущих задач:

- управление каталогом ИТ-услуг,
- управление инцидентами,
- управление конфигурациями,
- мониторинг управления ИТ-инфраструктурой,
- сервисная отчетность.

На основе целей и задач управления ИТ, зафиксированных в ходе интервью с руководителями функциональных департаментов банка, была произведена оценка существующих процессов управления. Для этого использовалась модель зрелости процессов по CoBit по пятибалльной шкале. Дополнительно были выявлены три группы рисков существующей системы ИТ-управления — риски потери управляемости, риски потери данных и риски несоответствия целям и задачам ДСИТ. Также в ходе обследования были зафиксированы проблемы и предложения по улучшению, сформулированные сотрудниками банка.

Специально для проведения аудита существующего документационного обеспечения деятельности эксперты компании «Инфосистемы Джет» разработали собственную методику. Это позволило провести всестороннюю оценку по различным срезам: полнота документационного обеспечения, содержание, актуальность регламентов, охват по видам деятельности, по организационным единицам, по объектам обслуживания. Результаты обследования содержали информацию обо всех видах документации, используемой в ДСИТ. На основе этих данных можно планировать как изменения документов, так и структурные преобразования.

«Для проведения ИТ-аудита важно не только применение обширного инструментария и владение набором методик. Большое значение имеют опыт консалтинговых практик и уровень экспертизы. Понимая это, мы доверили проект компании «Инфосистемы Джет», — комментирует **Александр Марченко, руководитель дирекции сопровождения информационных технологий Северо-Западного регионального центра ОАО Банк ВТБ.** —

«На выходе» мы получили документ, содержащий объективную оценку положения дел, созвучную мнению специалистов нашей ИТ-службы. Материалы аудита активно использовались нами при проведении ИТ-мероприятий по реорганизации ВТБ Северо-Запад в форме присоединения к Банку ВТБ».

«Комплексный аудит открывает широкие возможности для понимания того, насколько задачи бизнеса обеспечиваются с точки зрения ИТ-ресурсов. Оценке подвергаются все уровни и процессы: от оборудования до вопросов управления, от документационного обеспечения до процессов деятельности — в этой взаимосвязи компонентов и заключается комплексность. Руководство СЗРЦ понимает это и учитывает результаты аудита при планировании развития ИТ», — рассказывает **Андрей Шапошников, руководитель группы системной архитектуры компании «Инфосистемы Джет».**

Северо-Западный региональный центр ОАО Банк ВТБ получил полную и объективную картину состояния ИТ-инфраструктуры, системы управления ИТ-сервисами и документационного обеспечения работы ИТ-службы. В итоговом отчете изложены основные требования, рекомендации по оптимизации и модернизации с учетом особенностей организационной структуры и перспектив развития. Полученные данные СЗРЦ уже использует на практике — при планировании ресурсов, реструктуризации, составлении бюджетов и т.д.

## Компания «Инфосистемы Джет» подтвердила специализацию IBM Guardium

Компания «Инфосистемы Джет» прошла авторизацию по модели IBM Software Value Plus, тем самым получив право на распространение и внедрение инновационных решений IBM Guardium по защите баз данных.

Технологии Guardium решают наиболее актуальные в настоящее время задачи защиты баз данных и являются прекрасным инструментом в проектах по приведению ИТ-инфраструктуры заказчиков в соответствие с требованиями Федерального Закона «О защите персональных данных», требованиями стандарта PCI DSS и других регуляторов.

«По нашему опыту, технологии IBM Guardium обеспечивают максимальный уровень защиты данных, которые хранятся в корпоративных базах данных и обрабатываются бизнес-приложениями, — комментирует **Артем Медведев, руководитель направления безопасности баз данных компании «Инфосистемы Джет».** — Речь идет, прежде всего, о персональных данных, финансовых потоках организации, данных о держателях кредитных карт — всей информации, надежная защита которой критична для бизнеса».

«Наличие сертификации по программе IBM Software ValuePlus помогает заказчикам выбрать для реализации проекта партнера, подтвердившего свою квалификацию и имеющего необходимые знания и ресурсы для успеха проекта, — добавляет **Сергей Лихарев, руководитель направления решений по управлению информацией IBM.** — Получение компанией «Инфосистемы Джет» сертификации по решениям Guardium подтверждает серьезные инвестиции в развитие профессиональных компетенций и возможности по квалифицированному выполнению проектов по защите СУБД с помощью технологий IBM».

## Компания «Инфосистемы Джет» сертифицировала средство защиты баз данных IBM Guardium

Компания «Инфосистемы Джет» сообщает о сертификации продукта для защиты баз данных IBM InfoSphere Guardium в системе сертификации ФСТЭК. В настоящий момент компания является первой и единственной, завершившей процедуру сертификации специализированного средства для защиты баз данных IBM Guardium. Сертификация позволяет использовать продукт в качестве инструмента для построения систем защиты персональных данных в соответствии с требованиями № 152-ФЗ «О персональных данных».

Технологии IBM InfoSphere Guardium представляют собой программно-аппаратный комплекс мониторинга, аудита и контроля доступа к информации, обрабатываемой в современных СУБД корпоративного класса. Сертификационные испытания подтвердили, что комплекс IBM Guardium может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в информационных системах обработки персональных данных до 2 класса включительно.

«Наша компания имеет более десятка успешно выполненных проектов по созданию решений на основе продукта IBM Guardium, — рассказывает **Артем Медведев, руководитель направления безопасности баз данных компании «Инфосистемы Джет».** — Его преимущество состоит в том, что он позволяет оптимизировать затраты на создание системы защиты персональных данных и не требует внесения изменений в существующую инфраструктуру БД и приложений».

# Самый безопасный SOC

**Медведев Артем,**
**руководитель направления Security Operations Center**
**компании «Инфосистемы Джет»**

## Предпосылки создания Центра оперативного управления ИБ

По оценкам отечественных специалистов в области ИБ, в настоящее время уровень информационной безопасности в российских компаниях по сравнению с западными не очень высок, но темпы развития в разы выше. Это обусловлено не только новыми нормативными актами и законами, такими как 152-ФЗ, PCI DSS, СТО БР, но и осознанием того, что информационной безопасностью нужно заниматься серьезно, системно выстраивая процессы. Иначе есть риск не только потерять инфраструктурные элементы, но и понести реальные финансовые убытки.

Так, например, практически в каждой организации мы видим ситуацию, когда доступ пользователей к финансовой информации и транзакциям в базах данных не журналируется. И в случае несанкционированного доступа либо утечки информации из БД невозможно отследить, кто внес изменения в таблицы, откуда был осуществлен доступ и кто скопировал критичные данные.

Соответственно, несмотря на огромное количество антивирусов, экранов и других активных средств защиты информации, нет единой картины происходящего в инфраструктуре. Все элементы защиты по отдельности настроены и работают, но между ними нет единого связующего звена, которое бы позволило эффективно использовать комплекс средств защиты, максимально быстро выявлять инциденты и учиться действовать проактивно.

Как же можно повысить эффективность текущего комплекса средств защиты информации, различного сетевого оборудования и приложений? Эксперты компании «Инфосистемы Джет» видят решение многих текущих проблем обеспечения ИБ и повышения эффективности корпоративной защиты в построении Центра управления информационной безопасностью. Давайте определим, что мы вкладываем в это понятие, какие элементы могут входить в классический SOC, как добиться эффективности в выявлении и устранении инцидентов, связанных с информационной безопасностью.

**Сизифов труд**

В стремительно развивающейся инфраструктуре, теперь уже не десятки устройств, а сотни и даже тысячи. Одних маршрутизаторов или межсетевых экранов может быть несколько десятков. Все они пропускают через себя огромный объем информации, все события, происходящие на устройствах, записываются во внутренние журналы. Но они, по сути, бесполезны, так как невозможно централизованно следить за таким количеством событий, делать аналитику и выявлять инциденты, нарушающие политику ИБ.

## Практика SOC в России

Прежде чем высказывать экспертное мнение и давать какие-либо рекомендации, рассмотрим несколько подходов к организации Центров управления информационной безопасностью в России. Если говорить в общем, то SOC — это часть общего процесса управления ИБ наравне с управлением рисками, контролем утечек информации и управлением доступом. В большинстве российских компаний, строящих SOC, все эти процессы протекают параллельно с развитием стратегии обеспечения информационной безопасности.

### Главное – люди

Давайте рассмотрим практику построения SOC на конкретных, наиболее ярких, примерах. Один из крупнейших Центров управления ИБ принадлежит оператору связи. Компания охватывает несколько стран и имеет в штате более 40 тысяч сотрудников. Такие масштабы налагают свою специфику на работу с информацией, особенно в части регистрации событий, связанных с ИБ. Security Operations Center базируется на трех основополагающих направлениях — процессы, люди и технологии. Каждый участник SOC знает свои роли и обязанности, правила реагирования и процессы взаимодействия с другими.

Технологии SOC, внедренные в этой компании, покрывают несколько основных направлений. Во-первых, это подсистема сбора и корреляции событий ИБ, которая собирает журналы с более чем 2000 устройств. Данные поступают из различных источников — с сетевых устройств, приложений, операционных систем, баз данных. Подсистема мониторинга транзакций БД покрывает все основные СУБД различных производителей и версий. Подсистема защиты баз данных интегрирована в SOC и является одним из источников событий ИБ, доступных для анализа в главной консоли мониторинга. Активно развивается подсистема мониторинга состояния ИБ и контроля уязвимостей, которая также является элементом комплекса технологий защиты информации.

Уникальность SOC этой компании состоит в комплексном подходе к обеспечению информационной безопасности. Основной упор делается не столько на технологии, сколько на процессы и людей. Именно сотрудники компании обеспечивают оперативное реагирование на события и инциденты, максимально быстро выявляя и устраняя уязвимости и потенциальные угрозы. Благодаря единой информационной панели они централизованно собирают информацию с различных подсистем в режиме реального времени.

### Разделение труда

Другим интересным примером подхода к построению Центра управления информационной безопасностью является компания из нефтяной отрасли. По сути, от SOC руководство компании ждет показатели защищенности критичных данных, скорость выявления и устранения инцидентов, а также ряд других показателей SLA. Эта компания решила определить для себя критичные показатели уровня ИБ и не строить свой собственный Центр управления ИБ, а отдать эти функции компании-подрядчику, специализирующемуся на информационной безопасности. В этом случае каждый занялся тем, в чем он был силен. Нефтяная компания выставляла требования, основанные на запросах бизнеса, а компания-эксперт решала задачи, которые приводили к нужному результату.

Это два наиболее ярких примера подходов к построению SOC в российских компаниях. Оба эффективны и решают задачи бизнеса одинаково хорошо. Если вы планируете развивать в своей компании Центр управления ИБ, прежде всего, стоит обратить внимание на специфику отрасли, уровень требований высшего руководства к защищенности информации и необходимость выделения функций управления ИБ в отдельное функциональное подразделение.

## Больше не значит лучше

**Центр оперативного управления ИБ — гарантии и уверенность в уровне обеспечения информационной безопасности**

*Одним из наиболее мощных инструментов эффективного управления информационной безопасностью любого предприятия является Центр оперативного управления ИБ (Security Operations Center, SOC), который позволяет контролировать и поддерживать уровень информационной безопасности, требуемый бизнесом.*

Как показывает опыт, безопасность критичных бизнес-процессов компании, в том числе и информационная безопасность, является одним из требований современной практики ведения бизнеса. В связи с этим компании реализуют комплекс организационно-технических мер по обеспечению ИБ. Однако внедрение только средств за-

щиты, как правило, не дает понимания, насколько полученный уровень ИБ соответствует требуемому, а значит, умалчивает и об эффективности всей системы ИБ в целом. Внутренние и внешние аудиты не являются достаточными для решения данной задачи, поскольку носят периодический характер.

Без постоянного мониторинга ИБ в режиме реального времени крайне сложно иметь полную и достоверную информацию об имеющихся событиях и уязвимостях, текущих настройках и корректности функционирования средств защиты. В компаниях с развитой ИТ-инфраструктурой и большим количеством разнообразных средств защиты без специализированных технических средств выстроить полную картину весьма проблематично.

Кроме того, внедряемые средства защиты направлены лишь на снижение вероятности возникновения инцидентов ИБ. В случае, если инцидент произошел, без оперативного вмешательства ущерб от него может быть весьма серьезным. Поэтому важно своевременно реагировать на выявляемые в ходе мониторинга инциденты.

В то же время растущие требования законодательства и нормативных актов в области ИБ (ФЗ №152 «О персональных данных», PCI DSS, ISO/IEC 27001:2005, SOX, Basel II, СТО БР ИББС-1.0-2006, СТР-К) говорят о необходимости соответствовать им и проводить периодические проверки на их выполнение.

**Внедряя Центр оперативного управления ИБ,** компании одновременно реализуют часть процессов системы управления ИБ (СУИБ) в соответствии со стандартом ISO 27001 (процесс управления инцидентами ИБ, управление уязвимостями, управление изменениями, контроль соответствия законодательным и отраслевым требованиям), а также выполняют часть требований стандарта PCI DSS (требования разделов 1, 6, 10, 11, 12).

Без постоянного мониторинга состояния ИБ, оперативного реагирования на инциденты, управления уязвимостями и контроля выполнения требований законодательства, нормативных актов и внутренних корпоративных политик компаниям довольно сложно быстро и качественно проверить состояние уровня безопасности на соответствие требуемому, а также поддерживать безопасность на должном уровне.

Согласно выводам наших экспертов, исключительно наращивание средств защиты без решения данных задач, как правило, не является эффективной стратегией обеспечения информационной безопасности в компании.

## Централизация оперативного управления ИБ

Центр информационной безопасности компании «Инфосистемы Джет» разработал и внедряет комплексное решение рассматриваемых выше задач — Центр оперативного управления ИБ (Security Operations Center, SOC).

Центр оперативного управления ИБ представляет собой набор связанных и работающих процессов управления ИБ (мониторинг, управление инцидентами ИБ, управление уязвимостями, инвентаризация активов, управление изменениями, контроль политик безопасности) и их автоматизацию посредством внедрения тесно взаимосвязанных и дополняющих друг друга соответствующих технических систем:

- мониторинга состояния ИБ (мониторинг событий ИБ, аудит действий пользователей, управление уязвимостями/контроль конфигураций);
- управления инцидентами ИБ;
- контроля соответствия требованиям законодательства, международных и отраслевых стандартов, внутренних корпоративных политик.

SOC предоставляет полную картину текущего состояния ИБ в компании, что позволяет оперативно устранять выявляемые отклонения и обеспечивать заданный уровень ИБ. С его помощью можно отслеживать происходящие в информационной системе события, связанные с ИБ, анализировать и сопоставлять их с другими данными, контролировать имеющиеся уязвимости, осуществлять контроль конфигураций, отслеживать степень выполнения требований законодательства, нормативных актов и корпоративных политик, а также оперативно реагировать на выявленные инциденты ИБ.

**Центр оперативного управления ИБ** позволяет контролировать и оперативно управлять информационной безопасностью компании в режиме реального времени, быть уверенным в том, что требуемый уровень обеспечения ИБ достигнут и поддерживается, отслеживать выполнение заданных целевых показателей эффективности (KPI) обеспечения ИБ.

Ключевыми факторами, обеспечивающими эффективность подобных центров, являются: внедрение процессов мониторинга, управления уязвимостями и инцидентами; правильное разграничение ответственности между сотрудниками внутри компании; разработка и внедрение регламентов реагирования на инциденты ИБ и их последующего разбора.

## Мониторинг состояния ИБ

Мониторинг состояния ИБ включает в себя несколько систем.

**Система управления (мониторинга) событиями ИБ (Security Information Management System, SIMS)** реализует комплексный подход к решению задач сбора, анализа (корреляции) и контроля событий ИБ, поступающих от различных средств защиты. Она помогает решить следующие задачи:

- управление большим объемом событий ИБ;
- получение полной картины происходящего в информационной системе с точки зрения ИБ;
- мониторинг текущего уровня обеспечения безопасности (контроль достижения заданных показателей эффективности (KPI) обеспечения ИБ);
- своевременное обнаружение инцидентов ИБ;
- получение реальных данных для анализа и оценки рисков;
- принятие обоснованных решений по управлению ИБ;
- выполнение требований законодательства и нормативных актов по мониторингу событий, связанных с ИБ (ISO/IEC 27001:2005, PCI DSS, СТО БР ИББС, Федеральный закон № 152-ФЗ «О персональных данных» и др.).

На рынке систем управления событиями ИБ представлены технические решения различных производителей. Они отличаются по функционалу, спектру решаемых задач, сфере применения. Компания «Инфосистемы Джет» использует наиболее гибкие, мощные и постоянно совершенствующиеся продукты, имеющие качественную техническую поддержку на территории РФ и стран СНГ: **ArcSight ESM, RSA enVision, Symantec Security Information Manager (SSIM).**

**Система аудита действий пользователей** обеспечивает регистрацию и анализ действий пользователей (прежде всего, на уровне БД), рассылку уведомлений в режиме реального времени и подготовку отчетов о том, кто и к какой информации получает доступ и как эти действия могут нарушить требования внешних регулирующих органов или внутренние правила по информационной безопасности компании.

Система аудита действий пользователей контролирует злонамеренные действия пользователей, защищает от утечек конфиденциальной информации, дает ответы на вопросы: «Кто? Что сделал? Когда? Где? Откуда? Куда? С помощью каких средств?», готовит отчеты различного уровня (от руководителя компании до администратора информационной безопасности).

Центр информационной безопасности компании «Инфосистемы Джет» реализует систему аудита действий пользователей на базе отлично зарекомендовавших себя продуктов **IBM Infosphere Guardium и Imperva,** первый из которых легко интегрируется с продуктами ArcSight ESM, а второй обладает одним из самых мощных на рынке функционалов межсетевого экранирования для веб-приложений (Web Application Firewall).

**Рис. 1. Центр оперативного управления ИБ**

**Система управления уязвимостями/контроля** за конфигурациями позволяет получать данные по имеющимся уязвимостям в режиме реального времени, отслеживать динамику их устранения, контролировать производимые изменения, а также обеспечивать автоматизацию таких задач, как инвентаризация ресурсов и контроль за конфигурациями. Поиск уязвимостей критичных ресурсов проводится на постоянной основе различными способами: сетевое сканирование, тест на проникновение, системные проверки, анализ защищенности СУБД и web-приложений. Компания «Инфосистемы Джет» реализует данную систему на базе продукта **MaxPatrol (Positive Technologies).**

**Рис. 2. Система управления инцидентами ИБ**

### Управление инцидентами ИБ

**Система управления инцидентами ИБ** осуществляет регистрацию, оперативное реагирование и эффективное разрешение инцидентов ИБ, реализует полный цикл работ с ними. От того, насколько быстро и грамотно компания отреагирует и разрешит возникший инцидент ИБ, зависит размер наносимого ей ущерба. Поэтому подготовка к разрешению инцидентов приобретает особое значение.

Подготовительный этап включает планирование, определение ответственных, разграничение обязанностей, разработку планов по разрешению инцидентов и т. д. Далее осуществляется непосредственно регистрация инцидентов ИБ и реагирование на них с последующим разрешением.

