N.G. Miloslavskaya
National Research Nuclear University MEPHI,115409, Moscow, Kashirskoe sh., 31,
e-mail: NGMiloslavskaya@mephi.ru, ORCID iD is 0000-0002-1231-1805

Information Security Operations Centers

Keywords: information security, Security Operations Centers
At present information security (IS) incidents have become not only more numerous and diverse but also more damaging and disruptive. Preventive controls based on the IS risk assessment results decrease the majority but not all the IS incidents. Therefore, an IS incident management system is necessary for rapidly detecting IS incidents, minimizing loss and destruction, mitigating the vulnerabilities that were exploited and restoring organization's IT infrastructure (ITI), including its IT services. These systems can be implemented on the basis of a Security Operations Center (SOC). Based on the related works a survey of the existing SOCs, their mission and main functions is given. The SOCs' classification as well as the key indicators of IS incidents in II are proposed. Some serious first-generation SOCs' limitations are defined. This analysis leads to the main area of further research launched by the author.

Н.Г. Милославская
Национальный исследовательский ядерный университет «МИФИ», 115409, г. Москва, Каширское ш., 31,
e-mail: NGMiloslavskaya@mephi.ru, ORCID iD is 0000-0002-1231-1805

ЦЕНТРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Ключевые слова: информационная безопасность, центры управления безопасностью
В настоящее время инциденты информационной безопасности (ИБ) стали не только более многочисленными и разнообразными, но и более разрушительными. Превентивные средства управления и контроля на основе результатов оценки рисков ИБ снижают большинство, но не все инциденты ИБ. Таким образом, для быстрого обнаружения инцидентов ИБ необходима система управления инцидентами ИБ, сводящая к минимуму потери и разрушения, смягчающая уязвимости, которые были использованы, и восстанавливающая ИТ-инфраструктуру организации и ее услуги. Такие системы могут быть реализованы на основе центра управления безопасностью (ЦУБ). На основе анализа проведенных исследований представлены миссия и основные функции ЦУБ. Предложены классификация ЦУБ и основные показатели инцидентов ИБ. Определены серьезные ограничения первого поколения ЦУБ. Указаны основные области дальнейших исследований.

Введение

Даже в условиях современной кибервойны организации часто не понимают, какие активы их гетерогенных и сильно распределенных ИТ-инфраструктур (ИТИ) имеют наиболее важное значение для ведения бизнеса, какие риски связаны с этими активами, какие средства управления их информационной безопасностью (ИБ) должны быть спланированы и почему. На эти и многие другие вопросы дают ответы результаты различных проверок ИБ, включая мониторинг ИБ ИТИ и контроль используемых мер и средств защиты. Под мониторингом ИБ понимается постоянное (непрерывное) наблюдение за событиями, подлежащими регистрации и влияющими на обеспечение ИБ организации в конкретной среде (ИТ, системе, сети, сервисе), а также сбор, анализ и обобщение результатов мониторинга. Мониторинг ИБ осуществляется на основе контроля за соблюдением основных требований по обеспечению ИБ (контроль за штатным режимом функционирования среды) и применяемых законодательных норм [1, 2].

Анализ данных мониторинга ИБ преследует, как правило, следующие основные цели:

1) контроль за соблюдением в организации положений внутренних и внешних документов по обеспечению ИБ с целью выявления отклонений от принятых требований

бизнеса и обеспечения ИБ (например, зафиксированных в политике логического доступа к активам ИТИ);

2) контроль качества (эффективности и результативности) используемых мер защиты;

3) своевременное обнаружение уязвимостей в активах ИТИ, которые злоумышленники могут использовать для реализации атак на саму ИТИ, деловых партнеров и пользователей организации;

4) обнаружение событий ИБ, связанных с активами ИТИ и бизнес-процессами, часть из которых далее будет классифицироваться как инциденты ИБ;

5) реагирование на инциденты ИБ, включая установление их причин, активацию соответствующих средств управления и контроля ИБ в целях профилактики и сокращения и восстановления после воздействий;

6) предоставление признаваемых в суде доказательств в случае расследования компьютерных преступлений.

Постоянный поток различных данных о состоянии ИТИ организации, поступающий от многих СЗИ, SIEM-систем (систем управления информацией и событиями ИБ) и других интерфейсов управления сетевой безопасностью создает довольно большую нагрузку на персонал ИБ. Среди шума всех событий трудно отобрать те, которые действительно являются событиями ИБ и требуют внимания и немедленного реагирования. Резко возросшая к настоящему времени сложность осуществления мониторинга ИБ, с которой сталкиваются администраторы ИБ, настоятельно требует новых универсальных высокопроизводительных решений, которые соединят в себе отчетность, сложный анализ больших данных, возможности наглядной визуализации и моделирования развития ситуации, планирование ответных действия и совместную работу для более обоснованного принятия решений по управлению инцидентами ИБ (УИИБ). Так, в конце 1990-х годов в качестве организационной основы процесса УИИБ появился специализированный центр управления безопасностью (ЦУБ) со специально подобранными средствами защиты информации (СЗИ) и квалифицированным персоналом. В то время ЦУБ вполне эффективно справлялся со стоящими перед ним проблемами. Но сейчас, когда сетевая среда существенно усложнилась за счет появления новых технологий и поток предаваемой в ней информации определяется как «большие данные», возможностей ЦУБ для их обработки уже не хватает. Требуется разработка более современного, высокопроизводительного и защищенного центра управления сетевой безопасностью.