В процессе управления инцидентами ИБ важно не только разрешить их, но и проанализировать, насколько эффективно организован этот процесс. Необходимо периодически тестировать разработанные планы для поддержания их в актуальном рабочем состоянии и своевременного улучшения. Кроме того, важно проводить анализ произошедших инцидентов с целью дальнейшей корректировки текущих практик и принятия мер проактивной защиты.

Если при анализе выявлены незначительные отклонения, то проводятся корректирующие действия. Если же выявлены системные ошибки, обнаружена неэффективность применяемых планов и т.д. — производится активация подготовительного этапа.

Построение **Системы управления инцидентами ИБ** предполагает внедрение процесса управления инцидентами ИБ и (опционально) его автоматизацию.

### Контроль соответствий

**Система контроля соответствий** позволяет выполнять регулярные технологические проверки соответствия информационных систем внутренним политикам безопасности компании, техническим стандартам, требованиям нормативных актов, международным стандартам и т. п.

Данная система предоставляет возможность определить внутренний стандарт на базе международных стандартов (ISO 27001), рекомендаций производителя, «best practice» NSA, NIST, CIS, внутренних требований. А также постоянно контролировать соблюдение стандартов для сетевого оборудования, прикладных систем (ERP, CRM), операционных систем UNIX и Windows, различных СУБД.

Компания «Инфосистемы Джет» реализует систему контроля соответствий на базе продуктов MaxPatrol (Positive Technologies).

## Как построить Security Operations Center?

Существуют различные варианты построения SOC в зависимости от степени зрелости и текущих задач компании: от внедрения отдельных систем до комплексных решений. При реализации сложных масштабных проектов в ряде ситуаций оптимально поэтапное внедрение, когда на каждом этапе увеличивается область применения SOC как по территориальному охвату (например, сначала — головной офис, затем — регионы), так и по функциональным системам (система управления событиями ИБ, после — система управления уязвимостями).

### Как использовать SOC для решения задач бизнеса?

По нашему мнению, эффективность внедрения и использования технических средств максимальна, если компания четко понимает задачи, которые

предстоит решать при помощи инструментов SOC. Ниже представлена сводная таблица с возможными высокоуровневыми задачами, которые помогает решать Центр оперативного управления ИБ.

Мы рассмотрели лишь часть наиболее типовых задач, которые руководство компании может ставить перед подразделением, обеспечивающим информационную безопасность компании. Но стоит отметить, что перечисленные вопросы являются предпосылками разворачивания Центра оперативного управления ИБ.

### Какие выгоды получает компания при внедрении SOC?

Во-первых, при помощи SOC становится возможным организовать процесс непрерывного совершенствования защитных мер для обеспечения безопасности. Постоянный анализ текущих событий и инцидентов ИБ, выяснение причин их возникновения с привлечением различных подразделений позволяет оценить эффективность текущих мер защиты, понять их недостатки и выработать предложения по их замене или корректировке.

Во-вторых, внедрение SOC позволяет снизить прямые и непрямые затраты. При небольшом штате сотрудников, когда «не хватает рук», SOC позволяет сократить ресурсы, необходимые для ручной обработки событий ИБ и при увеличении количества контролируемых средств защиты. При этом не требует увеличения штата, а, напротив, позволяет оптимизировать работу сотрудников путем сведения данных на одну консоль и автоматизации проводимого анализа событий ИБ.

В-третьих, средствами Центра управления ИБ можно разделить полномочия контроля за ИТ-системами. Средства защиты, их администрирование и эксплуатация, как правило, находятся в ведении подразделения ИТ, в то время как ИБ отводятся только функции контроля. SOC — это, пожалуй, единственный инструмент контроля в руках у подразделений ИБ, позволяющий им отслеживать действия в ИТ-системах, что объективно снижает влияние человеческого фактора и повышает уровень информационной безопасности компании.

В-четвертых, наличие Центра оперативного управления просто необходимо при процедуре слияния или поглощения. Центр оперативного управления позволяет эффективно привести присоединяемую компанию в соответствие со стандартами ИБ, принятыми в головной организации. SOC дает возможность не только оперативно обнаружить расхождения, но и отследить их устранение с возможностью выставления и контроля соответствующих KPI ответственным за слияние подразделениям.

И, наконец, данные, предоставляемые SOC, существенно

| Задачи бизнеса | Решение с помощью SOC |
|---|---|
| **Сокращение расходов и потерь** | Создание Центра оперативного управления позволит сократить расходы за счет централизации управления, а также снизить ущерб, наносимый в результате возникновения инцидентов ИБ, за счет своевременного и эффективного реагирования. Использование процессного подхода делает реагирование и разрешение инцидентов ИБ более оперативным и позволяет использовать как собственный, так и мировой опыт по разрешению инцидентов ИБ. |
| **Повышение стоимости компании** | Центр оперативного управления ИБ повышает управляемость и стабильность компании, что ведет к увеличению ее стоимости.<br>Это становится особенно актуально, когда речь идет о слиянии и поглощении. Потенциальный собственник предпочитает понимать, какие инструменты используются для оперативного управления ИБ, ценит использование комплексного и системного подхода для решения задач ИБ. |
| **Соответствие требованиям законов и нормативных актов(как российских, так и международных)** | Наличие Центра оперативного управления свидетельствует о выполнении требований и рекомендаций по мониторингу и управлению инцидентами ИБ, прямо или косвенно присутствующих как в международных стандартах и нормативных актах (ISO/IEC 27001:2005,PCI DSS, Basel II, Sarbanes-Oxley Act), так и в российских (СТО БР, Федеральный закон о персональных данных (152-ФЗ), СТР-К, ГОСТ Р ИСО/МЭК 17799-2005). |
| **Управление операционными рисками** | Контроль операций и контроль конфигураций являются составляющими управления операционными рисками. Центры оперативного управления ИБ осуществляют мониторинг всех производимых действий, отслеживают факты изменений конфигурационных настроек, контролируют их соответствие установленным в компании требованиям, политикам.<br>Центр оперативного управления может быть использован как средство автоматизации при анализе рисков, предоставляя реальные данные о текущих уязвимостях и угрозах. |

**Рис. 3. Таблица с возможными высокоуровневыми задачами, которые Центр оперативного управления информационной безопасности помогает решать**

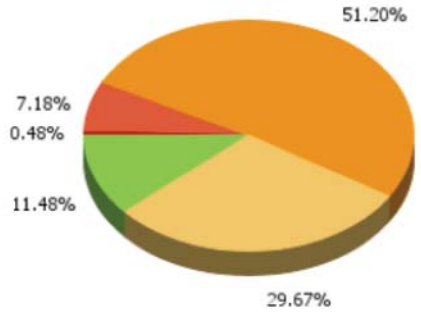
уточняют оценку рисков, которая является основой в выборе тех или иных мер защиты. Кроме того, формализация процедур снижает косвенные затраты компании, так как вопросы согласований без качественного обоснования занимают значительное количество рабочего времени сотрудников.

Какими средствами достигаются все эти цели и задачи? Давайте сделаем краткий экскурс в технологии Центра оперативного управления информационной безопасностью.

## Компоненты Центра Оперативного управления ИБ

Как уже отмечалось ранее, SOC — это комплекс организационно-технических мер. Компании, решившей внедрить SOC, в первую очередь, необходимо озаботиться созданием отдельного подразделения или группы специалистов, управляющих Центром. Это должны быть и аналитики, и администраторы, и операторы консолей централизованного мониторинга. Не менее важно формализовать процессы выявления и решения инцидентов ИБ. И если с организационной частью еще более-менее понятно, то при выборе технологий большинство заказчиков сталкиваются с трудностями.

Еще бы: на российский рынок за последние 2-3 года вышло огромное количество производителей продуктов по информационной безопасности, и выбрать из этого многообразия зачастую бывает крайне сложно. Проводить бесконечные тестирования и пилоты нецелесообразно, так как продукты этого направления тяжелые и сложные, тестирование может затянуться до 6-7 месяцев. А если надо провести испытания 3-4 конкурентных продуктов? Центр информационной безопасности компании «Инфосистемы Джет» может поделиться своим опытом. Наши эксперты провели тестирование и анализ практически всех присутствующих на российском рынке решений крупных производителей. Далее представлен обзор основных технологий типового Центра оперативного управления ИБ, которые имеют успешный опыт практического применения в наших проектах.




| Уровень | Количество уязвимостей | Доля уязвимостей |
|---|---|---|
| высокий уровень | 1 | 0.47% |
| высокий уровень (подозрение) | 15 | 7.17% |
| средний уровень | 107 | 51.19% |
| средний уровень (подозрение) | 62 | 29.66% |
| низкий уровень | 24 | 11.48% |
| Итого: | 209 | 100% |

**Рис. 4. Распределение уязвимостей по типу критичности**

### MaxPatrol – система контроля состояния ИБ

Система мониторинга состояния ИБ является одной из основополагающих и рекомендуемой к внедрению на первых этапах построения корпоративной системы защиты информации. Компания «Инфосистемы Джет» в качестве технологической платформы для построения SOC применяет продукты MaxPatrol производства компании Positive Technologies.

MaxPatrol представляет собой экспертную систему, используемую для обнаружений ошибок в защите ИТ-ресурсов. Применение системы позволяет:

- поддерживать в актуальном состоянии информацию об ИТ-парке;
- своевременно обнаруживать несанкционированные изменения;
- автоматически проводить инспекции на предмет поддержания компьютерных систем в защищенном состоянии.

Как следствие всего вышесказанного, система позволяет обнаруживать и своевременно устранять бреши в защите. Основными целями применения

системы обычно являются контроль эффективности процессов ИБ, контроль изменений и политик безопасности, инвентаризация ИТ-активов и оценка защищенности инфраструктуры компании.

Решение MaxPatrol является системой экспертного класса. Наиболее важный ее компонент — ежедневно обновляемая база знаний, которая содержит исчерпывающую информацию о существующих угрозах ИБ (вирусы, трояны, уязвимости прикладного обеспечения и т.п.). Поддержкой базы знаний занимаются ведущие эксперты отрасли. Информация содержит подробные рекомендации по устранению обнаруженных недостатков, требования к квалификации обслуживающего персонала. Уникальные эвристические проверки позволяют обнаруживать новые уязвимости и проверять нестандартные системы и системы собственной разработки.

Система MaxPatrol позволяет автоматизировать и централизовать процессы оценки эффективности управления ИТ- и ИБ-услугами, контроля состояния информационной безопасности, соответствия стандартам и поиска уязвимостей в информационных системах любого масштаба. Это дает возможность своевременно получать полную картину состояния защищенности, как всей системы, так и отдельных узлов.

### Какими могут быть предпосылки приобретения и внедрения системы MaxPatrol?

Зачастую процедуры инвентаризации, оценки защищенности и контроля политик безопасности проводятся нерегулярно либо с большими промежутками. Это приводит к тому, что информация теряет актуальность, и ситуация выходит из-под контроля. Комплексный подход и интеллектуальные средства автоматизации, реализованные в MaxPatrol, обеспечивают минимизацию трудозатрат, необходимых на решение задач мониторинга ИТ и ИБ, что позволяет своевре-

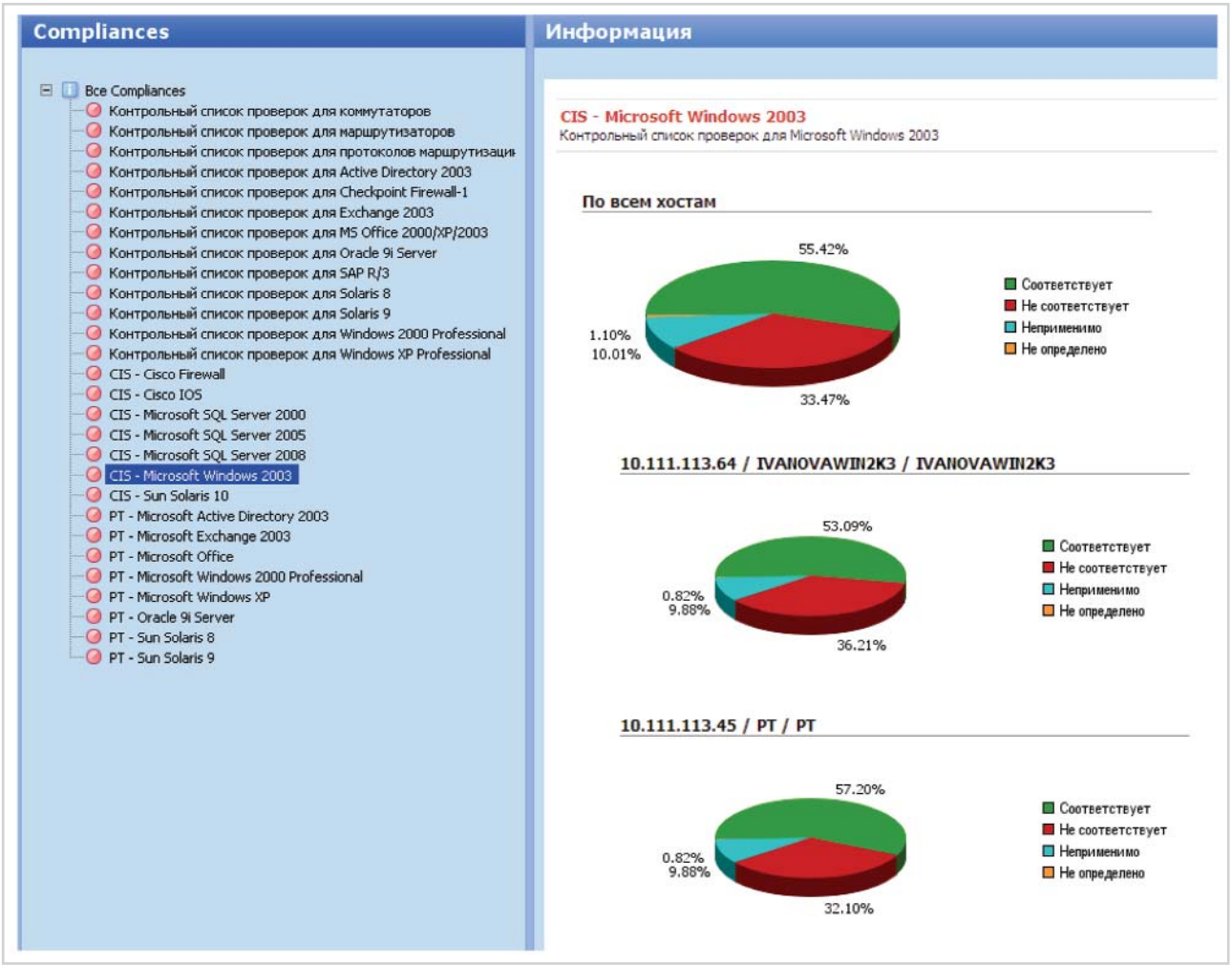



**Рис. 5. Информация по степени соответствия инфраструктуры компании требованиям CIS.**

менно обнаруживать проблемы, повышать управляемость и защищенность информационной системы.

Используя обширную и постоянно обновляемую базу знаний MaxPatrol, администраторы могут оперативно создавать эталонные шаблоны конфигураций систем, отслеживать несоответствующие требованиям политик безопасности системы и эффективно устранять обнаруженные недочеты. Механизмы генерации отчетов позволяют отслеживать изменения в защищенности отдельных узлов и подразделений, а также контролировать бизнес-метрики, такие как степень соответствия стандартам, эффективность устранения несоответствий, уровень контроля над информационной инфраструктурой. На рисунке 5 представлен верхнеуровневый отчет по соответствию рекомендациям PCI DSS (CIS Benchmarks).

Одним из факторов, влияющих на непрерывность работы ИТ- сервисов, ресурсов и систем, является состояние их конфигурационных настроек, отсутствие на рабочих станциях и серверах неразрешенных сервисов и ПО, наличие установленных обновлений и патчей. Ежедневно в прикладных системах, сетевых службах и операционных системах обнаруживаются новые ошибки и уязвимости.

В ведении ИТ-подразделений находится большое количество разнородного программного и аппаратного обеспечения — рабочие станции, серверы и сетевое оборудование головных офисов и территориальных управлений, — которое необходимо контролировать и следить за тем, что в нем происходит. Если этого не делать, то управлять ИТ-инфраструктурой становится невозможно.

В результате:

- настройки сетевого оборудования не соответствуют разработанным частным политикам и рекомендациям производителя;
- на серверах запущены неразрешенные сервисы, открыты неразрешенные порты;
- на рабочих станциях установлено нелицензионное или неразрешенное ПО;
- настройки рабочих станций не соответствуют разработанным частным политикам и рекомендациям производителя;
- на рабочих станциях и серверах антивирусное ПО не обновлено;
- системное ПО не обновлено и на него не установлены последние обновления безопасности.

Отсюда повышаются риски возникновения сбоев и отказов в работе ИТ-сервисов, ресурсов и систем. Частые сбои и отказы в работе ИТ-сервисов приводят к дезорганизации рабочих процессов и простою работников из-за невозможности выполнять свои должностные обязанности, и, в конечном итоге, к экономическому ущербу от недоступности ресурсов. Контролировать ИТ-инфраструктуру без определенных технических стандартов сложно. Поэтому необходимо определить конкретные технические требования (стандарты) для систем и осуществлять их контроль с помощью соответствующих средств автоматизации. Вручную это делать очень трудоемко и неэффективно.

Для повышения эффективности специалисты компании «Инфосистемы Джет» рекомендуют создать внутренние процессы, обеспечивающие непрерывный автоматизированный контроль информационных систем. Контроли должны реализовывать постоянный мониторинг и отслеживать изменения настроек сетевого оборудования, операционных систем серверов и рабочих станций.

**Важные действия:**

- организовать контроль соответствия информационных систем внутренним корпоративным требованиям и требованиям производителей;
- своевременно выявлять и устранять отклонения в ИС;
- оценивать эффективность деятельности ИТ-подразделений и процессов по контролю ИТ-инфраструктуры.

Таким образом, использование MaxPatrol позволит автоматизировать и централизовать процессы по управлению и контролю ИТ-инфраструктуры, предупредить различные типы инцидентов. Например, атаки внешних и внутренних злоумышленников, использование нелицензионного ПО, расхождение с требованиями технических стандартов и внутренних политик. При этом снизится экономический ущерб от недоступности ресурсов и потери конфиденциальной информации, а также будет выполнен ряд требований по информационной безопасности, предъявляемых международными платежными системами.

### Из чего состоит решение на базе MaxPatrol?

Система MaxPatrol построена на основе трехуровневой архитектуры, что обеспечивает высокое масштабирование и позволяет внедрять систему в крупных корпоративных сетях. Основным компонентом продукта является MP Server — модуль управления продуктом. Это серверный компонент, вы-

полняющий все основные функции распределенного сканера безопасности: сканирование, сбор данных, их обработку и сохранение в БД, формирование отчетов. В состав каждого MP Server входит модуль MP Scanner, который осуществляет сканирование. При необходимости к MP Server могут быть добавлены дополнительные сканеры, что позволяет увеличить производительность и учитывать топологию сети при сканировании (например, наличие межсетевых экранов и средств защиты). Кроме того, дополнительный сканер можно вынести за пределы исследуемого сегмента сети и одновременно выполнять сканирование как внутри сети, так и снаружи.

**Сервер консолидации (MP Consolidation Server)** аккумулирует информацию различных серверов MP Server и позволяет строить целостную картину защищенности крупной распределенной информационной системы. В качестве хранилища информации может использоваться внутренняя база данных или внешняя корпоративная СУБД. В качестве внешней СУБД используется Microsoft SQL Server 2000/2005.

**Локальный сервер обновлений (MP Local Update Server)** используется как единая точка поддержки базы знаний и исполняемых модулей компонентов в актуальном состоянии.

**Мобильный сервер (MP Mobile Server)** используется в качестве удобного рабочего инструмента аудиторов в области информационной безопасности. Это решение идеально подходит для проведения тестов на проникновение и аудитов внутренними аудиторами. Наличие встроенного модуля консолидации позволяет после проверки территориально удаленных сетей и подразделений (или физически изолированных сегментов) использовать результаты в общей отчетности, подготавливаемой продуктом, на базе MP Consolidation Server.

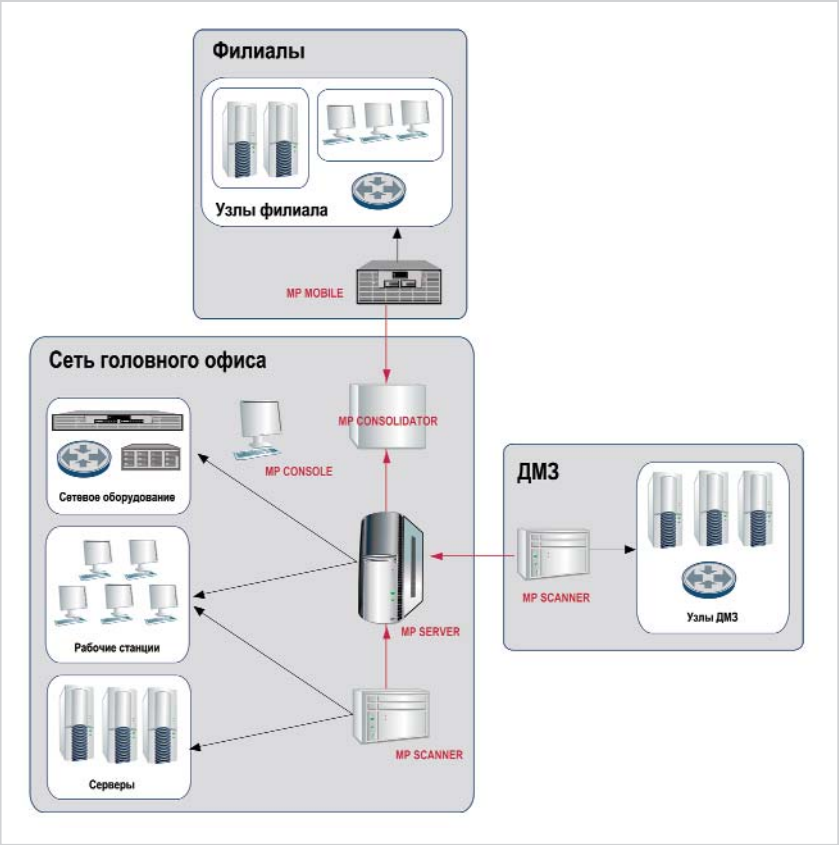



**Рис. 6. Пример архитектуры MaxPatrol для территориально-распределенной компании.**

Очевидно, что продукт MaxPatrol является корпоративным решением по мониторингу состояния информационной безопасности и способен решать задачи любой сложности в любых масштабах. Решение легко масштабируемо, все его компоненты централизуемы.

## Управление инцидентами ИБ

Управление инцидентами ИБ в рамках Центра мониторинга и управления информационной безопасностью реализуется набором организационных процессов и процедур. Они обеспечивают регистрацию, оперативное реагирование и эффективное разрешение инцидентов ИБ, а также полный цикл работы с инцидентами. От того, насколько быстро и грамотно компания среагирует и разрешит возникший инцидент ИБ, зависит размер наносимого ей ущерба. В связи с этим подготовка к разрешению инцидентов приобретает особое значение.

Подготовительный этап внедрения процессов включает планирование, определение ответственных, разграничение обязанностей, разработку планов по разрешению инцидентов и т.п. Далее осуществляется непосредственно регистрация инцидентов ИБ, реагирование на них и разрешение.

В процессе управления инцидентами ИБ важно не только разрешать их, но и анализировать эффективность принимаемых мер. Необходимо периоди-

чески тестировать разработанные планы для поддержания их в актуальном рабочем состоянии и для своевременной корректировки. Кроме того, нужно проводить анализ произошедших инцидентов с целью принятия мер проактивной защиты.

Если при анализе выявлены незначительные отклонения, то проводятся корректирующие действия. Если же выявлены системные ошибки, обнаружена неэффективность применяемых планов и т.п., производится активация подготовительного этапа.

### Система управления (мониторинга) событиями ИБ

Система управления событиями ИБ, входящая в состав Центра, реализует комплексный подход к решению задач сбора, анализа (корреляции) и контроля событий ИБ от различных

| Сотрудник службы безопасности | Должностные обязанности | Необходимая информация / требующиеся инструменты | Решение |
|---|---|---|---|
| **Руководитель** | Посредник между бизнесом и службой безопасности; постановка задач, обоснование бюджета | Общее состояние безопасности; Система показателей безопасности | Информационная панель с графиками и таблицами, разнообразные отчеты |
| **Архитектор ИБ** | Создание и поддержка политики ИБ и защитных мер. Общее понимание состояния безопасности и соответствия нормативным требованиям | Показатели эффективности применения политики и защитных мер | Разнообразные отчеты (по безопасности и выполнению нормативных требований), стандартные и легко изменяемые информационные панели, отчеты за исторический период и о тенденциях |
| **Менеджер ИБ** | Контроль использования ресурсов и бюджетных средств службы безопасности, контроль реакции на инциденты | Показатели по ресурсам и безопасности, в том числе статистика по реакциям на инциденты | Информационные панели состояния безопасности и производительности, в том числе: распределение нагрузки участников группы, частота инцидентов, распределение заданий по приоритетам для распределения задач, а также информационные панели по уязвимостям, в том числе для наиболее уязвимых данных, отсортированных по степени важности для бизнеса |
| **Аналитик** | Наблюдение за консолями управления, настройка устройств и управление уязвимостями, обнаружение инцидентов, реагирование на сигналы тревоги, проведение расследований, устранение проблем, техническое консультирование | Состояние данных и уязвимостей, информация об угрозах, данные в реальном времени и история предыдущих событий, исходная информация , информация о политиках и идентификационные данные. Требуется процедура совместной обработки возникающих инцидентов, инструменты для анализа событий, имеющих высокую степень риска | Информация о событиях, активах, базовом уровне активности, данные о уязвимостях для уменьшения числа ложных срабатываний и оповещений в реальном времени о событиях с высокой степенью риска; разнообразные правила корреляции (например, SANS Top 20); автоматические списки особого внимания (например, мониторинг деятельности привилегированных пользователя ); замкнутый цикл совместного управления инцидентами, начиная от поиска и идентификации и заканчивая разрешением, закрытием и архивированием |

**Рис. 7. Повышение эффективности работы службы безопасности**

средств защиты. Это позволяет в режиме реального времени эффективно идентифицировать инциденты ИБ с дальнейшей передачей их в систему управления инцидентами, получать реальные данные для анализа и оценки рисков, для принятия обоснованных и адекватных имеющимся рискам решений по обеспечению ИБ.

Система сбора и корреляции событий информационной безопасности является в своем роде «шиной», базовым инструментом для выявления и расследования инцидентов ИБ. Целями внедрения систем мониторинга событий, в большинстве случаев, являются сокращение ущерба от инцидентов ИБ за счет оперативного их обнаружения и реагирования. За счет формализации и автоматизации процесса управления инцидентами удается достичь сокращения затрат, а также повысить степень соответствия требованиям российских и международных стандартов.

Внедрение систем этого класса помогает значительно повысить эффективность работы службы информационной безопасности и предоставит всем технологическим подразделениям компании инструмент для автоматизированной обработки событий.

Говоря об эффективности обеспечения информационной безопасности, нельзя забывать, что эффективность достигается действиями людей, работающих в службе безопасности. Ниже мы приводим сводную таблицу соответствия ролей, требований и необходимых инструментов SOC для типового подразделения ИБ.

По нашему мнению, наиболее популярные и технически завершенные продукты на текущий момент — это ArcSight Enterprise Security Manager, RSA enVision, Symantec Security Information Manager.

Эти продукты позволяют реализовать практически любую задачу, связанную со сбором событий, анализом и выявлением угроз информационной безопасности. Ниже мы рассмотрим каждый из них по отдельности и остановимся на их преимуществах и различиях.

Начнем обзор с продукта компании HP ArcSight — лидера мирового и российского рынка решений SIEM (Security Information and Event Management).

## ArcSight ESM

Продукт компании ArcSight, приобретенной недавно компанией HP, на данный момент является лидером отрасли, как по количеству внедрений в России и за рубежом, так и по функциональным возможностям. Устанавливается как в виде ПО, так и в виде программно-аппаратных комплексов, что дает уникальную гибкость при выборе архитектуры внедрения и планировании масштабируемости решения. Это дает возможность получить детальный контроль и прогнозируемость стоимости системы в целом.

Решения Arcsight предназначены для сбора, обработки, корреляции и реагирования на события информационной безопасности, обладают свойствами масштабируемости, надежности, расширяемости и отказоустойчивости. Решения построены на базе продукта **ArcSight Enterprise Security Solution**, ядром которого служит продукт **ArcSight ESM (Enterprise Security Manager).** Данный продукт обеспечивает сбор, обработку и хранение событий безопасности, которые могут поступать из различных источников. **ArcSight ESM** поддерживает интеграцию с большим количеством прикладных систем и устройств (всего их около трех сотен) и поставляется с несколькими тысячами предустановленных правил корреляции. В состав системы входит агент Flex Connector, он позволяет осуществлять интеграцию с любым типом приложений и устройств.

Хранение и анализ журналов аудита производится с помощью решения **ArcSight Logger** — программно-аппаратного комплекса, которой может фиксировать и анализировать все данные журналов аудита организации, предоставляя сжатый и экономичный репозитарий для хранения логов.

Для более простого и эффективного сбора информации о событиях безопасности в составе решения на базе **ArcSight** могут использоваться программно-аппаратные комплексы ArcSight Connectors. Эти устройства являются первым эшелоном сбора и обработки событий, приводя логи к формату ArcSight. Далее обработанные события из устройств Connector Appliance пересылаются либо в базу данных ESM, либо на устройства Logger.

Классическая архитектура решения на базе продуктов ArcSight представлена на рис.8. При такой архитектуре нормализованные события хранятся в базе данных ESM, а оригиналы журналов событий могут быть отправлены на устройства Logger для хранения и отчетности перед аудиторами, которые предъявляют требования к неизменности логов.

Более подробно о продуктах ArcSight можно ознакомиться на сайте производителя по адресу www.arcsight.com.

Далее мы рассмотрим основные особенности продуктов ArcSight. Решения данного

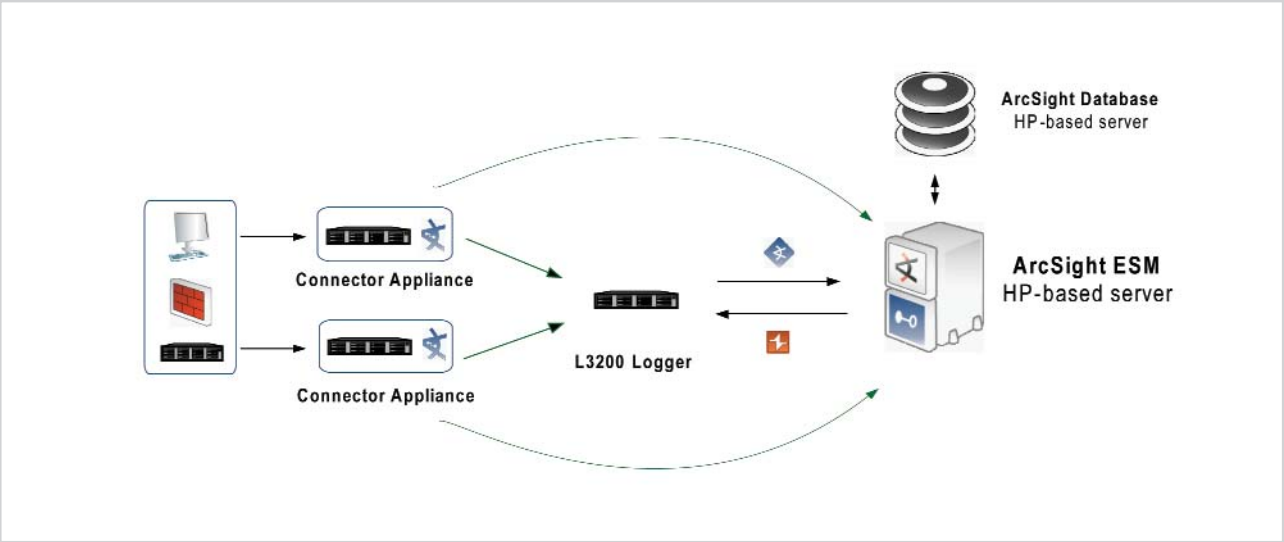



**Рис. 8. Архитектура системы сбора и анализа событий ИБ на базе продуктов ArcSight.**

класса являются «шиной» для всех остальных компонентов центра управления ИБ и, если так можно выразиться, его мозгом.

Продукт ArcSight ESM позволяет собирать и анализировать сообщения о нарушениях безопасности, поступающих от систем обнаружения вторжений, межсетевых экранов, операционных систем, приложений, антивирусных систем и любых других источников событий. Данная информация собирается в едином центре, обрабатывается и подвергается анализу в соответствии с заданными правилами по обработке событий, связанных с безопасностью.

Технология работы ArcSight ESM предусматривает обработку событий безопасности в четыре фазы: нормализация, агрегирование, корреляция и визуализация. В фазе нормализации и агрегирования события безопасности собираются из всех систем обнаружения вторжений (межсетевых экранов, операционных систем, приложений и антивирусных систем) и приводятся к единому формату сообщений Common Event Format (CEF). Сформированные сообщения коррелируются между собой. Механизмы корреляции основаны как на статистических методах, так и на дополнительно создаваемых правилах. ArcSight ESM отображает полученные результаты на централизованную консоль (разработанную на технологии Java), работающую в режиме реального времени.

Агрегирование событий — процесс удаления дублированных событий для уменьшения количества поступающих данных и экономии времени их последующей обработки и анализа. Это особенно важно, например, при сканировании портов, когда одинаковые события многократно генерируются межсетевыми экранами. Агрегирование событий также используется для удаления дублирований от множества IDS-систем.

Не менее интересными и важными при работе с событиями являются механизмы корреляции. ArcSight ESM уникально сочетает в себе две технологии корреляции, т.е. идентификации атак, которые не могут быть выявлены из одного события. Первая основана на правилах корреляции и отделяет ложные сообщения о нарушении безопасности от важных инцидентов. Она активирует правила политик безопасности. Сценарии подозрительной активности могут создаваться разработчиками программного обеспечения, консалтинговыми фирмами и самими пользователями. Вторая технология — статистическая корреляция — основывается на категоризации и оценке угроз, применяется для выявления потенциальных нарушений и аномалий безопасности. Обе технологии различны по способу работы и дополняют друг друга.

Коррелировать можно события не только из журналов операционных систем или логов сетевых устройств, это могут быть и более сложные события из разных компонент SOC. Так, в последнее время становится популярной и доказывает свою эффективность схема централизации анализа событий, полученных от различных продуктов SOC, таких как MaxPatrol, Imperva, IBM Guardium и даже других SIM-систем, например, Cisco MARS или enVision (см. рис.9). Такая реализация позволяет уменьшить скорость обработки событий и увеличить шансы выявления угроз.

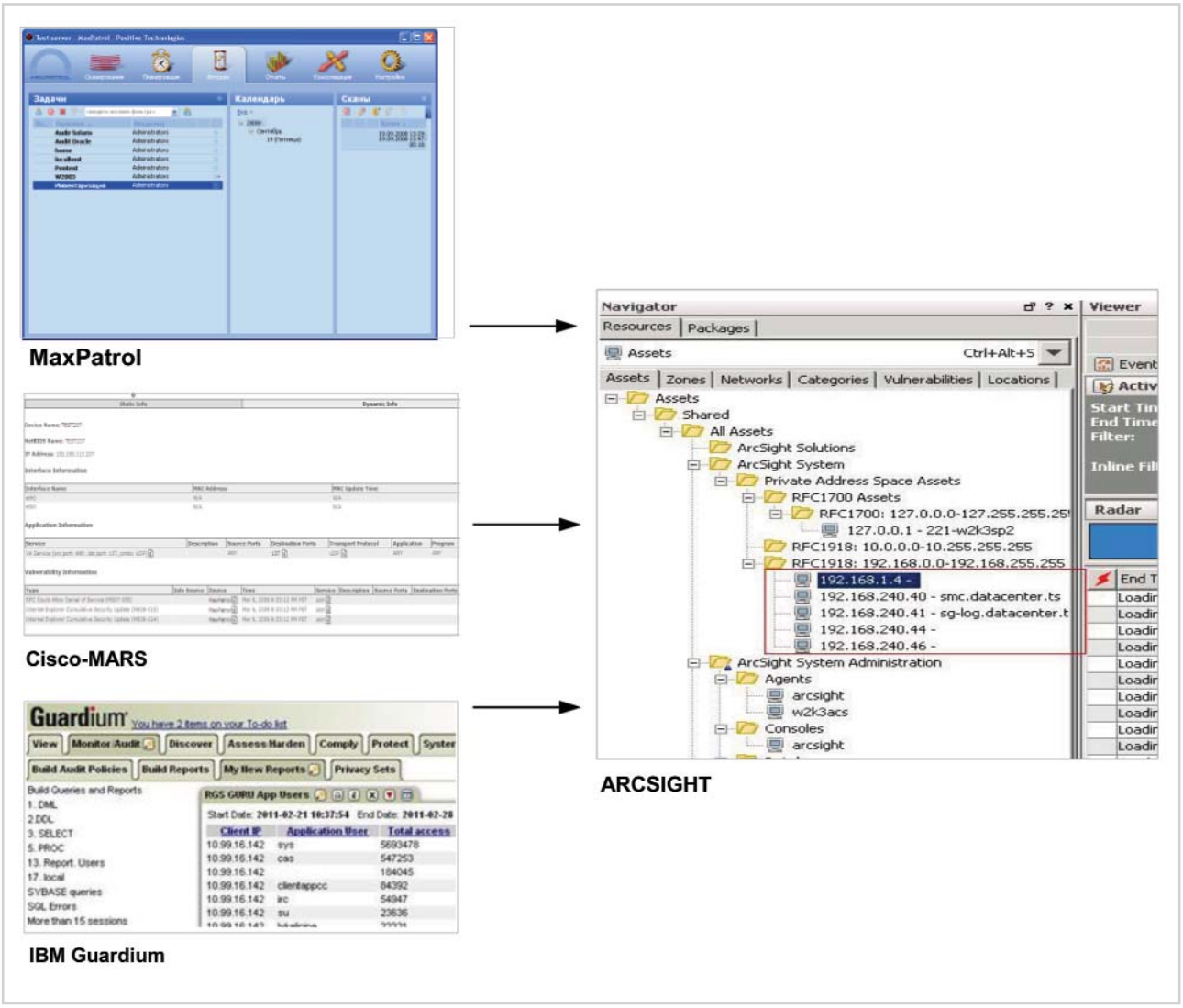



**Рис. 9. Объединение различных компонент SOC с помощью ArcSight.**

С использованием возможностей визуализации ArcSight ESM операторы, аналитики и администраторы могут оперативно получать всю информацию о состоянии безопасности сети, а также проводить при необходимости расследования нарушений безопасности и реагировать на них до того момента, как они начнут воздействовать на критически важные информационные ресурсы. Уникальность решений ArcSight состоит в том, что ими могут пользоваться как специалисты по безопасности, аналитики или аудиторы, так и руководители подразделений ИБ, отслеживая высокоуровневые показатели через консоль визуализации.