Таким образом, остальная часть статьи организована следующим образом. В разделе 1 кратко анализируются проводимые в этой области работы. Основные вербальные индикаторы инцидентов ИБ предлагаются в разделе 2. Раздел 3 выделяет миссию ЦУБ в процессе УИИБ (ПУИИБ). Классификация ЦУБ представлена в разделе 4. Некоторые серьезные ограничения первого поколения ЦУБ определены в разделе 5. Определение основной области дальнейших исследований завершает статью.

1. Обзор работ по теме исследования

В настоящее время существует достаточное количество международных документов, регулирующих различные аспекты УИИБ. Как правило, все эти документы последовательно рассматривать все стадии ПУИИБ: от планирования до совершенствования после анализа результатов самого процесса. Так, ИСО/МЭК 27001 «Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Требования» [3] содержит требования к разработке систем управления ИБ (СУИБ) организации независимо от ее деятельности и налагает некоторые общие требования к процессу управления ИБ, в том числе ПУИИБ в качестве его составной части.

В соответствии с пунктом 9.1 «Мониторинг, измерение, анализ и оценке» американского стандарта NIST 800-61 «Руководство по обработке инцидентов

компьютерной безопасности» [4] в процессе обработки компьютерных инцидентов должны быть выполнены, в том числе, следующие действия:

- разработана процедура обработки инцидентов;
- определены структура группы реагирования на инциденты и ее кадровая модель;
- созданы политика и план реагирования на инциденты;
- обнаружены событий ИБ с использованием соответствующих показателей;
- выявлены попытки и успех нарушений ИБ;
- определение того, были ли действий, предпринятые для разрешения нарушения ИБ, наиболее эффективными;
- вовлечение руководства в определение того, выполняется ли как ожидалось деятельность по обеспечению ИБ, делегированная людям или осуществляемая ИТ и СЗИ.

В ряде работ [5-7] описываются подходы к планированию, реализации, проверке и совершенствованию ПУИИБ. Основное внимание уделяется организации совместной работы группы реагирования на инциденты ИБ. Определяется порядок взаимодействия ролей различных участников ПУИИБ. Использование принципа ролей позволяет наделить сотрудников дополнительными обязанностями в рамках ПУИИБ без привязки к их должностям и должностным обязанностям. Подчеркивается, что ПУИИБ может быть реализован различными способами в зависимости от условий, в которых он будет работать.

Большинство заслуживающих внимания работ по тематике ЦУБ были опубликованы в конце 1990-х - начале 2000-х годов [8-18]. Вклад Cisco Systems Inc. в идею ЦУБ, его построение, эксплуатацию и техническое обслуживание трудно переоценить с 1998 г. и по настоящее время [19]. Последующие публикации в большей степени посвящены различным областям применения и рассматривают в основном используемые инструменты защиты компьютерных сетей [20-23]. Они ориентированы либо на технологии, исключая при этом людей и процессы, либо наоборот - на процессы и людей без технологий и инструментов.

2. Ключевые индикаторы инцидентов ИБ

Основными источниками событий ИБ в ЦУБ являются средства мониторинга ИБ и управления работой применяемых СЗИ, среди которых выделим следующие:

- лог-файлы систем мониторинга, управления и контроля ИБ;
- информация от отдельных контроллеров доменов, прокси-серверов, DNS, веб-и почтовых серверов и т.д.;
- файлы журналов операционных систем (ОС) и систем управления базами данных (СУБД);
- лог-файлов прикладного программного обеспечения (ПО), активного сетевого оборудования (с записью всех потоков и подключений) и используемых СЗИ, в том числе средств проверки целостности ПО, СЗИ от несанкционированного доступа и вредоносного кода, специализированные инструменты, такие как решения для обнаружения атак на конечных точках, межсетевые экраны, системы обнаружения и предотвращения вторжений, сканеры безопасности и SIEM-системы;
- результаты специальных запросов;
- информация от конкретных физических устройств контроля доступа, в том числе систем видеонаблюдения, систем охранной сигнализации и т.д.

На основе анализа различных нарушений ИБ в сетях предлагается несколько ключевых вербальных индикаторов инцидентов ИБ (также известных как индикаторы взлома) в сети организаций. Они связаны с типичными для конкретных атак действиями или их комбинацией и могут быть описаны следующим образом.

- Неавторизованный пользователь в сети или общие (совместно используемые) учетные данные.

• Несанкционированный доступ к конфиденциальным, персональным и финансовым данным.

• Несанкционированный внутренний хост (клиент или сервер) подключен к интернету.

• Чрезмерный доступ с одного или нескольких внутренних хостов на внешний вредоносный веб-сайт (из известных черных списков).

• Активность пользователя и фиксация появления вредоносных программ в нерабочие часы (в ночное время или в выходные дни).

• Несколько входов с одним и тем же идентификатором из разных мест в короткий промежуток времени.

• Внутренние хосты связываются либо с известными ненадежными адресатами или хостами, расположенными в другой стране, где нет ни одного бизнес-партнера организации, или с внешними хостами с использованием нестандартных портов или связкой «протокол-порт».

• Один хост/аккаунт пользователя пытается подключиться к нескольким узлам/ИТИ-ресурсам за несколько минут из разных регионов (признак того, что учетные данные пользователя возможно были украдены).

• Хосты, которые являются общедоступными или находятся в демилитаризованной зоне сети организации, связываются с некоторыми внутренними хостами, что указывает на вход снаружи внутрь и обратно, утечку данных и удаленный доступ к ресурсам ИТИ.

• Несколько тревог от одного хоста или повторяющиеся события на нескольких компьютерах в той же подсети в течение 24-часового периода (например, постоянные неудачи аутентификации).

• Повторная атака от одного источника или на одном хосте.

• Доступ к сервисной учетной записи для доступа к интернету или неавторизованному устройству.

• Сканирование сети и уязвимостей и исследование, проводимое с внутренних хостов, осуществляющих связь с несколькими хостами, в течение короткого времени, от неавторизированного хоста или в неразрешенное время.

• Чрезмерный исходящий (например, из интернета, электронной почты) или входящий (например, веб-) трафик от одного источника или к одному адресату.

• Отсутствие или повреждение файлов или появление новых, которые не были созданы внутренними пользователями.

• Исправленные или удаленные журналы от источника или прерывание ведения журнала.

• Выявление типичных, хорошо известных эксплойтов.

• Обнаружение нескольких зараженных хостов.

• Чрезмерные тайм-ауты сканирования от антивирусов.

• После очистки система повторно заражена вредоносной программой в течение короткого периода времени (сигнал о возможном присутствии хакерского средства типа руткита или продолжающейся атаке).

• Чрезмерные попытки блокирования порта от таких систем мониторинга, как антивирус.

• Несанкционированное устройство в сети или устройство, не соответствующее определенным установленным требованиям (политики, обновлений и т.д.).

• Многочисленные изменения административных учетных записей в короткие сроки.

• Несанкционированное изменение конфигурации устройства (включая СЗИ).

• Аномалии в исходных условиях доступа пользователей и аутентификации, сети, приложениях, подозрительная активность, атаки типа «отказ в обслуживании», вредоносные программы и т.п.

• Другие явные признаки, такие как отказы и сбои ПО, повторение некоторых конкретных и часто подозрительных событий, неправильные команды, случайные атрибуты, несоответствующие параметры сетевого трафика и прочее.

• Подозрительные события и процессы, трафик к известным уязвимого хостам и т.д.

Этот список далеко не полон и не ранжирован. Любая организация должна сформировать свой список событий и инцидентов ИБ и осуществлять свою собственную приоритизацию серьезности инцидентов. Например, для многих организаций доставка вредоносной электронной почты не столь критична, как активное управление и контроль зараженной рабочей станцией злоумышленником. Однако если организация предоставляет почтовые ящики, то последствия явно предсказуемы - потеря клиентов и, в худшем случае, всего бизнеса.

3. Миссия ЦУБ в управлении инцидентами ИБ

Постоянно возрастающая сложность управления ИБ в современных ИТИ и недостаток высококвалифицированного персонала является проблемой, которая будет существовать в обозримом будущем. Два важных источника этой проблемы - это огромный поток и разнообразие оповещений (сигналов тревоги), генерируемых системами управления доступом (СУД), антивирусами (АВ), системами обнаружения и предотвращения вторжений (СОПВ), межсетевыми экранами (МЭ), системам унифицированного управления угрозами (СУУУ), ОС, СУБД, системами управления информацией и событиями ИБ (SIEM) и т.д., и разнообразие задач, выполняемых подразделением ИБ, включая управление критичными активами, рисками, СЗИ, обновлениями, шифрованием, инцидентами ИБ и большими, связанными с ИБ, данными и т.д.

Только один МЭ может записывать ежедневно в журнале регистрации гигабайты данных, а СОПВ за тот же период может выдавать миллионы сообщений. МЭ нового поколения, содержащий СОПВ как неотъемлемую подсистему, порождает еще больше данных за счет корреляции событий ИБ, ранее воспринимаемых как никак не связанные между собой. В части информации, генерируемой СЗИ, преобладают ложные срабатывания (показатель враждебной активности, когда ее нет). Большинство сообщений - артефакты законного использования ресурсов ИТИ, просто никогда ранее не проявлявшиеся. Проблема заключается в том, чтобы вычленить и приоритезировать некоторые сообщения, которые действительно указывают на реальные угрозы и события ИБ. Необходимость выделения в белом шуме СУД, АВ, СОПВ, МЭ, СУУУ, ОС, СУБД, SIEM-систем актуальных для данной организации инцидентов ИБ приобретает решающее значение, что имеет и свои экономические основы, требующий от организации более результативного использования существующих СЗИ.

Ключ к более эффективной автоматизации операций по обеспечению ИБ ИТИ и приоритезации задач управления ИБ, в том числе быстрого устранения известных или новых («нулевого дня») угроз ИБ, заключается в создании собственного специализированной структуры организации. Эта структура известна как ЦУБ, которую определим как централизованную структуру, решающую вопросы обеспечения безопасности на уровне организации и включающую группу, состоящую в основном из аналитиков в области безопасности, занимающихся обнаружением, анализом, реагированием, информированием и предотвращением инцидентов безопасности [24]. ЦУБ управляет всеми операциями по обеспечению безопасности в организации и, в частности, осуществляет мониторинг, оценку и защиту собственной информации и информации других важных активов ИТИ, например, баз данных, серверов, сетей, веб-сайтов и т.д. ЦУБ устраняет необходимость вручную собирать, исследовать, классифицировать, анализировать и, в конечном итоге, дифференцировать информацию об инцидентах ИБ из различных источников в интранете (корпоративной сети) и интернете [19].