Внедрение системы мониторинга на основе продуктов ArcSight дает возможность автоматизировать процесс принятия решений по реагированию на события, связанные с нарушением безопасности. При этом применение систем мониторинга также позволяет значительно повысить эффективность уже установленных в организации средств защиты.

Закономерно возникает вопрос, какие же события можно и нужно отслеживать? Какие отчеты настраивать, какие параметры должны выводиться на консоли онлайн мониторинга?

По нашему опыту, если говорить об общих задачах и направленности отчетов, то, как правило, речь идет о формировании отчётов о частоте срабатывания правил межсетевых экранов и изменении настроек сетевого оборудования. Это позволяет оптимизировать работу межсетевого экрана за счет регулирования порядка срабатывания правил и гибкого аудита параметров настроек. Также важны отчеты о наличии антивирусных средств и их обновлений на наблюдаемых системах, оповещение об измене-

**Рис. 10. Пример консоли оперативного управления событиями для аналитика.**

ниях конфигурации критических систем, журналирование доступа к файлам аудита, контроль целостности данных файлов и аудит внутренних ресурсов системы.

Выполнение задач, связанных с управлением учетными записями пользователей, обычно реализуется контролем изменений парольной политики (отслеживание изменений привилегий учетной записи пользователя в домене, изменения и добавление новых пользователей, создание учетных записей с правами локального администратора, а также создание и удаление учетной записи в течение короткого промежутка времени).

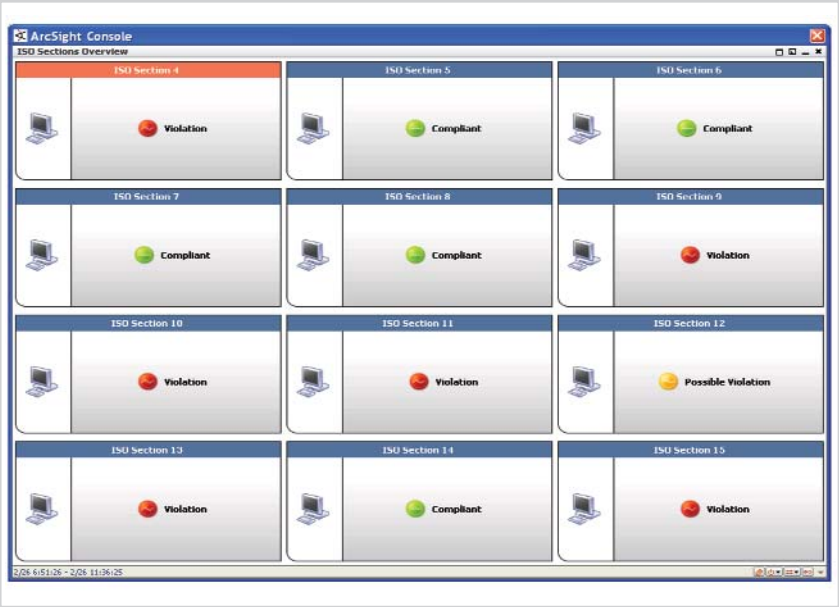



**Рис. 11. Пример так любимой руководителями «большой красной кнопки» в интерфейсе ArcSight.**

Часто системы класса SIEM позиционируются как системы контроля действий всех пользователей. Это довольно размытое понятие. Что же можно реализовать с помощью ArcSight? Наши эксперты отмечают, что наиболее интересно и эффективно отслеживание нескольких следующих подряд (число N задается в системе) неудачных попыток зарегистрироваться в домене в течение X минут, обнаружение регистрации в информационной системе пользователя, находящегося в командировке или в отпуске. Кроме того, полезно контролировать использование административ-

ного доступа к информационным системам (ресурсам) по незащищённым протоколам и использование административных привилегий пользователями, которым такой доступ не был предоставлен. Система учетных записей пользователей является одним из уязвимых мест в любой инфраструктуре. С помощью решений ArcSight можно контролировать использование учетных записей, установленных производителем оборудования, а также отслеживать факты повторного использования учетных записей пользователей, уже активных в системе. Эти и другие прикладные задачи система наглядно визуализирует и выводит на экран, что очень удобно.

Практически любая организация имеет в своем парке оборудование Cisco, в крупных компаниях его количество может достигать нескольких сотен единиц. Это порождает проблемы с обработкой огромного количества событий, генерируемых устройствами. Некоторые компании ограничивают срок хранения журналов несколькими часами, что делает невозможным расследование инцидентов месячной или даже недельной давности. Такие системы, как ArcSight позволяют не только сохранять длительное время все события с устройств Cisco, но и решать ряд прикладных задач, таких как обнаружение и предотвращение несанкционированного доступа в корпоративную сеть или сетевых атак на сеть и отдельные сервисы. Система может вести аудит действий администраторов сетевого оборудования. Из интересных событий обычно выделяют отслеживание входа/выхода на устройства с оповещением о событиях авторизации на АСО Cisco по встроенным учетным записям с запрещенных сетевых сегментов сети или отслеживание событий об изменении конфигураций оборудования Cisco. Кроме того, возможно отслеживать активность, направленную на сканирование сети или наличие вредоносного программного обеспечения во внутренней сети компании. Спектр решаемых задач чрезвычайно широк и ограничивается только фантазией администратора ArcSight или специалиста по информационной безопасности.

## RSA enVision

Другим сильным игроком рынка решений для сбора и анализа событий информационной безопасности, на наш взгляд, является решение RSA enVision производства компании EMC. Платформа RSA enVision позволяет организации построить единое интегрированное решение по управлению журналами регистрации событий по типу «три в одном», упрощая соблюдение отраслевых нормативных требований, повышая безопасность и снижая риски, а также оптимизируя ИТ-инфраструктуру и ее обслуживание. Все эти преимущества достигаются

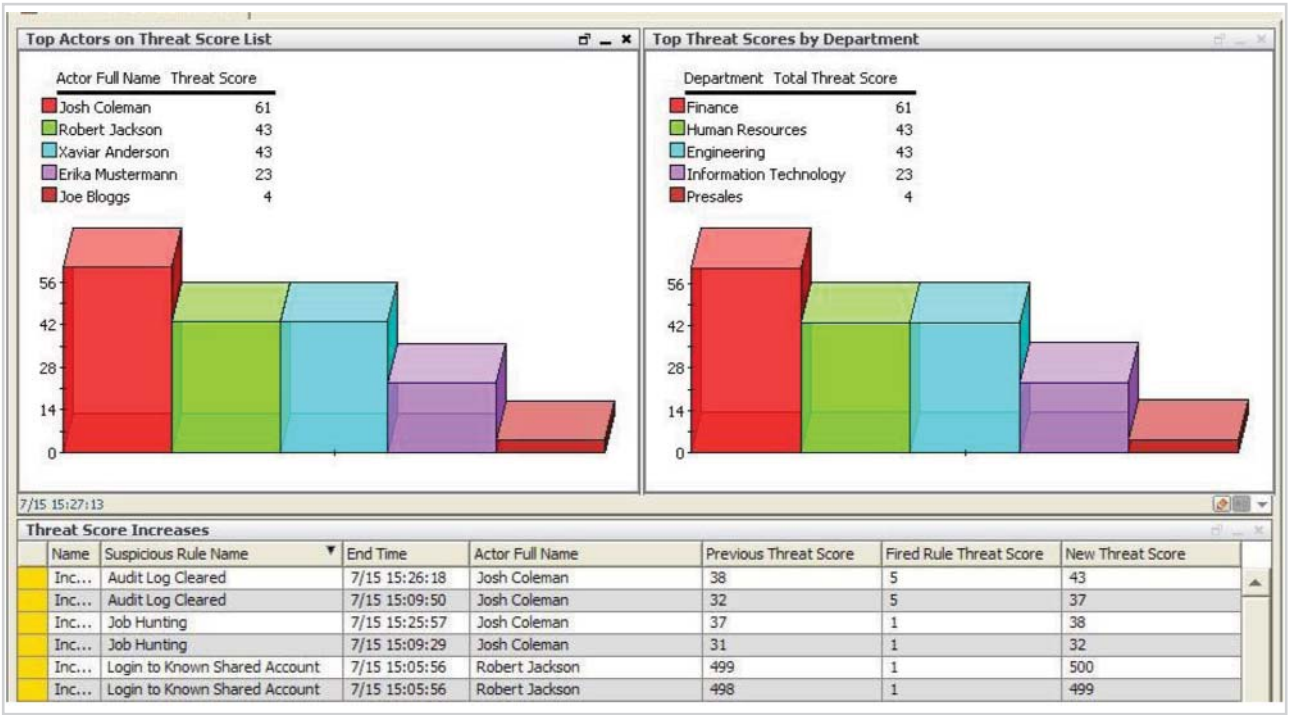



**Рис. 12. Визуализация действий пользователей и выявление нарушителей.**

**Joachim Kuehne, Senior Regional Sales Director, HP:**

«Обеспечение безопасности и защищенности информации в организации — нетривиальная задача. В прошлом основное внимание уделялось вирусам, ботам, червям и хакерским атакам, исходящим извне организации. Сейчас и в ближайшем будущем компаниям приходится уделять все больше и больше внимания утечкам информации, финансовым махинациям и различного рода мошенническим действиям, исходящим от сотрудников самой организации. Все новые требования регуляторов и законодательные акты, связанные с обеспечением безопасности информации, направлены на то, чтобы выявить и предотвратить именно эти внутренние угрозы.

Никогда еще не было так сложно обеспечить защищенность бизнеса. Как следствие, ценность автоматизированных систем мониторинга событий информационной безопасности, обеспечивающих выполнение требований регуляторов, как никогда высока. Современная система сбора и анализа событий ИБ (SIEM, Security Information and Event Management system) должна уметь собирать события ИБ, анализировать их и выявлять риски, связанные с информационной безопасностью, что позволит оперативно идентифицировать, определять приоритеты и пресекать утечки информации, хакерские атаки и внутренние угрозы.

Платформа Enterprise Threat and Risk Management (ETRM) на базе продуктов и решений ArcSight позволяет коррелировать события от различных информационных систем с информацией о ролях пользователей и сетевым трафиком для выявления нарушителей информационной безопасности, понимания что произошло, когда и где. Продукты ArcSight — это решения настоящего и будущего. Мы предоставляем систему мониторинга, которая нужна вам уже сегодня, но такие технологии, как виртуализация, облачные вычисления и современные сложные бизнес-приложения становятся все более и более важными в инфраструктуре любой организации. Решения ArcSight позволяют решать задачи по обеспечению информационной безопасности этих современных сервисов и технологий уже сейчас, при помощи платформы ETRM».

благодаря автоматическому сбору, анализу, оповещению об инцидентах, аудиту журналов регистрации событий, подготовке отчетов и надежному хранению всех журналов регистрации.

Система RSA enVision решает целый спектр задач. Это и сбор событий от устройств, и аудит действий администраторов/пользователей ИС. Система также обеспечивает корреляцию событий, хранение событий информационной безопасности с возможностью их последующего анализа и обработки за период не менее трех лет, контроля получения данных со всего оборудования, в том числе технологических сетей, и оповещении при его сбоях.

При этом RSA enVision для каждого получаемого события ИБ содержит следующую информацию:

- IP адрес (ID, hostname) узла;
- IP адрес (ID, hostname) терминала, с которого выполнялись команды;
- идентификатор пользователя;
- тип сообщения;
- время и дату сообщения;
- исходное тело сообщения, разбитое по полям.

Платформа RSA enVision позволяет извлекать журнальные файлы одновременно из десятков тысяч устройств, включая Windows-серверы, межсетевые экраны Checkpoint и маршрутизаторы Cisco без установки на них агентов, что гарантирует непрерывность и полноту сбора данных.

**Более подробно с возможностями платформы можно ознакомиться на сайте производителя по адресу www.rsa.com.**

Используя собственную передовую разработку — архитектуру IPDB, уже применяемую в сотнях организациях по всему миру, RSA enVision способен собирать все данные на всех уровнях информационной инфраструктуры — от сетевых устройств до приложений. Подсистема анализа LogSmart IPDB анализирует как поступающие в реальном времени, так и уже сохраненные данные. Подсистема предоставляет информацию в виде срезов данных и отчетов, способных удовлетворить широкий диапазон потребностей заинтересованных лиц организации — от IT-департамента до департамента безопасности, от контроля соответствия политик и анализа рисков до руководства компании. Особенность подсистемы LogSmart IPDB в том, что она не использует приложения третьих производителей, это и определяет ее беспрецедентное быстродействие. Данный показатель крайне важен в сетях

сложной и разветвленной архитектуры.

Платформу RSA enVision можно развернуть либо как автономное «plug-and-play» решение, либо как часть масштабируемой отказоустойчивой распределенной архитектуры для того, чтобы соответствовать требованиям крупной корпоративной сети. Вне зависимости от выбранного решения, оно будет включать в себя все необходимое программное обеспечение без каких-либо дополнительных затрат. Администрирование через Web-интерфейс и наличие Event Explorer, нашего весьма развитого аналитического инструмента, обеспечивают функционал для интуитивного контроля и расширенного, тщательно детализированного расследования инцидентов.

При развертывании в качестве автономного решения (серия ES) один функционально полный и защищенный аппаратно-программный комплекс (АПК) выполняет и сбор, и обработку, и анализ, и хранение данных.

В случае выбора распределенной архитектуры (серия LS), в требуемых местах устанавливаются специализированные АПК, каждый из которых выполняет свою ключевую задачу: локальные и удаленные сборщики осуществляют сбор данных, серверы данных управляют собранными данными, а прикладные серверы производят анализ данных и генерацию отчетов. Сами данные могут храниться с использованием разнообразных решений из широкого набора систем хранения от RSA и EMC.

Обратим внимание на отличительные особенности данного продукта. В первую очередь, стоит отметить комплексный подход производителя к безопасности. Всем известны продукты RSA SecurID, системы хранения от EMC материнской компании RSA, а также недавно приобретенный продукт Netwitness, который является новейшей разработкой и последним словом ИТ- технологий в информационной безопасности. Это обеспечивает легкую интеграцию различных компонентов системы мониторинга и указывает на серьезность подхода к информационной безопасности.

Продукт RSA enVision имеет ряд функциональных особенностей, благодаря которым он популярен и используется наравне с продуктами ArcSight. В

**Рис. 13. Web-интерфейс Event Explorer от RSA**

России несколько компаний используют продукт enVision совместно с ArcSight, решая сложные задачи по мониторингу событий ИБ в технологических сетях. К технологическому оборудованию относят устройства таких производителей, как Ericsson, Siemens, Nokia, Cisco VPN, терминальные сервера Citrix и аналогичные.

Данные задачи появились благодаря тому, что административные функции по управлению технологическим оборудованием выполняются не сотрудниками компании, а сторонней организацией, т.е. управление передается на аутсорсинг. В связи с этим возникла потребность по тотальному контролю всех операций на таких системах. Здесь продукт enVision оказался удобнее ArcSight, поскольку первый уже имеет встроенную систему хранения IPDB и собранные данные хранятся в неизменном виде, в защищенном от изменений формате. Эти данные могут являться доказательной базой при расследовании инцидентов и могут храниться длительное время из-за различных механизмов сжатия. Благодаря технологиям IPDB устройства RSA enVision могут гарантировать высокую производительность сбора данных при скромных требованиях к аппаратному обеспечению, обходясь без тяжелой артиллерии в виде SAN, кластеров Oracle и т.п.

Высокая скорость обработки входных данных позволяет упростить процесс настройки системы — на начальном этапе внедрения нет необходимости разбираться, какие события сохранять, какие отфильтровывать, а какие обрабатывать в режиме реального времени.

Обратим внимание, на практике оказалось, что подключить нестандартное устройство с плохо структурированным журналом событий проще, чем в ArcSight, в котором требуется сложная разработка специальных коннекторов, длительный разбор форматов логов в специализированной среде разработки.

Кроме того, есть специальная методика, которая позволяет подключать новые журналы постепенно, то есть разбирать новые сообщения шаг за шагом и добавлять их в парсер по мере обработки. При этом новые парсеры можно использовать и для собранных ранее данных.

Вышеописанные особенности позволяют не только собирать события со специфических устройств технологической сети, но и проводить их корреляцию, а также выявлять инциденты. Кроме того, корреляцию в данном случае возможно осуществить и с событиями, собранными с устройств по безопасности, рабочих станций и других классических источников событий ИБ.

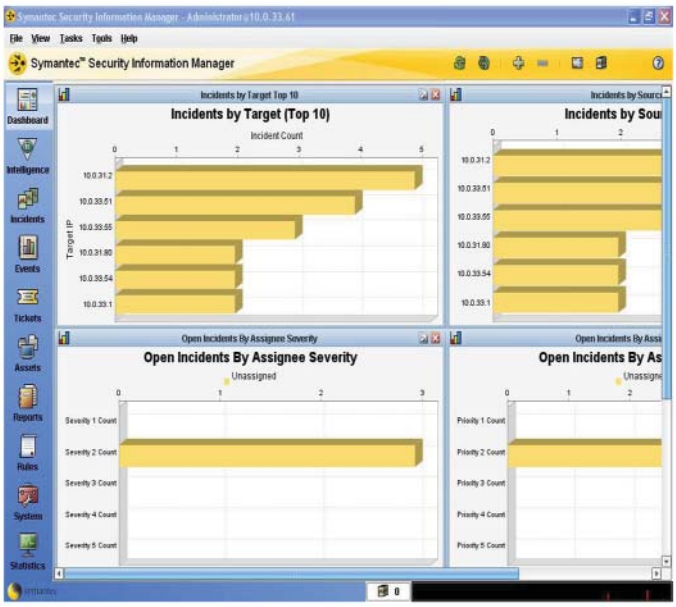



**Рис. 14. Удобство управления инцидентами с помощью SSIM**

## Symantec Security Information Manager

Длительное время одним из самых популярных в России продуктов для мониторинга и управления инцидентами информационной безопасности был продукт Security Information Manager производства компании Symantec. Как и конкурентные решения, SSIM выполняет функции сбора событий ИБ с различных устройств и приложений, аналитики и выявления инцидентов ИБ. На основе собранных данных Symantec SIM помогает выявлять угрозы безопасности, направленные на наиболее важные бизнес-приложения, определять их приоритеты, анализировать и устранять эти угрозы.

Сопоставление недостатков защиты сети и хостов в режиме реального времени с помощью службы **Symantec Global Intelligence Network** — одно из ключевых преимуществ данного продукта, делающее его системой оперативного реагирования на инциденты с акцентом на обеспечение безопасности наиболее важных для бизнеса информационных ресурсов.

Symantec Global Intelligence Network представляет собой глобальную сеть, использующую ловушки для обнаружения злонамеренной активности по всему миру. Вся эта информация перерабатывается в правила и используется в Symantec SIM при анализе и корреляции событий.

Анализ безопасности в режиме реального времени осуществляется с использованием внешнего стандарта выявления угроз безопасности — процесс, описанный в открытых стандартах **Distributed Management Task Force (DMTF).** Данный метод предусматривает классификацию угроз и проблем безопасности с учетом степени воздействия события на среду, способа атаки и целевых ресурсов. Такая классификация, называемая «Эффекты, механизмы и ресурсы» (EMR), лежит в основе модуля анализа данных Symantec SIM. Благодаря гибкости интеллектуальных правил на основе шаблонов, отдельное правило может занять место нескольких более конкретных, применяемых в стандартных подходах. В результате значительно упрощается процедура обслуживания и создания правил, которые могут охватывать множество условий.

Напомним, что кроме сбора данных организации должны соблюдать официальные требования по хранению архивов, обеспечивая надлежащую работу средств хранения и извлечения данных. Продукт Symantec SIM превосходит стандартные продукты контроля информации о безопасности на основе реляционных баз данных, для которых характерны дополнительные начальные затраты и необходимость длительного администрирования баз данных. С Symantec SIM не требуется администрирование базы данных. Кроме того, он сохраняет события в архивных файлах в указанном месте. Архив реализован в виде самостоятельного модуля, который отслеживает использование диска и срок хранения отдельных архивных файлов. При достижении указанного ограничения дисковой памяти или даты истечения срока действия файла Symantec SIM удаляет старые архивные файлы, чтобы освободить место новым. Для хранения файлов можно выбрать программно-аппаратный комплекс, напрямую подключенный диск (DAS), сетевое устройство хранения (NAS) или сеть хранения данных (SAN). Важное преимущество архивов Symantec SIM в том, что они работают быстрее обычных баз данных, поскольку в отличие от нескольких сотен функций базы данных они оптимизированы для выполнения одной задачи — сохранения большого объема событий. Коэффициент сжатия в Symantec SIM достигает 30:1. Нормализованные данные вместе с исходной информацией о событиях фиксируются и сохраняются для анализа происшествий. И, наконец, для обеспечения конфиденциальности и целостности архивы имеют электронную цифровую подпись.

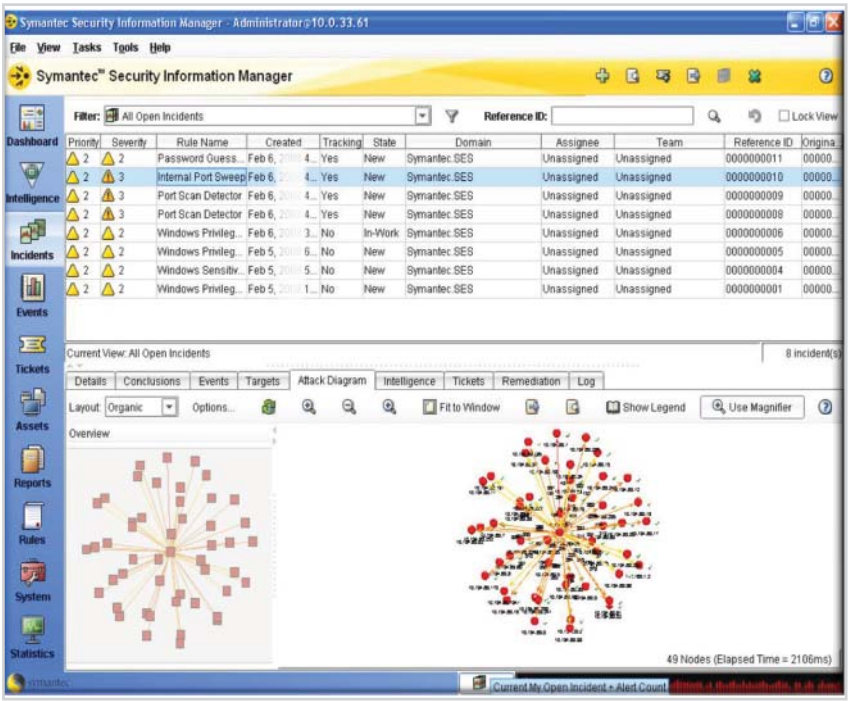



**Рис. 15. Административная консоль позволяет отслеживать не только техническую информацию, но и строить карты событий верхнего уровня.**

Сильной стороной продукта также является подход производителя к комплексным решениям. Всем известны средства защиты конечных станций SEP, продукты защиты от утечек информации Symantec DLP и другие решения в области ИБ от Symantec.

Завершая обзор основных решений в области мониторинга и управления инцидентами информационной безопасности хочется отметить следующее. Все рассмотренные продукты являются лидерами в своей нише и с их помощью можно решать практически любые зада-

чи, связанные со сбором и анализом событий ИБ.

Далее поговорим о достаточно новом для России направлении — решениях для контроля действий пользователей в базах данных и бизнес-приложениях. Эта область обеспечения ИБ только набирает популярность, хотя контроль транзакций в корпоративных базах данных, на наш взгляд, — один из ключевых моментов в комплексной системе обеспечения информационной безопасности.

## Контроль действий пользователей баз данных и приложений

Системы электронного документооборота, хранилища персональных данных, данные о платежных картах клиентов имеют постоянно растущую коммерческую ценность и стали основной целью для злоумышленников. Повсеместное внедрение веб-приложений, появление новых сервисов, лавинообразное расширение ИТ-инфраструктуры организаций привело к невозможности контролировать обычными средствами информационные потоки в базах данных, действия пользователей с данными бизнес-приложений. В ответ на эти тенденции появились специализированные системы для обеспечения безопасности таких сложных, многозвенных, территориально-распределенных систем.

Функционал мониторинга активности в базах данных попытались реализовать все основные производители СУБД и бизнес-приложений, но преимущества встроенных средств контроля порождают и их недостатки. Средства СУБД недостаточно гибкие для определения различий между пользователем и злоумышленником. Использование родных средств журналирования приводит к многократному увеличению нагрузки на серверы, падает производительность приложений и качество предоставляемых сервисов.

Средства контроля трафика запросов к БД от третьих производителей на отечественном рынке появились сравнительно недавно. Интерес к этим средствам вызван все возрастающей проблемой внутренних злоумышленников, участившимися случаями воровства данных, а также наличием различных нормативных документов, требующих обеспечить контроль доступа к конфиденциальным данным.

Системы аудита и контроля действий пользователей баз данных позволяют регистрировать активности пользователей на уровне БД и проводить анализ собранной информации. Это позволяет в режиме реального времени рассылать уведомления и подготавливать отчеты о том, кто получает доступ и к какой именно информации, а также как эти действия могут нарушить требования внешних регулирующих органов или внутренние правила безопасности.

Сейчас практически каждая организация использует веб-приложения (например, интернет банкинг), бизнес-приложения, такие как SAP, OEBS, Siebel и частной разработки. Большинство таких приложений работает по трехзвенной архитектуре. Такая архитектура выбрана для оптимизации производительности приложений и осуществляется применением метода «connection pooling», при котором используется единая учетная запись для доступа к базе данных. Данный метод скрывает имена конечных пользователей приложений, осуществляющих доступ к БД, то есть становится невозможным идентификация конечного пользователя приложения, запросившего информацию. Пользователь СУБД для пула соединений будет один — AppUser.

Такой метод организации доступа пользователей бизнес-приложений к информации, хранящейся в корпоративных базах данных дает ряд преимуществ, таких как повышение производительности работы приложения, снижение нагрузки на СУБД и т.п., но в то же время снижает уровень информационной безопасности приложения, так как становит-

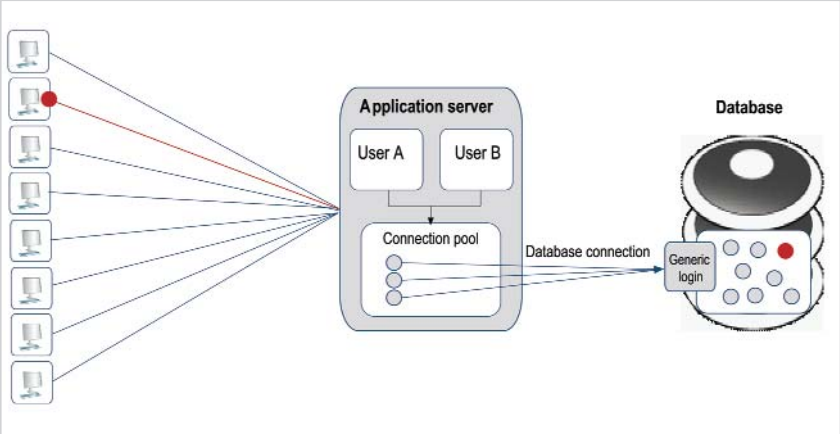



**Рис. 16. Применение метода «connection pooling» при организации доступа к БД пользователей приложения**

ся невозможно контролировать действия конечных пользователей.

Таким образом, смещая баланс в сторону повышения уровня информационной безопасности, приходится жертвовать качеством сервисов, и наоборот.

Оптимальным выходом видится использование специализированных решений, которые бы взяли на себя функционал по контролю над информационными потоками и при этом не сказывались бы на производительности информационных систем.

Многоуровневая архитектура корпоративных приложений постоянно меняется, необходимо контролировать пользователей приложений в соответствии с их текущими ролями, а особенное внимание уделять контролю привилегированных пользователей. Помимо пользователей приложений необходимо контролировать пользователей баз данных, осуществляя мониторинг как доступа на уровне приложений, так и прямого доступа на уровне СУБД. Обеспечение прозрачности всех активностей — ключевой момент в предотвращении мошеннических действий. Решения класса DAM помогают осуществлять контроль всех сессий СУБД (входы, SQL-код, выходы и т.п.), всех исключений СУБД (ошибки, неудачные попытки авторизации), блокирование нежелательных сессий, производить оповещение о различных событиях информационной безопасности. Помимо мониторинга активности в базах данных, решения класса DAM позволяют управлять изменениями объектов СУБД и окружения, управлять уязвимостями СУБД. Предотвращение утечки данных из БД реализуется путем проверки извлекаемой информации, обнаружением аномалий в функционировании, автоматического обнаружения и классификации критичных данных.

Решения IBM Guardium, Imperva, Oracle DBF и другие осуществляют контроль всего SQL-трафика, идущего от клиента к серверу, включая локальные запросы, а не только отдельных SQL-запросов, на которые настроены опции аудита СУБД. Таким образом, максимально снижается риск упустить какое-либо событие, связанное с БД. Любое обращение к БД фиксируется, затем анализируется на основе заведенных в системе правил, и в случае их срабатывания формируется событие ИБ.

Правила позволяют не только отследить такие стандартные события, как факт входа/выхода в/из БД, обращение к данным, изменение структуры БД и т.п., но и позволяют осуществлять контроль по объему скаченных данных, по используемому приложению для обращения к БД. Таким образом, есть возможность отследить несанкционированное копирование или удаление информации, кражу баз данных. Все правила легко задаются с помощью GUI и глубоких знаний SQL/PL-SQL не требуется. Также есть возможность установить фильтры на наличие определенных слов, условий в SQL-запросах, определить список доверенных пользователей и источников запросов. Такую фильтрацию стандартными средствами СУБД сделать либо невозможно, либо для этого требуется писать сложные SQL-скрипты, как, наример, при использовании Oracle Fine-Grained Auditing.

Для предотвращения неавторизованных или подозрительных действий со стороны пользователей используются политики безопасности. Политики безопасности позволяют ограничивать доступ к базам данных или конкретным таблицам на основе различных параметров:

- учетные записи пользователей;
- IP-адреса;
- MAC-адреса;
- сетевые протоколы;
- типы SQL-команд;
- имя приложения;
- время суток и др.

Решения класса DAM контролируют все активности в базах данных, предоставляя детализированную отчетность для дальнейшего расследования событий информационной безопасности, автоматизируя процесс аудита на соответствие требованиям регуляторов и предотвращая утечки информации. Такие отчеты могут содержать различную информацию, такую как ошибки SQL или неудачные попытки аутентификации; административные команды, например, изменяющие структуры баз данных — DDL (create, drop, alter); запросы на выборку данных (select); команды, управляющие учетными записями, их ролями и правами доступа, например, DML (grant, revoke) и другие команды связанные со спецификой СУБД.

## IBM Guardium

Продукт Guardium компании IBM позволяет реализовать полный цикл обеспечения безопасности информации в базах данных. С его помощью можно автоматически собрать и классифицировать информацию об имеющихся базах данных и типу данных, хранящихся в них, что позволяет не упустить недавно созданные базы данных или тестовые инсталляции. Продукт имеет встроенный ска-

нер уязвимостей, что позволяет выявлять и контролировать уязвимости на серверах СУБД. Этот функционал в какой-то мере дублирует функционал MaxPatrol, но является узкоспециализированным и оптимизирован на работу именно с СУБД. Несмотря на широкий спектр функций, реализованных в Guardium, самыми востребованными остаются две из них. Это непрерывный аудит и журналирование всех запросов в БД и возможность блокировки несанкционированного доступа данных. Причем блокировка сессий пользователей БД реализована на уровне агентов, что позволяет избежать установки устройств Guardium в разрыв сети.

Агенты осуществляют сбор информации о всех выполняемых субъектами доступа запросах к СУБД и возвращаемых им данных, которые впоследствии отправляют на сервера сбора и корреляции, где принимается решение об оповещениях или блокировке доступа.

Решение позволяет точно идентифицировать субъекта доступа по ряду показателей, таких как MAC-адрес или IP-адрес компьютера, с которого осуществляется доступ, имя пользователя в ОС, имя пользователя в приложении, имя пользователя в СУБД.

Для каждого устройства формируется универсальная политика безопасности, формируемая правилами трех типов. Правила первого класса — Access rules — это правила контроля доступа к среде, которые позволяют разграничивать доступ к объектам базы данных, на основании собранной информации. Правила второго класса — Exception rules — правила обработки исключений, таких как ошибки при доступе к несуществующему объекту, неуспешной попытке аутентификации. И последний тип правил — Extrusion rules — правила обработки возвращаемых пользователю значений, которые анализируют данные, полученные пользователем в результате запроса в базу, и принимают решения о дальнейших действиях.

Удобство такого подхода в том, что правила можно комбинировать, создавая политику безопасности, назначать приоритеты или задавать условия определения инцидентов по итогам отработки правил.

Агенты, устанавливаемые на каждом сервере СУБД, имеют общий конфигурационный

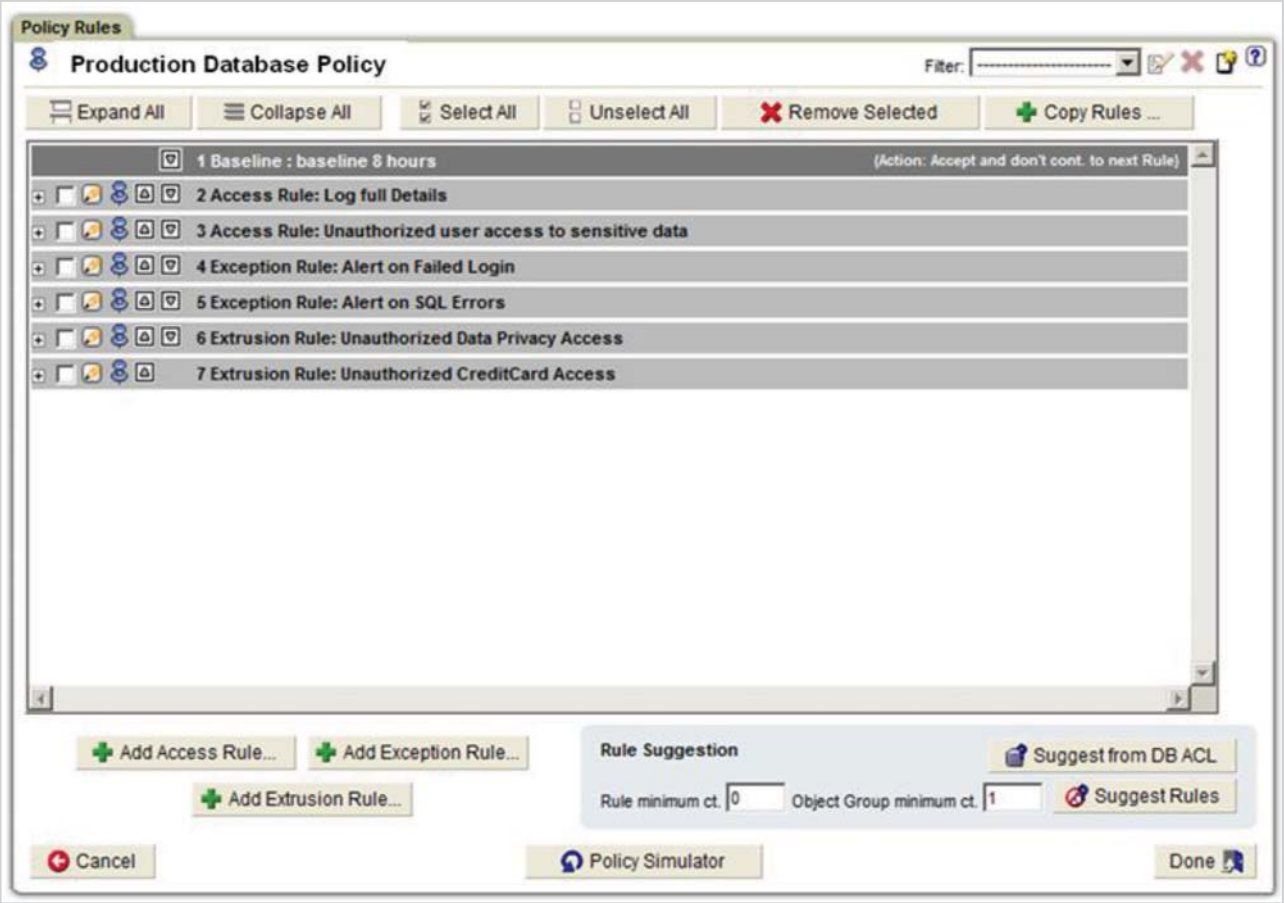



**Рис. 17. Удобство работы с правилами в Guardium.**

```
SQL> insert into cc (i, cardnumber, name) values(1, '1234567890123456', 'Joe Smith');
1 row created
SQL> insert into cc (i, cardnumber, name) values(2, '1234567890123457', 'John Henry');
1 row created
SQL> insert into cc (i, cardnumber, name) values(3, '1234567890123458', 'James McDowl');
1 row created
SQL> insert into cc (i, cardnumber, name) values(1, '1234567890123456', 'James Smith');
1 row created
```

**Рис. 18. Пример нормализованной информации, хранящейся в базе данных Guardium.**

файл, который определяет адрес резервного коллектора для агента с учетом предполагаемой пиковой загрузки резервного коллектора. Таким образом, управление всеми агентами осуществляется централизованно и, в случае выхода из строя одного из устройств, нагрузка перекидывается на другие устройства, что позволяет обеспечить непрерывность мониторинга.