В сетевой среде ЦУБ является ядром защищенного функционирования интранета как основной части ИТИ организации, обеспечивая непрерывную защиту, обнаружение и реагирование на возникающие угрозы ИБ и свершившиеся инциденты ИБ, а также дистанционно эксплуатируемые злоумышленниками и непрерывно устраняемые по указанию ЦУБ уязвимости в защите в реальном масштабе времени. С SIEM-системами первого поколения в качестве основного компонента, ЦУБ как совместно используемый сервисный и аналитический центр управления ИБ централизованно собирает данные с десятков и сотен СЗИ (СУД, АВ, СОПВ, МЭ и т.д.) и обобщает в единую картину информацию об уровне ИБ ИТИ, помогая его персоналу быстро разобраться в текущей обстановке и мгновенного принимать решения и реагировать на критические проблемы и уязвимости за счет своевременной минимизации рисков ИБ.

ЦУБ должен иметь все необходимое (ПО, аппаратные средства, организационные меры) для реагирования на новейшие угрозы ИБ в ИТИ организации, анализа собственных внутренних, периметровых и внешних сетевых соединений, обнаружения на ранних стадиях и прерывания атак для выведения ЦУБ из строя (типа «распределенный отказ в обслуживании»), сбора признаваемых в суде доказательств при серьезных инцидентах ИБ в ИТИ и многое другое.

Не каждое нарушение ИБ обязательно приводит к немедленному критическому для бизнеса негативному воздействию, поскольку злоумышленникам обычно требуется время на выполнение нескольких предварительных шагов для получения несанкционированного доступа к отдельному сетевому элементу и потом всей сети в целом. Тщательное выявление и своевременное предупреждение такого рода поведения является лишь одной из многих задач, которые могут быть решены с помощью ЦУБ. Таким образом, в его функции входят сетевой анализ, мониторинг среды и устройств, обнаружение аномалий и злоупотреблений, защита от вредоносных программ, корреляция событий, подстройка под текущую ситуацию SIEM-системы и т.д.

Возвращаясь к проблеме, обозначенной в начале данного раздела, отметим, что в штате любого ЦУБ должно быть несколько операторов, работающих с текущими данными, и аналитиков безопасности, которые выполняют исключительно их анализ (их количество, конечно, зависит от размера и сложности ИТИ организации) [19]. Они осуществляют углубленный и консолидированный анализ ранее не происходивших и неизвестных событий ИБ и уязвимостей, характеристики новых атак, опираясь на различные источники и исторические данные самой организации. У них должно быть четкое понимание локальной, региональном и глобальной среды и событий, которые могут повлиять на безопасность бизнеса их организации.

ЦУБ должен работать постоянно в круглосуточном режиме и выполнять следующие типовые функции:

- поддержка функционирования с командной консоли, используемой для выполнения различных команд для расширенного администрирования, поиска неисправностей и решения возникающих проблем;
- отслеживание состояния и восстановление активов ИТИ после инцидентов ИБ;
- сканирование уязвимостей ИТИ-активов и активов ЦУБ с последующим управлением установкой обновлений для устранения уязвимостей;
- прослушивание трафика для захвата всех данных, передаваемых по сетевым каналам, и поиск в нем любой информации, которая может быть полезна для выявления неисправностей и отклонений от штатного функционирования и, в конечном счете, обнаружения событий ИБ;

• управление конфигурацией устройств, предназначенное для автоматизации и полного контроля всего жизненного цикла ИТИ-активов (таких как конфигурации коммутаторов, маршрутизаторов, МЭ и других сетевых устройств);

• централизованное управление всеми СЗИ во всей ИТИ, реализующее идею единого управления процессами их конфигурирования, настройки политик безопасности, оценки статуса, генерации отчетов о функционировании и т.д.;

• управление рисками ИБ и их ранжирование на основе анализа воздействия на бизнес, включая пассивную оценку и активную обработку рисков ИБ;

• управление информацией об ИБ за счет сбора журналов событий, их хранения, архивирования и подготовки соответствующие отчетности;

• обработка событий и инцидентов ИБ, состоящая из их обнаружения, оповещения, установленных ответных действий, ведения отчетности с непрерывным механизмом обратной связи и, при необходимости, эскалации на высшие уровни;

• поддержка собственной локальной ГРИИБ ЦУБ, которая сотрудничает с вышестоящей Национальной группой реагирования на чрезвычайные ситуации;

• осуществление действий по сбору доказательств и реконструкции инцидента ИБ и изучению сетевой среды в судебно-признаваемом порядке для идентификации, сбора, сохранения, восстановления, анализа и представления фактов и доказательств в электронном виде, связанные с компьютерными преступлениями.

Так, ЦУБ может помочь организации выявить источники атак, нацеленные на ее сотрудников (типа фишинг-атаки через электронную почту), с целью устранить уязвимости и любые связанные с ними риски ИБ и дать им сосредоточиться в первую очередь на решении задач бизнеса. Обнаружение IP-адреса хорошо известного ботнет-сервера внутри сети организации, скорее всего, указывает на то, что одна или несколько ее систем были взломаны. Другим типичным подозрительным событием является доступ к базам данных или файлам с одной из рабочих станций организации с помощью USB-устройства, указывающий, что одна из политик ИБ, а именно политика ограничения использования USB, была нарушена и что контроль безопасности, обеспечивающий это, был обойден.

В работе ЦУБ для определения вредоносных IP-адресов, URL, приложений или чего-то еще, что может повредить ИТИ-активы, и выявления чаще всего эксплуатируемых злоумышленниками уязвимостей используют различные средства выделения, фильтрации, нормализации, категоризации, корреляционный и другие методы анализа и эвристики.

Эффективность ЦУИБ разумно измерять на основе того, как инциденты ИБ обрабатываются, локализуются, изолируются, управляются и устраняются.

4. Типы ЦУБ

Существует ряд решений, предлагающих функциональность ЦУБ и отличающихся по стоимости, производительности и реализуемым функциям. ЦУБ может быть описана с разных точек зрения (таблица 1): тип владения, цель и сценарии развертывания, вариант реализации, возможность ответных действий, метод корреляции (корреляция рассматривается как зависимость между сущностями в рамках ЦУБ). Данная классификация не претендует на полноту, так как любая организация может выбрать свой собственный набор атрибутов ЦУБ при разработке своей собственной ЦУБ.

Таблица 1. Классификация ЦУБ

Классификационный параметр	***Содержание параметра***	***Описание***
Тип владения	собственный	Преимущества: собственные знания об ИТИ больше, чем у третьей стороны; легче настроить более эффективные решения; больше вероятность заметить корреляции в пределах ИТИ; меньшая стоимость. Недостатки: большие начальные инвестиции; должны быстро показать эффективность; проще сговор между взломщиком и командой, осуществляющей мониторинг; меньше вероятность выявить шаблоны, накопленные за многолетний опыт работы организации.
	аутсорсинг	Преимущества: отсутствие капитальных вложений; часто дешевле; меньше возможности сговора между взломщиком и командой, осуществляющей мониторинг; беспристрастность; соглашение об уровне сервиса. Недостатки: меньше знаний об ИТИ; снижение бдительности персонала; риск неправильного обращения с данными вне организации; ненадежность для долгосрочной перспективы использования.
Цель развертывания	контроль	ЦУБ позволяет наблюдать за уровнем защиты объектов и прогнозировать его изменение.
	управление	ЦУБ помогает активно воздействовать на ИБ объекта.
	кризисное управление	ЦУБ начинает функционировать только во время кризиса.
Сценарий развертывания	централизованный	ЦУБ базируется на выделенном устройстве/сервере, который выполняет все функции, связанные с управлением ИБ. Преимущества: скорость, простота установки и относительно низкая стоимость. Недостаток: ЦУБ подходит только для небольших и средних сетей (менее ста СЗИ).
	распределенный	ЦУБ использует несколько устройств/серверов, одновременно выполняя балансировку нагрузки между ними. Распределение нагрузки может быть основано на географическом (различные серверы отвечают за разные части сети) или функциональном (часть функций выполняется одним сервером, часть другим) принципе. Поскольку используются несколько устройств, стоимость ЦУБ больше, а его развертывание и обслуживание сложнее. Хотя в целом балансировка нагрузки дает более высокую производительность и эффективность ЦУБ.
Вариант реализации	программный	ЦУБ создан на базе специализированного ПО, установленного на одном/нескольких серверах. Преимущество: возможность использования серверов ЦУБ для решения дополнительных задач.
	аппаратный	ЦУБ - «коробочное» решение на базе одного/нескольких серверов с предварительно установленным ПО. Преимущество: снижение времени развертывания. Поскольку это изолированная среда, на серверах ЦУБ не может быть установлено никакое дополнительное ПО.

	инфраструк-турный	ЦУБ построен с использованием имеющихся ПО и аппаратных средств (например, имеющаяся база данных Oracle используется для хранение событий. Консолидация нескольких баз данных реализуется с использованием репликации. Нормализация, агрегирование и корреляция реализуются в БД с помощью SQL-скриптов и т.д.). Преимущества: относительно низкая стоимость решения и повышенная гибкость. Недостатки: необходимость доработки ЦУБ, включая правила нормализации, агрегирования и корреляции, и использование SQL-программирования для реализации этих правил.
Возможность ответных действий	без ответных действия	ЦУБ работает как классическая система обнаружения вторжений (СОВ): она контролирует и осуществляет приоритезацию событий ИБ. В случае обнаружении атаки никаких ответных действий не предпринимается. ЦУБ обычно используется в средах с высокими требованиями к доступности (например, в банковском деле или медицине), потому что ложные срабатывания не требуют создания правил безопасности и блокировки сервисов. Основная цель ЦУБ: обработка данных об ИБ, визуализация и установление приоритетов событий ИБ, а также соблюдение нормативных требований.
	с воз¬ можностью ответных действий	ЦУБ использует концепцию системы предотвращения вторжений (СПВ): атака не только обнаруживается, но и проводятся ответные действия по недопущению распространения атаки. ЦУБ понимает все составляющие атаки, вплоть до адресов взломанных и смежных систем. Автоматически определяется доступное устройство блокировки атаки на пути ее распространения, на котором автоматически запускаются соответствующие команды, которые могут быть использованы для снижения риск - быстрого и точного предотвращения или сдерживания атаки. ЦУБ обычно используется в средах с высокими требованиями к конфиденциальности. Быстрая автоматическая реакция на угрозы ИБ является его основным преимуществом.
Методика корреляции	статисти-ческая	Для определения серьезности инцидента ИБ ЦУБ применяет статистические алгоритмы, а затем присваивает угрозе ИБ оценку, основанную на стоимости актива. Он смотрит на поведение сети и идентифицирует угрозы ИБ на основе наличия и вероятной тяжести аномальных событий. Он также позволяет измерять эффективность, так как с течением времени число аномальных событий должно уменьшаться по мере того, как ИТИ становится более защищенной. Преимущества: в процессе работы ЦУБ не требуется специальных знаний о моделях угроз ИБ или сценариях атак и до начала его работы не требуется определения правил или показательного базового уровня (статистически нормального состояния), что помогает в определении приоритетов событии ИБ, основанных на стоимости ИТИ-активов.