Информация, поступающая в устройство, приводится к типовому виду в независимости от исходного формата (нормализуется) и фильтруется. Механизм определения необходимости хранения той или иной информации определяется с помощью внутренних правил, составляющих политику безопасности устройства.

При этом каждый запрос анализируется и раскладывается на отдельные поля, объединение которых в различных вариантах позволяет получать информацию в виде произвольного отчета.

При этом Guardium обеспечивает возможность регистрации не только даты и времени входа (выхода) пользователя в систему (из системы), результат попытки входа (успешная или неуспешная), но и другие параметры, в том числе время совершения того или иного действия, время начала и окончания сессии, протоколы доступа к СУБД, сетевые параметры клиента и сервера, имя пользователя в БД и ОС, а также многие другие.

Возникающие инциденты, связанные со срабатыванием правил политики безопасности, результаты корреляции событий и другие результаты выгружаются на устройство агрегатор. Это позволяет реализовать централизованный мониторинг активности пользователей, иметь полную информацию о возникающих инцидентах для всех защищаемых баз данных, автоматически и централизованно оповещать уполномоченных сотрудников и управлять процессом реагирования на инциденты с помощью встроенной системы управления инцидентами.

Guardium предоставляет встроенный механизм корреляции событий, происходящих в результате нарушения политик, для генерации оповещений о нужных ситуациях в среде — например, можно сформировать одно оповещение о подозрительной деятельности при наступлении нескольких событий, таких как отказ в доступе на нескольких серверах СУБД с одного клиентского IP-адреса. Комбинируя правила в политиках можно создать гибкую систему контроля и мониторинга доступа к среде СУБД.

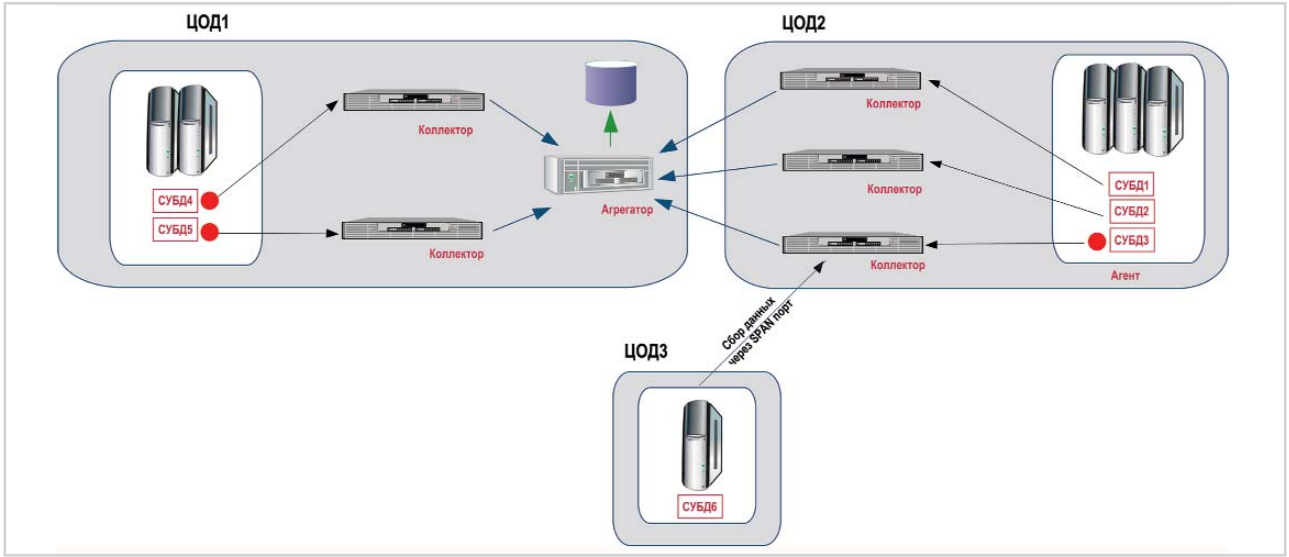



**Рис. 19. Архитектура IBM Guardium для распределенных компаний.**
**Возможен сбор данных как с помощью пассивного мониторинга через SPAN порт, так и с помощью агентов.**

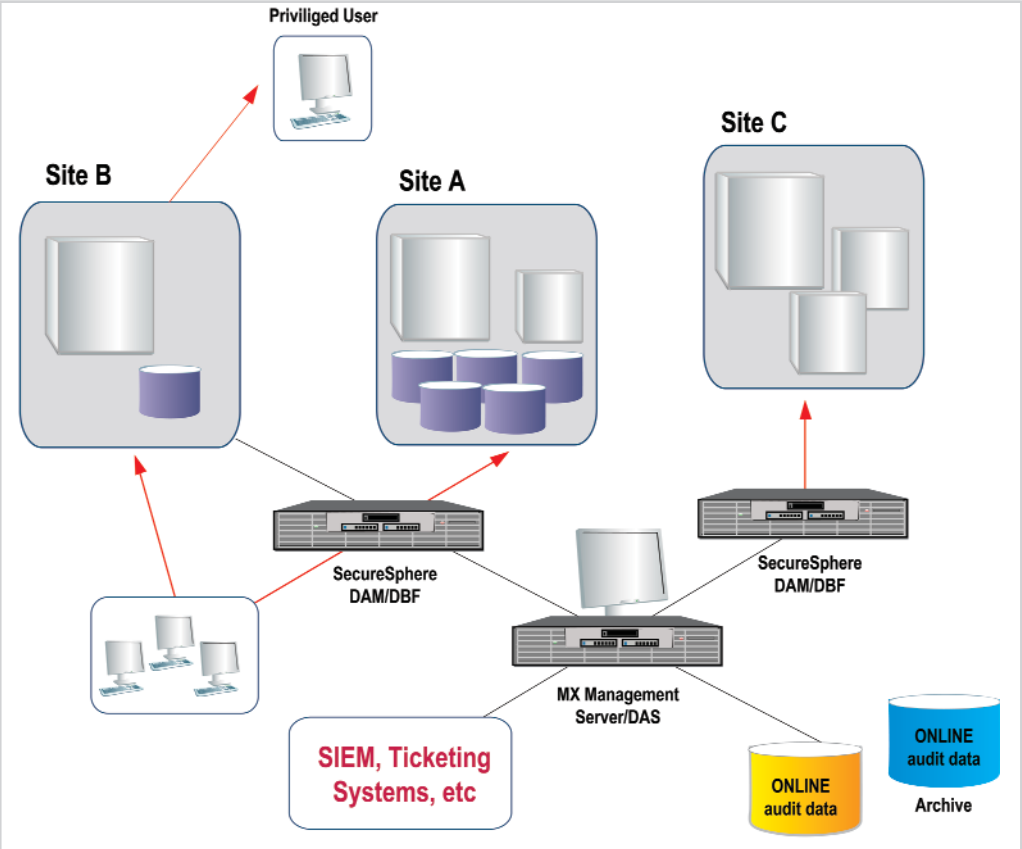



**Рис. 20. Комплексный подход Imperva к защите баз данных и приложений.**

Основным из преимуществ продукта IBM Guardium является то, что он позволяет интегрироваться практически с любым приложением, даже отечественной разработки. Интеграция Guardium с приложениями позволяет сделать абсолютно прозрачной запросы пользователей приложения к базам данных, а корреляция событий на уровне агрегатора позволяет получить полную картину происходящего в инфраструктуре баз данных и бизнес-приложений.

Вторым сильным игроком на российском рынке является компания Imperva и ее линейка продуктов SecureSphere. Подход Imperva несколько отличается от подхода IBM. Продукты линейки Imperva SecureSphere позволяют осуществлять комплексную защиту Web-приложений, а также достаточно надежно защищать данные, передаваемые через Web-приложения и хранимые в базах данных. И совсем недавно компания представила новый продукт линейки SecureSphere File Security, позволяющий отслеживать доступ к файлам, включая доступ привилегированных пользователей и приложений, выявлять и оповещать о нарушениях политики безопасности, а также блокировать при необходимости.

Продукт SecureSphere File Security является частью линейки SecureSphere Data Security Suite и интегрируется в общую систему защиты баз данных и приложений.

## Imperva

Наряду с классическими средствами по периметровой и хостовой защите (МЭ, IDS/IPS, шифрование каналов передачи данных, антивирусное ПО и т.д.) применяют и дополнительные меры защиты. Это может быть использование виртуальной клавиатуры, карточек с сеансовыми ключами, ввод кода, указанного на картинке, проверка вводимых данных и т.д. Но реализация подобных мер по тем или иным причинам не всегда возможна. Нередки ситуации, когда сотрудники, которые разрабатывали Web-приложения, попросту уже не работают в компании, а также, когда доработка или изменение кода слишком трудоемки.

Недостаток же базовых средств защиты состоит в том, что они зачастую недостаточно эффективны в борьбе с атаками на Web-приложения. Поэтому для их защиты необходимо использовать специализированные средства. Для обеспечения безопасности работы приложений используются межсетевые экраны веб-приложений (WAF, Web Application Firewall). Чаще всего решения этого класса представляют собой программно-аппаратные комплексы, которые применяют наборы правил и политик безопасности к наблюдаемому HTTP-трафику, идущему от приложений к базе данных и в обратном направлении. Эти решения позволяют контролировать такие известные типы атак, как Cross-site Scripting (XSS) или SQL-

инъекции. Настраивая правила под бизнес-приложения, можно обнаруживать и блокировать множество атак. Однако объём работ для выполнения этой настройки может быть существенен, кроме того, эта работа должна выполняться при внесении изменений в приложение.

Определённое влияние на появление решений этого класса оказал стандарт PCI DSS, требующий защиты информации о кредитных картах в публичных веб-приложениях по крайней мере, одним из двух методов: анализом кода веб-приложения: вручную, сканированием исходных кодов или оценкой уязвимости, либо установкой точки применения политики безопасности и централизованным автоматизированным методом.

Решения класса WAF часто называют 'Deep Packet Inspection Firewalls' (МСЭ с глубоким анализом пакетов), т.к. они анализируют каждый запрос и ответ на уровнях HTTP/HTTPS/SOAP/XML-RPC/Web-служб. При этом сами данные в базе данных остаются незащищёнными, их использование не отслеживается (фактически инспектируется только часть сетевых запросов к БД, идущих от сервера приложений). Как и обычные МСЭ защиты периметра, WAF необходимы, но далеко не всегда достаточны.

Устройства SecureSphere WAF предназначены для защиты Web-приложений от широкого спектра угроз. В отличие от традиционных систем IPS устройства SecureSphere способны отслеживать Web-сессии, проводить сравнительный анализ элементов структуры Web-приложений (cookie, параметры, поля форм и др.) с ожидаемыми элементами, хранимыми в их профилях, профилировать HTTP, HTTPS и XML-трафик. Среди наиболее распространённых атак, нацеленных на веб-приложения, можно выделить атаки на бизнес логику (parameter tampering), подмена сессий (session hijacking), повторение легальных сессий (session replay), подмена фрагментов данных (cookie injection, cookie poisoning), подбор паролей, нелегальное изменение HTTP пакетов (double encoding, malicious encoding) и атаки на XML и SOAP.

**Что лучше?**

Если говорить о сравнении продуктов Imperva с решением IBM Guardium, можно выделить несколько основных отличий. Во-первых, Guardium использует внутреннюю базу данных для хранения данных мониторинга и аудита, а Imperva хранит собранные данные в файлах. Оба подхода имеют и преимущества, и недостатки. Хранение данных мониторинга в базе данных значительно снижает скорость обработки запросов и записи в хранилище. Но зато увеличивает скорость работы с такими данными. Отчет проще выгрузить из структурированной базы данных, чем из файлового хранилища. Во-вторых, решение IBM намного сложнее при внедрении, в то время как продукты Imperva можно поставить в режим обучения и за несколько недель построить baseline, на основании которой можно достаточно оперативно сформировать политику безопасности. Но сложность во внедрении продуктов Guardium обусловлена огромным количеством настроек, параметров и функций, что в свою очередь дает преимущество опытному внедренцу в виде возможностей реализовать любую задачу. Из ключевых различий можно выделить еще и размер вендора. Софтверный гигант IBM обеспечивает отличный уровень технической поддержки пользователей, но все изменения в продукт вносятся с размеренностью и неспешностью, присущей всем большим компаниям. В это же время, компания Imperva достаточно небольшая, не имеет официально представительства в России и технической поддержки русскоязычных пользователей, но зато имеет возможность максимально оперативно и точно вносить изменения в продукт, удовлетворяя изысканные запросы пользователей.

Устройства Imperva автоматически профилируют Web-приложения с целью моделирования их структуры. Анализируя Web-трафик за определенный интервал времени, они создают профиль стандартного поведения приложения (автоматическое создание «белого» списка активности Web-приложений и пользователей). Далее устройства проводят корреляционный анализ отклонений от профиля с сигнатурами атак и при необходимости блокируют угрозу.

Использование профилей является действенным инструментом для выявления аномального поведения пользователей, ошибок в логике системы, определения типовых ролей и корректности предоставления ролей. Аналогичный подход верен и для продуктов Imperva для защиты баз данных. Для определения базового состояния контролируемой среды СУБД платформа Imperva сначала функционирует некоторое время в режиме обучения, анализируя весь трафик среды. В процессе обучения, платформой накапливается и анализируется статистика по загрузке SQL-трафика. После обучения автоматически формируются политики для их рассмотрения и даль-

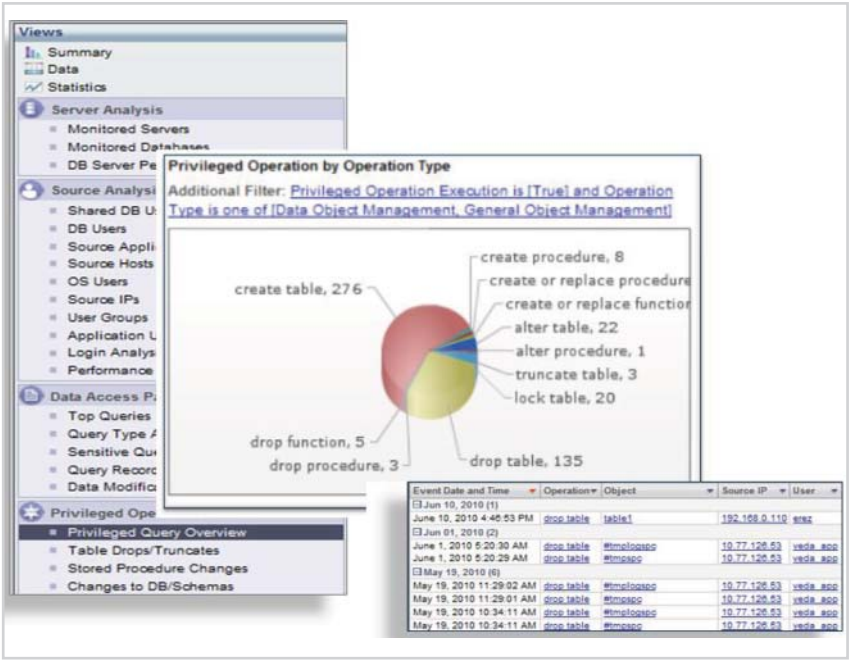



**Рис. 21. Удобный интерактивный интерфейс для анализа данных аудита.**

нейшего применения эксплуатирующим платформу персоналом, как для нормального функционирования среды, так и для аномального поведения (доступ к критичным данным с неизвестных IP-адресов, доступ к системным таблицам или копирование данных с продуктивных систем на другие машины). Необходимо обеспечить максимальную безопасность в период обучения платформы Imperva, чтобы подозрительная активность не вошла в базовый «слепок» нормального функционирования среды, либо тщательно проанализировать, отредактировать и принять предложенные платформой после обучения политики.

## Прикладные аспекты СОК

Каждая компания, решившаяся на построение Центра оперативного управления информационной безопасности, в первую очередь, ожидает от SOC повышение эффективности решения тех или иных прикладных задач в области защиты информации и обеспечения должного уровня ИБ. Это могут быть как частные задачи по защите информации и оперативному управлению, так и выполнение каких-либо требований в области обеспечения ИБ. Далее мы рассмотрим основные прикладные аспекты применения SOC в российской действительности. В первую очередь, это защита персональных данных и данных о держателях платежных пластиковых карт.

### SOC и защита персональных данных

Необходимость обеспечения безопасности персональных данных в наше время — объективная реальность. Информация о человеке имеет большую ценность. Более того, в руках мошенника она превращается в орудие преступления, в руках уволенного сотрудника — в средство мщения, в руках инсайдера — товар для продажи конкуренту. Именно поэтому персональные данные сегодня нуждаются в самой серьезной защите!

Сегодня вряд ли можно представить деятельность организации без обработки информации о человеке. В любом случае организация хранит и обрабатывает данные о сотрудниках, клиентах, партнерах и поставщиках. Утечка, потеря или несанкционированное изменение персональных данных приводит к невосполнимому ущербу, а порой и к полной остановке деятельности компании.

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государство требует от организаций обеспечить надежную защиту персональных данных. Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных» регулирует отношения, связанные с обработкой и защитой сведений, которые принадлежат физическим лицам (субъектам персональных данных).

К персональным данным относится «любая информация, принадлежащая определенному физическому лицу, либо данные, которые могут однозначно такое лицо идентифицировать». Это может быть фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПДн.

Оператором ПДн является «государственный орган, муниципальный орган, юридическое или физическое лицо, организующее или осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных», то есть все без исключения организации, которые имеют собственные отделы кадров, хранят и обрабатывают дан-

ные о клиентах, партнерах, подрядчиках и т.п.

Российским законодательством предусмотрена гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение требований ФЗ № 152 «О персональных данных».

Система защиты ПДн является неотъемлемой частью общей системы обеспечения безопасности организации (используются уже имеющиеся в организации наработки по ИБ, при необходимости создаются новые компоненты системы, которые интегрируются без снижения производительности и не усложняют инфраструктуру).

Система защиты ПДн повышает фактическую защищенность и способствует выполнению требований бизнеса по защите коммерческой тайны.