на основе правил	Для выявления в течение заданного временного интервала вероятных сценариев атак при наблюдении определенного ряда событий ЦУБ использует предварительно определенные правила условной логики. Правила могут быть предустановлены поставщиком ЦУБ или реализованы покупателем после тщательного анализа сетевого трафика. Это чрезвычайно эффективно при определении конкретных угроз ИБ на основе предварительных знаний о моделях атак. Многие продукты реализуют конечный набор правил, покрывающих самые общие сценарии, но они могут быть дополнены правилами пользователей. Здесь важна помощь со стороны производителя в написании новых правил. Правило может применяться к длительному событию, тогда менеджер правил сохраняет состояние события в течение разумного периода времени до того, как другие важные события вызовут сигнал тревоги или выйдет время для исходного события. В ином случае будет происходить много ложных срабатываний, или, что более важно, нельзя будет определить «слабые и медленные» атаки, которые характеризуются малым количеством ежедневных событий в течение длительного временного интервала. Недостатки: требуется много времени для поддержания в актуальном состоянии сотен правил, слишком много ложно положительных и ложно отрицательных срабатываний для постоянно обновляемых методов атак.
на основе уязвимостей	ЦУБ берет данные о событиях ИБ от сетевых СОВ и соотносит их с БД известных уязвимостей и профилями уязвимостей для хостов из сканеров безопасности, присваивая определенное значение каждому активу. Это помогает уменьшить ложно положительные срабатывания за счет уменьшения «шума» в работе сканера, а также помогает персоналу ЦУБ определить, какие атаки реальны и какие активы фактически уязвимы для атак. Преимущества: наиболее эффективны в распознавании сценариев конкретных атак, в том числе новых для ИТИ сценариев, и особенно подходят для устранения ложно положительных срабатываний и увеличения эффективности за счет фокусировки на реальных событиях ИБ, которые соответствуют имеющимся уязвимостям. Недостатки: требуется создание правил корреляции атак, использующих особые уязвимости особо подверженных им активов, а написание таких правил чрезвычайно трудоемко.
на основе соглашения об уровне сервиса (СУС)	ЦУБ связывает события ИБ с требованиями очень важно для бизнеса СУС, что помогает оценить потери от взломанных и вышедших из строя сетевых элементов или компонентов. ЦУБ строит модели бизнес-процессов и анализирует влияние различных инцидентов ИБ на эти процессы. Недостаток: основные трудности заключаются в определении состава бизнес-процессов и активов, их стоимости (эти трудности естественны для процессно-ориентированного анализа рисков в области ИТ).

на основе соблюдения требований	ЦУБ связывает события ИБ с существующими законами, политиками и стандартами в области ИБ (корпоративными и нормативными). Он требует специальной установки и настройки, поскольку возможно только статическое связывание, так как каждая ИТИ имеет свою собственную политику ИБ.
смешанная	Когда все типы корреляции применяются совместно, они могут значительно улучшить обнаружение реальных атак и повысить эффективность управления ИБ. Работа сотрудников ЦУБ становится гораздо проще, когда они могут получать единый профиль риска для событий на основе взаимосвязанных статистических данных об угрозах, основанных на правилах предупреждениях, имеющихся уязвимостях и стоимости активов.
без корреляции	ЦУБ подходит для небольших сетей, где ЦУБ выполняет только агрегирование данных об ИБ, а все решения принимаются и выполняются персоналом ЦУБ.

5. Ограниченность ЦУБ первого поколения

Первые ЦУБ с устаревшими на сегодняшний день основанными на правилах SIEM-системами первого поколения хорошо справлялись с задачей защиты от традиционных атак несколько лет назад. Но в настоящее время, когда ландшафт атак характеризуется более целенаправленными, скрытным и продвинутыми технологиями (например, атаки типа APT и атаки на стороне клиента), можно заключить, что они не рассчитаны на увеличение объемов информации об ИБ в современных гетерогенных ИТИ и им не удается сохранять полный контроль над сложной сетевой ситуацией. Таким образом, ранее описанный функционал ЦУБ первого поколения обладает следующими важными ограничениями:

- невозможность работы в крупномасштабных, глобально развернутых, неоднородных, сильно распределенных и сложно связанных ИТИ с подключением пользователей из любого места и в любое время;
- невозможность обеспечить высокую степень надежности/устойчивости при сборе, передаче и обработке событий ИБ, что делает их уязвимыми к атакам на SIEM-системы и сам ЦУБ;
- зависимость от централизованных правил корреляции, обрабатываемых на одном узле, что затрудняет масштабируемость, создает уязвимости и единые точки отказа;
- ограниченные возможности анализа, оценки и визуализации уровня ИБ, поскольку ЦУБ осуществляет мониторинг всех событий на сетевом уровне и обеспечивает не очень сложную сортировку и поиск неисправностей во внутренних сетях;
- отсутствие реакции на выявленные атаки в режиме реального времени; в дополнение к автоматизированным операциям аналитики ЦУБ должны оценивать в режиме реального времени большие объемы данных и вручную реагировать на них;
- недостаточная производительность для обработки больших объемов всех ранее накопленных, только что собранных и аналитически выведенных на их основе данных, известных как технология «больших данных»;
- невозможность интерпретации данных более высоких уровней, таких как «сервис» или «деятельность»;

• большое количество ложных срабатываний, поскольку выявляются лишь известные или простые в обнаружении события;

• SIEM-системы первого поколения в качестве ядра ЦУБ;

• ручная интеграция различных технологий защиты в едином ЦУБ.

Заключение

Новая реальность более частых и сложных атак и «взлом как сервис» делает атаки на ИТИ организаций более профессиональными, доступными и опасно эффективными. Организации должны противопоставить этому надлежащим образом разработанные и централизованные системы управления ИБ, сочетающие в себе автономные SIEM-системы и СЗИ, обработку массового потока связанных с ИБ больших данных, работу в соответствии с едиными и постоянно контролируемыми и модифицированным политиками ИБ и жесткое соблюдение разнообразных нормативных требований.

Для реализации такого подхода и автоматизации ряда рутинных операций и реагирования на инциденты ИБ, которые не требуют принятия решений экспертами, для любой современной организации необходим центр управления ИБ, борющийся с этими проблемами и более продвинутый, чем традиционный ЦУБ.

На первый план выходят следующие требования к современным ЦУБ:

• максимальная автоматизация рутинных операций, приближающая реагирование на инциденты ИБ к режиму реального времени;

• реализация полной видимости происходящего в ИТИ;

• контекстный анализ поведения (выявление отклонений по сравнению с нормальным поведением или функционированием), а не просто сигнатурный анализ;

• поддержание повышенного уровня ИБ для ИТИ.

ЦУБ второго поколения - Центр интеллектуального управления безопасностью (ЦИУБ) - с интегрированной архитектурой защиты от атак объединяет полную прозрачность и контроль и контекстно-управляемый интеллект с его действенным и всеобъемлющим пониманием и управлением знаниями в области ИБ, что позволяет постоянно контролировать сеть и более важные высокие уровни ИТИ. Реализуя ЦИУБ, организации имеют целостный детальный взгляд на «здоровье» их ИТИ и способны не только обнаруживать и распознавать атаки, но и эффективно обрабатывать новые угрозы ИБ, прежде чем они причинят вред, и предотвращать инциденты ИБ, постоянно собирать и получать обобщенные знания о сетевых атаках.

В целях расширения автономности управления инцидентами ИБ в рамках одной организации и углубления ее знания о ИТИ наше дальнейшее исследование направлено на объединение всех преимуществ ЦИУБ и Центра управления сетью (ЦУС) с их уникальными и совместно применимыми инструментальных средствами управления сетевой безопасностью.

СПИСОК ЛИТЕРАТУРЫ:

1. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Серия «Вопросы управления информационной безопасностью». В 5 т-х. Т. 5: Проверка и оценка деятельности по управлению информационной безопасностью. Москва: Горячая линия-Телеком. 2014. 2-е изд. 166 с.

2. ISO/IEC 27035:2011 {{Information technology -- Security techniques -- Information security incident management».

3. ISO/IEC 27001:2013 {{Information technology -- Security techniques -- Information security management systems -¬ Requirements)).

4. Cichonski P., Millar T., Grance T., Scarfone K. «NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide,» August 2012. [Электронный ресурс]. URL: http://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-61r2.pdf (дата обращения 23.03.2016).

5. Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003. [Электронный ресурс]. URL: http://www.cert.org/archive/pdf/03hb001.pdf (дата обращения 23.03.2016).