При построении SOC в рамках реализации системы защиты ПДн специалисты нашей компании применяют современные технологии ведущих производителей в области защиты информации. К ним, в частности, относятся решения класса Security Information Management (ArcSight, Symantec, RSA envision), Database Activity Monitoring (IBM Guardium, Imperva), Identity Management и Information Right Management (Oracle), Data Loss Prevention («Инфосистемы Джет», Symantec, RSA), Configuration&Vulnerability Management (Positive Technologies).

Продукты класса Security Information Management, такие как ArcSight, Symantec SIM и RSA enVision применяются для обеспечения централизованного управления системой защиты персональных данных, что является требованием п. 2.4. раздела II. Методы и способы защиты информации от несанкционированного доступа Приказа ФСТЭК России № 58 от 5 февраля 2010 г. Данные системы осуществляют сбор, анализ (корреляцию) и контроль событий ИБ от различных средств защиты, что позволяет в режиме реального времени эффективно идентифицировать инциденты ИБ, с дальнейшей их передачей в систему управления инцидентами ИБ, получать реальные данные для анализа и оценки рисков, для принятия обоснованных решений по обеспечению ИБ и защите ПДн.

Решения по защите БД, такие как IBM Guardium, Imperva и Oracle позволяют реализовать функции регистрации и учета (в соответствии с п. 2.3 раздела II. Методы и способы защиты информации от несанкционированного доступа Приказа ФСТЭК России № 58 от 5 февраля 2010 г.) обращений всех пользователей к базам данных, содержащих ПДн, без снижения производительности серверов СУБД и значимого влияния на инфраструктуру информационных систем. Особенно необходимы продукты такого уровня в крупных территориально-распределенных организациях. Так, решения IBM Guardium выступают единой точкой контроля доступа всех пользователей, в том числе привилегированных, к базам данных любых производителей.

Требование по обеспечению анализа защищенности в соответствии с п. 2.2 раздела II. Методы и способы защиты информации от несанкционированного доступа Приказа ФСТЭК России № 58 от 5 февраля 2010 г. специалисты компании «Инфосистемы Джет» реализуют с помощью продукта MaxPatrol компании Positive Technologies. Данная система позволяет проводить регулярную инвентаризацию ресурсов ИС, выявлять уязвимости, связанные с ошибками в конфигурации программного обеспечения информационных систем персональных данных, которые могут быть использованы нарушителем для реализации атаки на систему, осуществлять контроль изменений настроек сетевого оборудования, операционных систем серверов и рабочих станций.

## SOC и PCI DSS

В рамках любого проекта по приведению инфраструктуры в соответствие требованиям PCI DSS можно выделить несколько ключевых бизнес задач. Во-первых, необходимо максимально упростить процесс аудита, во-вторых, сэкономить на внешних аудиторах, также ограничить доступ аудиторов к критичной информации. И, конечно, хранить данные аудита в течение длительного времени, чтобы всегда была возможность оперативно получить доступ к необходимым отчетам.

Наши эксперты говорят, что выполнение всех требований PCI DSS и решение внутренних задач заказчика наиболее просто и эффективно выполнить при помощи инструментов Security Operations Center.

В требованиях стандарта PCI DSS применительно к СУБД есть ряд требований, необходимых для выполнения и реализуемых нашими специалистами в рамках проектов по приведению инфраструктуры в соответствие стандарту. В любой системе обработки платежных карт должна быть реализована возможность контроля появления данных о платежных картах в объектах, не предусматривающих их содержание. Согласно требованию 6.1 стандарта PCI DSS должны отслеживаться установленные обновления безопасности и возможность проведения виртуальных обновлений. В требовании 6.2 указана необходимость ранжирования обнаруженных уязвимостей для их дальнейшего

эффективного устранения. Выполнение требования 8.5.8 стандарта PCI DSS должно обеспечить возможность обнаружения использования групповых, разделяемых или встроенных учетных записей. Требования 10.2.1 стандарта PCI DSS применительно к СУБД говорит о необходимости регистрации любых доступов к данным о платежных картах. Так как данные о платежных картах хранятся в базах данных, то необходимо контролировать доступы всех пользователей к базам данных, а особенно привилегированных пользователей, о чем говорит требование 10.2.2. Контролировать необходимо не только обращение к данным, но и все действия, выполненные с использованием административных привилегий. Более того, необходимо не только обеспечить мониторинг доступов к данным о платежных картах, а также, в соответствие с требованием 10.2.3 обеспечить регистрацию доступа ко всем журналам регистрации событий. Требование 10.2.4 стандарта PCI DSS применительно к СУБД говорит о необходимости возможности регистрации неудачных попыток логического доступа, а 10.2.5 о необходимости регистрации использования механизмов идентификации и аутентификации. Также необходимо регистрировать создание и удаление системных объектов на сервере СУБД и обеспечить защиту журналов регистрации от внесения изменений. Требование 11.3 обязует проводить поиск уязвимостей и ошибок в конфигурации СУБД и окружения.

Все эти и некоторые другие требования по контролю действий пользователей, имеющих доступ к данным о платежных картах, возможно успешно реализовать только при помощи решений SOC. Очевидно, что регистрировать все события, контролировать журналы регистраций, проверять на уязвимости и защищать от утечек неавтоматизированным методом невозможно.

### SOC и внутренние задачи

Помимо выполнения требований ряда регуляторов, SOC призваны решать бизнес задачи заказчиков. К таким задачам относятся и борьба с мошенничеством, и организация взаимодействия ИТ и ИБ департаментов с выработкой единых регламентов, стандартов по информационной безопасности и контроля их исполнения.

Порой мы сталкиваемся с очень четкой, но узкой постановкой задачи, как, например, контроль изменений или удаление накладных, выгрузка специфических отчетов, доступ к страховым полисам определенных сотрудников или контроль соответствия определенных настроек на сетевом оборудовании требованиям по информационной безопасности.

Спектр задач, решаемых с помощью SOC, необычайно широк. Можно реализовать практически любой функционал, требующий сбор информации, ее обработку и выработку мер реагирования, будь то сетевое оборудование, рабочие станции, базы данных или технологическое оборудование, например, базовые станции операторов связи.

## В Заключение

Несмотря на то, что Центры оперативного управления информационной безопасностью в России пока что не сильно распространены, уже есть уникальный опыт построения таких центров и примеры, которые можно ставить в пример всем организациям. На данный момент насчитывается около 50 внедрений систем мониторинга и управления инцидентами ИБ на базе продуктов ArcSight ESM, Symantec SIM и RSA enVision. Лидерство в этой области в России уверенно держит ArcSight, имея более 30 внедрений. Количество инсталляций MaxPatrol колеблется также в районе 50, но надо учитывать, что MaxPatrol продукт относительно новый, на рынке появившийся пару лет назад и по прогнозам экспертов к концу 2011 года количество систем управления уязвимостями на базе MaxPatrol может достигнуть сотни. В области защиты баз данных наложенными средствами количество внедрений продуктов Guardium, Imeprva, Embarcodero и Netforensics Dataone уже перевалило за пятьдесят, причем интерес к таким продуктам проявляют не только телекоммуникационные компании и крупные банки, как традиционно уделяющие внимание информационной безопасности, но и компании из промышленной отрасли, небольшие сервис-провайдеры и даже государственные компании, так как продукты проходят сертификацию в ФСТЭК, получая возможность защищать конфиденциальную информацию в государственных организациях.

Отрадно, что растет число компаний, которые не только внедряют разрозненные средства защиты, но уже в полной мере пользуются преимуществами полноценных SOC-ов. Из наиболее известных центров оперативного управления ИБ можно выделить SOC в Билайне, МТС, ТНК-ВР и ряде других крупных организаций, информацию о которых можно найти в сети.

Не пора ли и Вам задуматься над всеми прелестями и выгодами от организации Центра оперативного управления информационной безопасности в своей компании?

# Экспертное мнение

**Некоторыми аспектами специфики внедрения с нами поделились эксперты компании «Инфосистемы Джет». Специалисты не только рассказали об основных трудностях при внедрении продуктов SOC, но и, опираясь на свой опыт, дали советы, как их избежать и главное, как использовать технологии SOC максимально эффективно.**

Андрей Черных,
эксперт по защите баз данных и приложений
компании «Инфосистемы Джет»

Продукты класса Imperva и IBM Guardium бесспорно обладают довольно широким функционалом, однако для успешного внедрения необходимо приложить немало усилий по подготовке инфраструктуры и внутренних процедур заказчика. В нашей практике мы довольно часто сталкиваемся с ситуациями, когда подготовка и настройка информационных систем к внедрению продуктов Imperva или Guardium происходит уже на стадии внедрения, а не перед ним.

Зачастую заказчик не особенно хорошо представляет себе, где хранятся защищаемые данные, что именно необходимо защищать и каких пользователей контролировать.

Важный аспект успешности внедрения и дальнейшего функционирования продуктов класса Imperva и IBM Guardium касается агентов, контролирующих трафик с серверов баз данных. У заказчика вполне обоснованно возникают серьезные опасения, связанные с влиянием агентов на работу и производительность промышленных серверов СУБД. Поэтому до начала внедрения производится предварительное длительное функциональное и нагрузочное тестирование на непромышленных серверах. Стоит отметить, что чем тщательнее будет осуществлена данная проверка, тем меньше вероятность возникновения неожиданных ситуаций в процессе внедрения и эксплуатации.

Еще одна особенность, которая требует пристального внимания — это тщательное составление и тестирование политики безопасности. Нужно понимать: что именно необходимо контролировать, каких целей и задач необходимо достичь в результате внедрения. В следствие этого возникают избыточные правила фильтрации трафика и реагирования на события, что в свою очередь приводит к появлению большого количества ложных срабатываний. Избежать всех этих трудностей поможет тщательная подготовка к внедрению. Мы рекомендуем, прежде всего, провести анализ и корректировку текущих политик безопасности и доступов к информации, спланировать тестирование продукта, пройти краткий курс обучения и только затем приступать к внедрению. При этом внедрение следует производить поэтапно, сначала покрывать критичные системы, а затем подключать к системе менее важные базы данных и контроль непривилегированных пользователей.

В первую очередь, необходимо контролировать доступ подозрительных пользователей к критичным для бизнеса объектам. Если доступ к критичным объектам осуществляется через приложение — с большой долей вероятности это один пользователь базы данных, в этом случае желательно отслеживать действия к данным объектам и всех остальных пользователей. Безусловно, основную угрозу несут привилегированные пользователи, администраторы баз данных. Их активность необходимо тщательно регистрировать и расследовать в связи с наличием у них практически неограниченного доступа к любой информации в базах данных.

Безусловным плюсом при внедрении таких продуктов, как Imperva и Guardium, может стать интеграция их с SIEM-системами как ArcSight ESM или RSA enVision. С одной стороны, Imperva и Guardium позволяют довольно гибко создавать необходимые отчеты, которые вполне удобны в использовании. С другой — анализировать инциденты для заказчика с большим количеством различных систем, как показывает практика, удобнее в центральной консоли SIEM-продукта. Это позволяет проводить корреляцию событий и выявлять инциденты гораздо быстрее и эффективнее. Вероятнее всего, заказчик будет недоволен удобством использования отдельно стоящей системы с непривычным и глубоко техническим описанием инцидентов ИБ.

Если говорить о наиболее востребованных и полезных отчетах, в первую очередь, я бы предложил выводить в отчетах информацию о несанкционированных доступах пользователей к бизнес-критичным объектам. Для этого необходимо отслеживать появление новых ролей и прав на эти объекты. Кроме того, желательно отслеживать создание представлений на основе объектов, поскольку, скорее всего, такое представление не будет контролироваться администратором по безопасности.

Несмотря на широкий функционал продуктов Imperva и Guardium, в них существуют свои особенности. Могу отметить несколько пожеланий на пути «к совершенству». Так в продуктах Imperva хотелось бы иметь настраиваемый механизм корреляции событий информационной безопасности и возможность изменять интерфейс в зависимости от потребностей. В настоящий момент возможно только изменение цвета интерфейса. В продукте IBM Guardium можно было бы усовершенствовать интерфейс, сделать его более дружественным для нетехнических специалистов. Также хотелось бы получить более открытую архитектуру продукта (в настоящее время полный административный доступ к консоли устройств Guardium имеет только техническая поддержка IBM).

Несмотря на вышесказанные пожелания, хочу отметить комфортную работу с данными продуктами. В целом, я доволен решениями класса Imperva и IBM Guardium. Более того, в своей практике я не сталкивался с задачами, которые нельзя было бы решить с их помощью.

Евгений Рудацкий,
руководитель направления PCI DSS
компании «Инфосистемы Джет»

Помимо защиты данных клиентов и держателей платежных карт, задача стандарта PCI DSS — максимально упростить расследование инцидентов информационной безопасности. Поэтому все требования стандарта нацелены на то, чтобы собирать максимум событий и информации об активности пользователей. Эта информация консолидируется в едином хранилище, и любой доступ к данным держателей платежных карт должен контролироваться. Инструменты SOC обеспечивают необходимый уровень оперативности расследования инцидентов и контроля действий пользователей при обращении к критичным данным. При выявлении какого-либо инцидента, средства Центра оперативного управления ИБ помогут максимально оперативно расследовать инцидент, выявить нарушителя, восстановить полную картину произошедшего, понять кто осуществил несанкционированный доступ, когда и каким способом. И все наши заказчики это осознают.

Когда мы начинаем общение с новыми заказчиками по проекту приведения в соответствие требованиям PCI DSS, мы нередко слышим от них, что логи можно просматривать в ручном режиме, без каких-либо специализированных средств автоматизации сбора и анализа событий. Но со временем наши заказчики начинают глубже понимать требования стандарта. Ведь необходимо понимать, что он охватывает огромное количество систем, серверов, приложений и сетевых устройств и контролировать доступ нескольких сотен или даже тысяч пользователей в десятки корпоративных систем, обрабатывающих данные о платежных картах, практически невозможно. Даже отдельно взятая база данных процессинга банка среднего размера может генерировать несколько тысяч транзакций в секунду от сотен пользователей, как внутренних, так и внешних (например, клиентов банка). Обработать такой объем событий в ручном режиме весьма затруднительно, не говоря уже о корреляции событий между различными серверами и системами и выявлении из этого потока информации каких-либо инцидентов.

Более того, Центр оперативного управления ИБ, построенный в рамках проекта PCI DSS, обычно в дальнейшем расширя-

ется на весь банк: к централизованному мониторингу подключаются все системы компании. Таким образом, система оперативного управления важна не только для подразделений информационной безопасности, но и для ИТ-служб и аудиторов.

При этом управление инцидентами становится задачей корпоративного масштаба. Без систем класса SOC, невозможно оперативно выявлять угрозы и их устранять. Невозможно даже представить как, имея только журналы syslog, можно эффективно обнаружить какой-либо инцидент и тем более восстановить полную картину атаки на информационную систему.

Стандарт PCI DSS претерпевает изменения как минимум раз в 2 года. Более того, каждый год необходимо проходить повторный аудит на соответствие требованиям. Таким образом, грамотно построенный SOC позволит минимизировать дальнейшие затраты банка на выполнение требований регуляторов, аудиторские проверки.

В настоящее время направление SOC в России находится на начальном этапе развития. Большинство заказчиков только начинают задумываться о создании полноценного Центра оперативного управления ИБ, многие внедряют разрозненные компоненты. Надеюсь, что это направление и дальше будет активно развиваться в отечественных компаниях, и в скором времени наши заказчики ощутят всю эффективность и пользу от внедрения таких центров.

Владислав Силуянов,
эксперт по проектированию систем ИБ
компании «Инфосистемы Джет»

Большинство утечек информации происходит изнутри компании. Поэтому основной акцент при построении защиты стоит делать на защите от инсайдеров (по статистике, 90 процентов нарушителей — внутренние пользователи). Есть несколько подходов к защите от внутренних утечек. Одним из таких подходов является сбор событий из различных источников, таких как операционные системы, приложения, сетевые устройства. Когда события собраны, происходит их анализ и выявление инцидентов на основании собранной информации. При таком подходе угрозы выявляются после анализа собранных событий при помощи различных корреляций и отчетов. В результате можно достоверно сделать вывод о произошедшей утечке информации и идентифицировать нарушителя. Недостаток такого метода в том, что об инциденте служба безопасности узнает уже после того, как произошла утечка информации.

Есть и другой подход: производится полный анализ на уязвимости информационных систем, проводится сканирование, определяются недостающие «заплатки» программного обеспечения и обеспечивается поддержание в актуальном состоянии всех программных и аппаратных компонент информационных систем. В этой области безусловным лидером является продукт MaxPatrol отечественного разработчика компании Positive Technologies. Продукт известен широкому кругу заказчиков по своему «младшему брату» — решению XSpider.

Также на отечественном рынке доступна услуга сканирования информационных ресурсов на уязвимостями, которую предоставляет компания Qualys. Такой подход интересен тем, что защищается не сама информация непосредственно, а системы, ее обрабатывающие за счет выявления и устранения уязвимостей. Чем более защищена система, тем меньше вероятность совершения успешной атаки на нее.

Обеспечить защиту от внутренних нарушителей можно также путем задания необходимой политики безопасности и распределения доступа к информационным системам. Этот подход реализуют системы класса IDM. Робот централизованно раздает права и полномочия пользователям, тем самым исключая возможность внесения некорректных или избыточных прав доступа, а также осуществляется мониторинг тех прав доступа, которые пользователь имеет на данный момент. Всегда есть возможность сравнить текущие права с эталоном, которых записывается и хранится в базе системы IDM. Недостаток такого подхода в том, что правила и политики для определения и выделения прав доступа задаются изначально человеком. Если на этапе внедрения политики были определены и заданы некорректно, то система IDM будет выдавать пользователям неверные роли и права, даже не подозревая об этом.

Не менее интересной является защита непосредственно пользовательских рабочих станций, когда агенты устанавливаются на рабочие места пользователей. Примером продуктов, реализующих этот функционал, мо-

жет быть Spectr360 или Insider. По заданной политике безопасности агенты отслеживают действия пользователей и в случае, если эти действия противоречат заданной политике, их действия блокируются. По такому же принципу работают продукты DLP, которые построены на агентской технологии. Так как практически все пользователи работают на рабочих станциях, подход достаточно эффективен, но, правда, для компаний небольшого размера. При количестве рабочих станций в несколько сотен, а тем более тысяч, становится затруднительно эксплуатировать такое количество агентов.

Также нельзя не отметить подход, при котором защищается ядро хранения информации — базы данных. Такие продукты как Guardium и Imperva ведут мониторинг http и sql трафика, контролируя доступ пользователей непосредственно к базам данных, их таблицам и различным критичным объектам серверов СУБД. Преимущества в том, что обычно наиболее критичные данные хранятся в корпоративных базах данных и злоумышленник будет пойман при попытке получить к ним доступ. Но есть у этого метода и минус -за пределами баз данных или приложений, информация не контролируется.

В любом случае, нельзя выбрать один из предложенных подходов и слепо внедрять продукты, реализовывать принципы защиты, заложенные только в одном из них.Центр оперативного управления ИБ предоставляет отличную платформу для интеграции различных методов защиты информации и продуктов в единую консоль мониторинга и управления информационной безопасностью на всем предприятии. Только при таком комплексном подходе можно говорить о достойном уровне ИБ в вашей компании.