6. West-Brown M.J., Stikvoort D., Kossakowski K.-P., Killcrece G., Ruefle R., Zajicekm M. Handbook for Computer Security Incident Response Teams (CSIRTs). April 2003. [Электронный ресурс]. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305 (дата обращения 23.03.2016).
7. Alberts C., Dorofee A., Killcrece G., Ruefle R., Zajicek M. CMU/SEI-2004-TR-015 «Defining Incident Management Processes for CSIRT». October 2004.
8. Bace R.G., Intrusion Detection. Indianapolis: Macmillan Technical Publishing, 2000.
9. Van Wyk K.R., Forno R. Incident Response, Sebastopol, CA: O'Reilly Media, Inc., 2001.
10. Schultz E.E., Shumway R. Incident Response: A Strategic Guide to Handling System and Network Security Breaches, Sams, 2001.
11. Northcutt S. Network Intrusion Detection (3rd Edtion). IndianapolisNew Riders Publishing, 2002. 512 p.
12. Spitzner L. Honeypots: Tracking Hackers, Addison-Wesley Professional, 2002.
13. Prosise C., Mandia K., Pepe M. Incident Response and Computer Forensics, Second Edition, McGraw-Hill/Osborne, 2003.
14. Bejtlich R. The Tao of Network Security Monitoring: Beyond Intrusion Detection, Boston, MA: Pearson Education, 2005.
15. Bejtlich R. Extrusion Detection: Security Monitoring for Internal Intrusions, Addison-Wesley Professional, 2005.
16. Лукацкий А.В. Ситуационные центры по информационной безопасности. Журнал {{Information Security/Информационная безопасность». 2005. № 2. С. 28-30.
17. Романов В.В. Ситуационные центры в решении проблем информационной безопасности. Журнал «Information Security/Информационная безопасность». 2006. № 3-4. С. 28.
18. Bidou R. Security Operation Center Concepts & Implementation. 2005. [Электронный ресурс]. URL: http://iv2-technologies.com/~rbidou/ SOCConceptAndImplementation.pdf (дата обращения 31.01.2016).
19. Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press. 2015. [Электронный ресурс]. URL: https://supportforums.cisco.com/sites/default/files/security_operations_center_9780134052014_ch_1_final___0.pdf (дата обращения 23.03.2016).
20. Fry C., Nystrom M. Security Monitoring, Cambridge: O'Reilly, 2009.
21. Rajnovic D. Computer Incident Response and Product Security, Indianapolis, IN: Cisco Press, 2011.
22. Sanders C., Smith J. Applied Network Security Monitoring: Collection, Detection, and Analysis, Boston, MA: Syngress, 2013.
23. Bejtlich R. Practice of Network Security Monitoring, San Francisco, CA: No Starch Press, 2013.
24. Security Operations Center. [Электронный ресурс]. URL: http://resources.infosecinstitute.com/security-operations-center/ (дата обращения 23.03.2016).

REFERENCES:

1. Miloslavskaya N.G., Senatorov M.Y., Tolstoy A.I. «Information Security Management Issues» Series. In 5 volumes. Volume 5: Checks and Assessment of Information Security Management Activity. Moscow: Goriachaja linia-Telecom. 2014. 2nd edition. 166 p.
2. ISO/IEC 27035:2011 «Information technology -- Security techniques -- Information security incident management)).
3. ISO/IEC 27001:2013 «Information technology -- Security techniques -- Information security management systems -- Requirements».
4. Cichonski P., Millar T., Grance T., Scarfone K. «NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide,» August 2012. URL: http://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-61r2.pdf (access date 23.03.2016).
5. Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003. URL: http://www.cert.org/archive/pdf/03hb001.pdf (access data 23.03.2016).
6. West-Brown M.J., Stikvoort D., Kossakowski K.-P., Killcrece G., Ruefle R., Zajicekm M. Handbook for Computer Security Incident Response Teams (CSIRTs). April 2003. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305 (access date 23.03.2016).
7. Alberts C., Dorofee A., Killcrece G., Ruefle R., Zajicek M. CMU/SEI-2004-TR-015 «Defining Incident Management Processes for CSIRT». October 2004.
8. Bace R.G., Intrusion Detection. Indianapolis: Macmillan Technical Publishing, 2000.
9. Van Wyk K.R., Forno R. Incident Response, Sebastopol, CA: O'Reilly Media, Inc., 2001.
10. Schultz E.E., Shumway R. Incident Response: A Strategic Guide to Handling System and Network Security Breaches, Sams, 2001.
11. Northcutt S. Network Intrusion Detection (3rd Edition). IndianapolisNew Riders Publishing, 2002. 512 p.
12. Spitzner L. Honeypots: Tracking Hackers, Addison-Wesley Professional, 2002.
13. Prosise C., Mandia K., Pepe M. Incident Response and Computer Forensics, Second Edition, McGraw-Hill/Osborne, 2003.
14. Bejtlich R. The Tao of Network Security Monitoring: Beyond Intrusion Detection, Boston, MA: Pearson Education, 2005.
15. Bejtlich R. Extrusion Detection: Security Monitoring for Internal Intrusions, Addison-Wesley Professional, 2005.
16. Lukatskiy A. Security Operations Centers. «Information Security» Journal. 2005. Vol. 2. Pp. 28-30. (In Russian)
17. Romanov V. Operations Centers in Solving Information Security Problems. «Information Security» Journal. 2006. Vol. 3 -4. P. 28. (In Russian)
18. Bidou R. Security Operation Center Concepts & Implementation. 2005. URL: http://iv2-technologies.com/~rbidou/ SOCConceptAndImplementation.pdf (access date 31.01.2016).

19. Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press. 2015: URL: https://supportforums.cisco.com/sites/default/fdes/security_operations_center_9780134052014_ch_1_final__0.pdf (access date 23.03.2016).
20. Fry C., Nystrom M. Security Monitoring, Cambridge: O'Reilly, 2009.
21. Rajnovic D. Computer Incident Response and Product Security, Indianapolis, IN: Cisco Press, 2011.
22. Sanders C., Smith J. Applied Network Security Monitoring: Collection, Detection, and Analysis, Boston, MA: Syngress, 2013.
23. Bejtlich R. Practice of Network Security Monitoring, San Francisco, CA: No Starch Press, 2013.
24. Security Operations Center. URL: http://resources.infosecinstitute.com/security-operations-center/ (access date 23.03.2016).