Максим Жевнерев,
эксперт по системам мониторинга и управления ИБ
компании «Инфосистемы Джет»

Любой проект по внедрению системы мониторинга и управления инцидентами ИБ — процесс трудоемкий и длительный. Мы рекомендуем использовать в качестве технологической платформы продукты компании ArcSight как наиболее технически совершенное и законченное решение.

Как правило, внедрение централизованной системы мониторинга событий ИБ на базе ArcSight разделяется на 2 этапа: сбор событий и настройка системы.

Для успешного завершения первого этапа необходимо максимально подробно провести обследование систем заказчика. Нужно четко понимать с каких устройств мы будем получать события, какие версии источников событий используются у заказчика. Исходя из этой информации, принимается решение об использовании стандартных коннекторов ArcSight, их доработке либо разработке новых. Основная сложность в данном случае — корректная настройка аудита на всех источниках событий.

Критерий завершения этапа по сбору событий — подключение всех источников к ArcSight и настройка правил, отчетов и консолей для мониторинга состояния подключенных систем и наличия событий.

Второй этап более сложный, так как требует более тесного взаимодействия с заказчиком и его участия в процессе разработки правил корреляции, отчетов, консолей. Процесс настройки достаточно длительный, он может занимать несколько месяцев. Важно помнить, что после завершения внедрения продукта процесс мониторинга и донастройки не должен прекращаться. И если не выполнять этого условия, в ArcSight будет много ложных срабатываний и эффективность системы резко снизится.

Если говорить о конкретных задачах и этапах в проекте по внедрению системы мониторинга, то, на наш взгляд, наиболее оптимальным будет изначально определить несколько конкретных задач, которые должен решать ArcSight. На основании этого нужно выбрать только те источники событий, которые необходимы для решения каждой конкретной задачи. В дальнейшем можно расширять систему, добавляя новые источники и решая новые задачи.

Например, поставлена задача отслеживания использования административных привилегий и управления учетными записями. Для ее решения, скорее всего, понадобятся данные из следующих систем:

1) Контроллеров домена.
2) Операционных систем серверов, на которых данную активность нужно отслеживать.
3) Межсетевых экранов\сетевых устройств.
4) Систем авторизации.
5) Баз данных.
6) IDM -системы.

При этом подключение антивирусных средств, систем IDS\IPS можно оставить на будущее.

В зависимости от состава и полноты источников событий для системы мониторинга можно говорить об эффективности обработки событий и выявления инцидентов ИБ.

Так, например, полезным будет подключить к системе мониторинга не только базовые элементы обеспечения ИБ, такие как антивирусы и межсетевые экраны, но и другие системы управления ИБ. Например, довольно эффективна интеграция системы мониторинга со сканерами уязвимостей. Результаты сканирования MaxPatrol лишь дополняют и расширяют возможности ArcSight. При этом следует отметить, что из MaxPatrol в ArcSight или Symantec SIM попадает только информация о найденных сервисах и уязвимостях (режимы Pentest и Audit). Режим compliance в данном случае остается незатронутым, и отчеты по нему можно получить только в MaxPatrol.

На мой взгляд, интеграция систем мониторинга и систем управления уязвимостями оправдана в следующий случаях:

1) В ArcSight полностью сформирована сетевая модель, и есть необходимость в использовании сканера безопасности для заполнения информации об уязвимостях\используемых сервисах в Assets. В этом случае ArcSight сможет автоматически подстраивать приоритеты событий, использовать данные об уязвимостях\сервисах в корреляционных правилах и отчетах.

2) В случае необходимости построения сетевой модели и заведения списка устройств. Для этого при выпуске отчета MaxPatrol включаются только данные об уязвимостях с уровнем «Informational».

Более сложные системы, а также программное обеспечение собственной разработки, требуют особого внимания и разработки специальных коннекторов к ним. Для реализации сбора событий с нестандартных источников нужно досконально изучить систему логирования источника. Каким образом система ведет логирование событий (база данных, файл, отправка событий по syslog\snmp и т.д.)? Какая информация есть в этих журналах? Есть ли возможность доработки системы логирования? Если это файлы, то можно ли их забирать удаленно и как часто они перезаписываются?

В идеальной ситуации каждое событие, которое генерирует источник, должно быть распознано коннектором. В противном случае должен быть определен перечень необходимых для обработки событий, а остальные игнорироваться.

Как правило, для успешной разработки от Заказчика необходимо получить следующие данные:

- документацию на систему логирования и\или контакты разработчиков системы;
- выборку из логов системы за достаточно длительный промежуток времени;
- возможность доступа к самой системе либо построения аналогичной на наших стендах.

С точки зрения использования системы мониторинга и управления ИБ в качестве средства выявления угроз, финансовых рисков и утечки информации, наиболее интересны:

- функции и отчеты по отслеживанию использования «чужих» учетных записей для аутентификации в системе;
- изменения конфигурации систем;
- создание пользователей с административными привилегиями на короткий промежуток времени;
- отчеты по удалению\копированию пользователями данных.

Игорь Ляпунов,
директор Центра информационной безопасности
компании «Инфосистемы Джет»

В настоящее время задачи по мониторингу событий информационной безопасности, по адекватному реагированию на инциденты вышли на первый план. Внедрение дополнительных активных средств защиты (межсетевых экранов, средств предотвращения атак, различных фильтров) уже не дает заметного повышения уровня безопасности, а иногда даже наоборот — снижает ее за счет повышения сложности и роста энтропии системы. Большинство крупных компаний, наших заказчиков, концентрируют свои усилия на повышении именно управляемости системы, ее прозрачности и «аудируемости». Ведь одной из основных задач системы безопасности помимо отражения атак является их уверенное, своевременное обнаружение, предоставление максимума информации для разбора инцидентов.

# MaxPatrol: универсальное решение может быть индивидуальным

**Борис Симис,**
**директор по развитию компании Positive Technologies**

**MaxPatrol – выдающийся продукт не только на отечественном рынке, но и на мировом. Это решение, которое успешно сочетает в себе самые сложные механизмы проверки защищенности ИТ-систем и устранения возможных уязвимостей. О том, как будет развиваться продукт в ближайшем будущем на российском и мировом рынках расскажет наш собеседник Борис Симис, директор по развитию компании Positive Technologies.**

**JI: Управление уязвимостями – довольно узкая область. Почему PT решили развивать продукт именно такой специфики?**

**Борис Симис:** Область, в которой работает Positive Technologies, скорее относится к контролю защищенности информационных ресурсов. Мы – экспертная компания, разрабатывающая прикладные решения в области информационной безопасности.

На наш взгляд, на российском рынке сегодня более востребованной является не классическая модель «ПО как сервис» или в иноземной терминологии модель SaaS, а предоставление именно сервиса, т.е. практически готового процесса по контролю защищенности, отслеживанию изменений, анализу рисков и т.д. Это позволяет заказчикам передать провайдеру не только функции, связанные с техническим обслуживанием систем, но и ряд экспертных и процессных задач, уменьшая требования к штатному расписанию. Именно компания Positive Technologies стала первооткрывателем на этом рынке. В 2005 году мы предлагали сканер XSpider в виде услуги. Это был своего рода «пилотный» проект, который обогнал запросы рынка информационной безопасности в России. Позже мы запустили подобный проект, но уже основанный на продукте другого класса – системе контроля защищенности и соответствия стандартам MaxPatrol, которую приобретают как ПО, а с 2010 года и как услугу. Это интересно, прежде всего, тем, кто задумался о контроле защищенности своего внешнего информационного периметра

и хочет это сделать быстро и с наименьшими затратами.

**JI: Заказчикам какой отрасли наиболее интересен MP?**

**Б.С.:** Есть отрасли, где существует прямая зависимость между бизнесом и ИТ — это телекоммуникации, банки, промышленность. Отмечу, что в последние несколько лет можно было наблюдать все более усиливающуюся отраслевую специфику проектов по информационной безопасности. Безусловно, это не отменяет базовых решений по ИБ, таких как антивирусная защита, межсетевые экраны, VPN — сегодня они стали типовыми и присутствуют в той или иной мере у каждой организации.

Но на рынке сейчас становятся все более востребованными решения по защите бизнеса, учитывающие его специфику. Отдельные решения для телекоммуникационных компаний или решения по защите ERP-систем в промышленности. Это интересные, сложные решения и за ними будущее.

**JI: Если говорить о практической полезности продукта, какие основные задачи поможет решить внедрение MP?**

**Б.С.:** Система MaxPatrol разработана для того, чтобы можно было контролировать комплексную безопасность компании. Собственно, что делает MaxPatrol? Сканирует информационную систему предприятия, выявляет уязвимости, после чего выдает задания на исправления последних. И, конечно же, контролирует систему на соответствие корпоративным политикам безопасности.

Если говорить о том, что получит заказчик при внедрении MaxPatrol, то я бы выделил четыре основные задачи. Во-первых, это уверенность в том, что не появится критичной уязвимости, о которой он не узнает. Во-вторых, это контроль: постоянный аудит тысяч единиц сетевого оборудования, серверов, рабочих станций, ERP, БД на соответствие политикам безопасности. Далее заказчик получает знания, т.е. четкие рекомендации по исправлению ошибок для специалистов. И наконец, управляемость, а именно KPI для анализа руководством состояния защищенности всей организации.

**JI: Какие преимущества MaxPatrol перед конкурентами Вы выделили бы в первую очередь?**

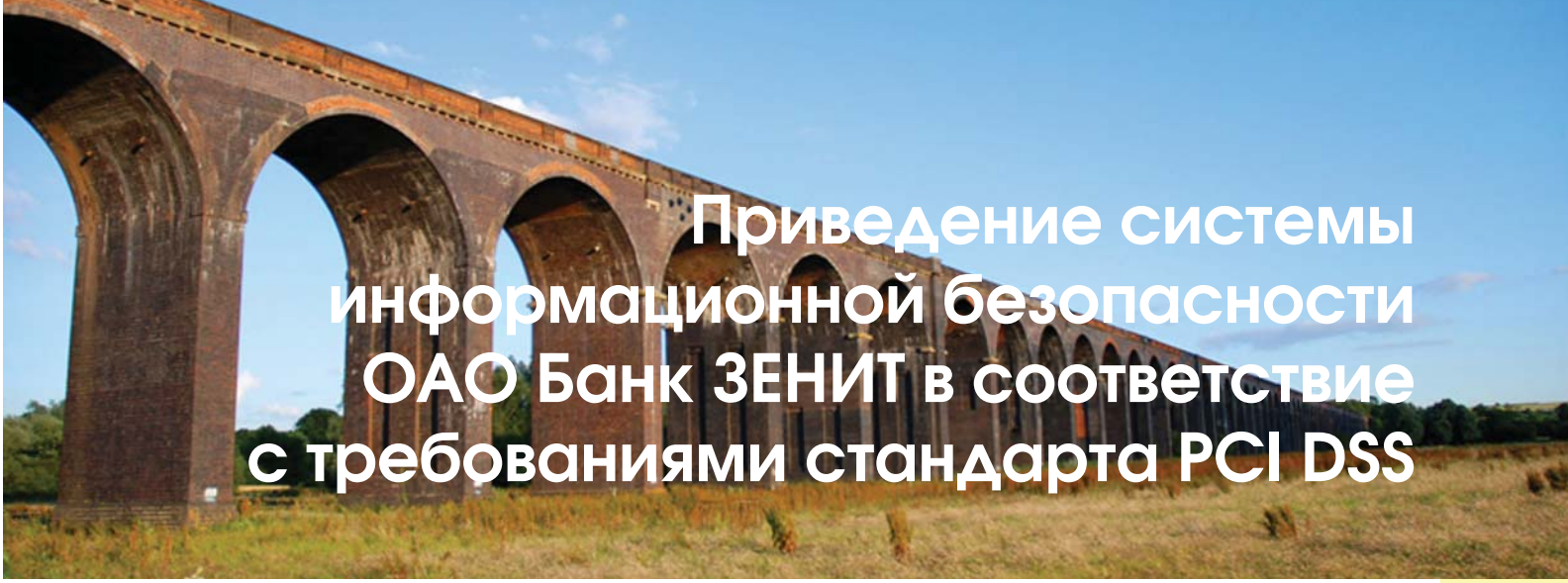
**Б.С.:** MaxPatrol — первый в мире продукт, объединивший механизмы системных проверок, тестирования на проникновение и контроля соответствия стандартам, включая анализ сетевого оборудования, операционных систем, СУБД, прикладных и ERP-систем и веб-приложений. Основой для разработки MaxPatrol послужил наш другой продукт — профессиональный сканер безопасности XSpider и десятилетний опыт экспертов Positive Technologies, полученный в ходе внедрения и эксплуатации XSpider в ведущих российских и зарубежных компаниях. В результате, в системе MaxPatrol реализованы общемировые передовые технологии, а также учтены особенности российского рынка.

**JI: Сейчас довольно популярны продукты компании Apple, а именно iPad. Многие заказчики высказывают пожелания вывода интерфейса продуктов на планшет. Возможно ли визуализировать отчеты MP на iPad?**

**Б.С.:** Да, при необходимости, возможно.

**JI: Планируется ли интеграция MP с распространенными SIEM решениями, типа ArcSight или RSA enVision? Насколько это полезно и актуально?**

**Б.С.:** Интеграция не планируется, поскольку MaxPatrol уже интегрирован и успешно используется в связке с SIEM решениями. :)



# Приведение системы информационной безопасности ОАО Банк ЗЕНИТ в соответствие с требованиями стандарта PCI DSS

ОАО Банк ЗЕНИТ был учрежден в декабре 1994 года Академией народного хозяйства при Правительстве РФ, нефтяной компанией «Татнефть» и рядом других юридических лиц. Одним из важных направлений деятельности ОАО Банк ЗЕНИТ является комплексное обслуживание корпоративных клиентов. Банк также занимает сильные позиции на рынке инвестиционных услуг и частных инвестиций. Как член Ассоциации Российских Банков, представленный в Совете Ассоциации, ОАО Банк ЗЕНИТ активно участвует в процессах, идущих в рамках российской банковской реформы.

## Задача

ОАО Банк ЗЕНИТ имеет собственный процессинговый центр для обработки транзакций по международным платежным картам. Одной из важнейших задач Банка является обеспечение сохранности данных пользователей, особое внимание уделяется вопросам защищенности технологических операций и процессам управления информационной безопасностью (ИБ). Оказываемая Банком процессинговая поддержка держателей карт и банков-партнеров должна осуществляться в строгом соответствии с требованиями ИБ, предъявляемыми международными платежными системами, в том числе требованиями стандарта PCI DSS.

Банком ЗЕНИТ перед исполнителем проекта были поставлены задачи разработать и внедрить процессы управления информационной безопасностью в соответствии с требованиями стандарта PCI DSS.

Одним из обязательных условий для Банка ЗЕНИТ было минимальное вмешательство в сложившиеся бизнес-процессы. Это связано с тем, что процессинговый центр Банка работает в непрерывном режиме 24x7, а операции Банка осуществляются по всему миру. При остановке работы процессингового центра осуществление банковских операций было бы невозможно, это не только критично с точки зрения клиентов банка, но и несет в себе определенные репутационные риски для Банка».

«Проект комплексный, и задача состояла в том, чтобы не только обеспечить соответствие стандарту PCI DSS, но и требованиям Федерального закона № 152-ФЗ «О персональных данных» и стандарта СТО БР ИББС, — комментирует **Евгений Рудацкий, руководитель направления PCI DSS компании «Инфосистемы Джет»** — Однако в первую очередь необходимо было выполнить требования стандарта PCI DSS в связи со строгими ограничениями сроков со стороны международных платежных систем».

Работы по сертификации на соответствие стандарту PCI DSS и оценке состояния системы защиты могут выполнять только специализированные компании, обладающие соответствующим статусом. Исполнителем проекта была выбрана компания «Инфосистемы Джет», обладающая статусами Qualified Security Assessor (QSA, для аудита), Approved Scanning Vendor (ASV, для сканирования сети) и имеющая богатый опыт реализации подобных проектов.

## Решение

Работы над проектом выполнялись в три этапа: анализ соответствия требованиям стандарта, выявление несоответствий и внедрение специализированных средств защиты, проведение независимого сертификационного аудита. На первом

этапе специалисты «Инфосистемы Джет» провели полное обследование, в ходе которого решались задачи соответствия не только стандарту PCI DSS, но и требованиям федерального закона № 152-ФЗ «О персональных данных» и отраслевого стандарта СТО БР. По результатам обследования был разработан перечень рекомендаций по повышению уровня безопасности данных о держателях карт.

Наиболее масштабный — второй этап проекта, в ходе которого специалисты интегратора спроектировали и внедрили комплекс организационных и технических мер, направленных на устранение несоответствий и требуемых стандартом:

- внедрение системы мониторинга пользователей баз данных;
- построение процесса анализа и реагирования на события информационной безопасности;
- разработка организационно-распорядительной документации;
- существенная модернизация системы обнаружения вторжений;
- внесение изменений в систему контроля межсетевого взаимодействия;
- построение процессов поиска уязвимостей и управления изменениями ИТ-инфраструктуры банка.

Предложенное техническое решение включало как внедрение новых средств защиты, так и модернизацию имеющихся средств.

«Руководство ОАО Банк ЗЕНИТ принимало активное участие в проекте, что во многом способствовало скорейшему решению проектных задач, — комментирует **Евгений Рудацкий, руководитель направления PCI DSS компании «Инфосистемы Джет».** — Благодаря этому нам удалось завершить проект в поставленные сроки с минимальным вмешательством в сложившиеся бизнес-процессы банка».

Для оценки защищенности и подготовки к сертификационному аудиту по окончании второго этапа было проведено сканирование уязвимостей и тестирование на возможность проникновения в систему.

Завершающим этапом проекта стало проведение экспертного аудита и итоговая сертификация по требованиям стандарта. Аудит проводила отдельная команда сертифицированных специалистов компании «Инфосистемы Джет». Его результатом стало подтверждение соответствия системы информационной безопасности требованиям стандарта PCI DSS.

Стандарт PCI DSS разработан в целях повышения уровня обеспечения безопасности в индустрии платежных карт. Организации, которые производят обработку и хранение информации о держателях платежных карт и работают с международными платежными системами, должны каждый год подтверждать соответствие защищенности своих платежных систем требованиям стандарта PCI DSS.

## Результат

Отчет о результатах аудита был направлен в международные платежные системы, которые подтвердили соответствие ОАО Банк ЗЕНИТстандарту PCI DSS. Полученный Банком сертификат является подтверждением высокого качества совместно проделанной работы.

«Внедренные организационные и технические меры помогают выполнению требований ФЗ-152 и стандарта СТО БР ИББС, а главное, обеспечивают реальную защиту информации, — добавляет **Евгений Рудацкий, руководитель направления PCI DSS компании «Инфосистемы Джет».** — В настоящее время планируется завершение аналогичных работ в Банке, связанных с отечественной законодательной базой».

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Главный редактор: Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01 факс (495) 411 76 02
*e-mail: JetInfo@jet.msk.su* *http://www.jetinfo.ru*

Подписной индекс по каталогу Роспечати **32555**

**Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем**