Ковалев Д. О.
Московский инженерно-физический институт (государственный университет)

ИДЕОЛОГИЯ И РЕАЛИЗАЦИЯ ОПЕРАЦИОННЫХ ЦЕНТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной статье вводится понятие операционного центра информационной безопасности, как средства централизованного управления проблемами информационной безопасности организации, анализируется история развития данного понятия, приводится описание и функции, идеология, а также подходы к построению операционных центров информационной безопасности.

1. Введение

Операционный центр информационной безопасности — это централизованная компонента, предназначенная для комплексного управления проблемами ИБ организации. Данный термин предлагается автором по аналогии с устоявшимся понятием сетевого операционного центра, решающего аналогичные задачи в области управления телекоммуникационной инфраструктурой. В зависимости от размеров организации ОЦИБ может представлять собой либо выделенный программный продукт, либо целый набор программных и аппаратных средств, основной задачей которого является управление ИБ организации.

Первые программные реализации ОЦИБ начали появляться в 2000—2002 годах. Примерами таких программ являлись Netforensics nFX Open Security Platform (OSP), CA eTrust Security Information Management (SIM), Arcsight Enerprise Security Manager (ESM), Symantec Security Information Manager и т. д. Их целью являлось повышение уровня защищенности информационных и телекоммуникационных ресурсов, а также повышения уровня контроля над работой средств защиты информации (СЗИ). Принцип работы этих продуктов заключался в сборе, агрегации, корреляции и визуализации большого количества данных аудита ИБ, полученных от различных СЗИ: межсетевых экранов, маршрутизаторов, систем обнаружения вторжений, журналов регистрации событий операционных систем (ОС). Процесс работы типового продукта происходил в четыре этапа:

· этап нормализации — на данном этапе собирались различные сообщения с объектов мониторинга и приводились к единому формату;

· этап агрегации — на данном этапе определялись и удалялись дублируемые сообщения и происходило распределение оставшихся сообщений по различным категориям. Также на данном этапе происходила системная оценка событий, позволяющая ранжировать угрозы согласно их значимости;

· этап корреляции — на данном этапе происходил анализ агрегированных данных и выявление закономерностей, сигнализирующих о попытке проведения сетевой атаки;

· этап визуализации — на этапе визуализации происходило графическое представление данных безопасности, прошедших через все предыдущие этапы. Визуализация позволяла сотрудникам службы безопасности быстро идентифицировать угрозы и производить соответствующие действия по их предотвращению.

На рис. 1 приведен пример обработки данных решением Netforensics.

Перед продуктами ставились следующие задачи:

· управление и мониторинг в режиме реального времени состояния следующих объектов: виртуальные частные сети, межсетевые экраны, системы обнаружения и предотвращения вторжений, системы отражения DDoS-атак, решения для борьбы с вирусами, шпионскими программами и другим вредоносным кодом, обновления программного обеспечения, персональные и портативные компьютеры, серверы и других решений, имеющих отношение к сфере безопасности;

· динамическая визуализация угроз ИБ на единой консоли управления, с целью их дальнейшего анализа и анализа их последствий;

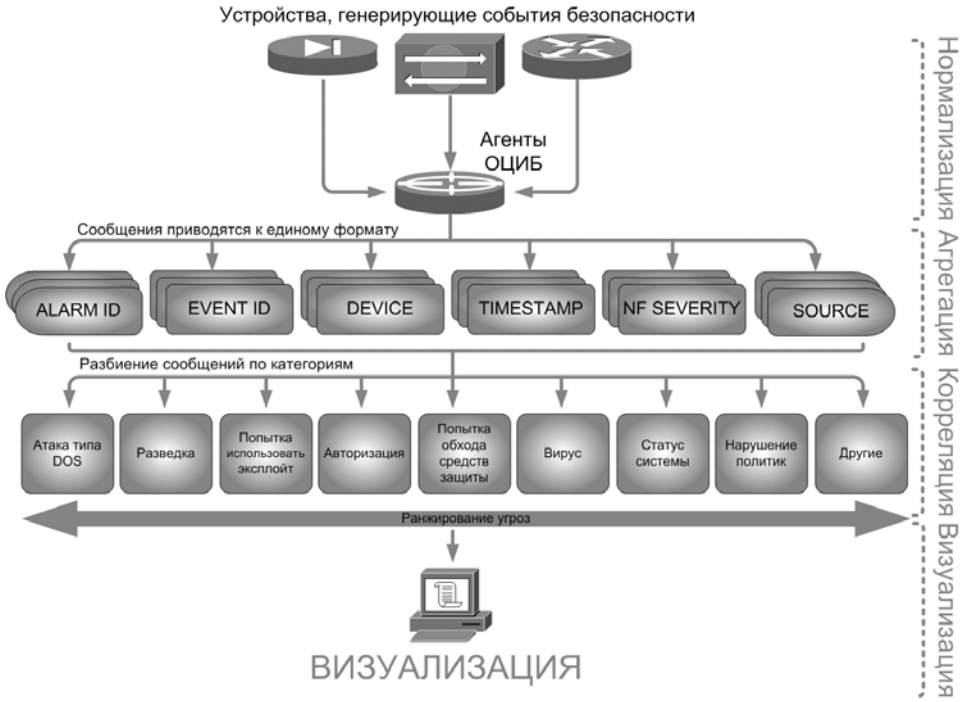

Рис. 1. Этапы обработки данных

· анализ данных журналов безопасности, сведений об уязвимостях, информации о ресурсах и сигналах тревоги;

· немедленное принятие ответных мер при возникновении потенциальных угроз ИБ и быстрое разрешение проблемных ситуаций в сфере безопасности;

· построение графических отчетов по событиям ИБ [1]

Со временем круг решаемых задач расширился, к ним добавились следующие:

· оценка рисков для анализа общей защищенности телекоммуникационной сети и активов, находящихся в ней;

· приоритезация обработки инцидентов ИБ;

· документирование инцидентов ИБ и поддержание базы данных знаний по обработке инцидентов ИБ;

· долговременное хранение данных аудита для обеспечения доказательств в случае проведения расследований и отслеживания состояния ИБ организации в течение времени.

Стандарт ГОСТ ИСО/МЭК 27001 устанавливает требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию системы управления информационной безопасностью (СУИБ). Стандарт представляет собой наилучшие практики по управлению безопасностью организации. Поскольку основной задачей ОЦИБ является управление проблемами ИБ, то ГОСТ ИСО/МЭК 27001 во многом определяет стратегию развития ОЦИБ. Это значит, что к задачам ОЦИБ в ближайшее время будут добавлены следующие положения обязательного для выполнения Приложения А к стандарту ГОСТ ИСО/МЭК 27001:

· А.7 — Управление активами;

· А.14 — Управление непрерывностью бизнеса;

· А.15 — Обеспечение соответствия требованиям нормативных документов.

Таким образом, ОЦИБ прошли путь от программных продуктов по концентрации и анализу журналов регистрации событий ИБ до комплексных решений по управлению проблемами ИБ, реализующим и поддерживающим СУИБ организации.

Сегодня каждый крупный производитель в области ИБ предлагает свой ОЦИБ, среди них можно выделить: Arcsight ESM, Network Intelligence envision, Novell Sentinel, Cisco MARS, Symantec SIM, Netforensics nFX OSP; CA eTrust Security Command Center, Intellitactics Security Manager, ActiveWorx, IBM Tivoli Risk Manager, NetIQ Security Manager, LogLogic, Sensage, NeuSecure, Checkpoint Eventia. В некоторых из решений уже частично присутствуют функции для реализации вышеперечисленных положений стандарта ГОСТ ИСО/МЭК 27001, остальные стараются не отставать от лидеров. Большинство из продуктов реализуют одинаковый функционал, но не все решения одинаковы.

До настоящего момента ОЦИБ рассматривались лишь как технические средства, а такому важному компоненту как организационная составляющая уделялось недостаточно внимания. ОЦИБ не будет работать, если нет соответствующих нормативных документов, работающих процедур и команды ИБ специалистов, которые поддерживают его. Организационный уровень ОЦИБ — это та часть, которая в конечном итоге будет определять, насколько эффективно будет работать ОЦИБ в целом. Выделение в ОЦИБ двух частей: инфраструктурной составляющей и методов поддержки принятия решений, также является шагом вперед по направлению от частных ОЦИБ, разрабатываемых различными компаниями, в сторону открытых систем. Независимость данных компонент улучшит переносимость ОЦИБ и способность к взаимодействию.

Чтобы успешно реализовать проект ОЦИБ необходимо понимать, зачем он нужен, какие идеи и философские концепции в него заложены, то есть идеологию ОЦИБ, а также понимать способы его построения как на техническом, так и на организационном уровне. Эти важные вопросы рассмотрены далее.

2. Идеология ОЦИБ

Две основные цели любого бизнеса, в том числе в банковской отрасли, — это постоянное повышение доходов и сокращение издержек. Информационная безопасность — это состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере [2]. Следовательно, информационная безопасность имеет непосредственное отношение к бизнесу организации. Процессы обеспечение ИБ, с одной стороны, направлены на обеспечение конфиденциальности, целостности и доступности информационных активов и инфраструктуры организации, гарантируя выполнение поставленных организацией бизнес целей, с другой стороны, являются вспомогательными по отношению к бизнесу процессами, требующими затрат на реализацию и поддержку.

Дисциплина ИБ охватывает достаточно большую область знаний. Международный стандарт ГОСТ ИСО/МЭК 17799-2005 устанавливает основные руководящие принципы для инициирования, реализации, поддержки и усовершенствования руководства информационной безопасностью в организации. Цели, приведенные в этом международном стандарте, обеспечивают общее руководство по решению общепринятых задач управления информационной безопасностью. Стандарт содержит несколько разделов. В каждом разделе содержится некоторое число основных категорий безопасности. В одиннадцати разделах описываются:

- политика ИБ;
- организационные вопросы безопасности;
- классификация и управление активами;
- вопросы безопасности, связанные с персоналом;
- физическая безопасность и защита от воздействий окружающей среды;
- управление передачей данных и операционной деятельностью;
- контроль доступа;
- разработка и обслуживание информационных систем;
- управление инцидентами ИБ;
- управление непрерывностью бизнеса;
- соответствие требованиям [3].

Каждое из обозначенных направлений ИБ требуют определенных ресурсов, как человеческих, так временных и финансовых. В небольших организациях в большинстве случаев процессы обеспечения ИБ достаточно прозрачны в силу небольшого количества активов, и перечисленные направления реализуются в рамках одного единого подразделения ИБ. В средних и крупных организациях, к которым относятся банки, как правило, создается выделенное структурное подразделение под каждое из перечисленных направлений. Функции, выполняемые этими подразделениями, с одной стороны, достаточно разные, с другой стороны, близкие друг к другу и имеют пересекающиеся области деятельности. Это предоставляет возможность для качественного улучшения работы процессов соответствующих подразделений, реализации более рационального управления данными процессами и сокращение издержек бизнеса на уровне процессов обеспечения ИБ.

Одним из способов повышения управляемости данными процессами в средних и крупных компаниях, в соответствие с практикой международного опыта, является создание общих центров обслуживания [4]. Общий центр обслуживания — это подход, при котором происходит логическое объединение нескольких взаимодействующих подразделений (родственных вспомогательных бизнес-процессов) с целью рационализации их функционирования. Объединение происходит как на организационном (создание управлений), так и на техническом уровне (использование специализированных программно-аппаратных средств). Подобный подход используется, например, в экономической сфере, когда для ведения бухгалтерского и налогового учета, расчета заработной платы всех подразделений компаний или даже дочерних предприятий создается выделенное подразделение с собственной организационной структурой, использующее специализированную систему управления ресурсами (1С:Бухгалтерия). Аналогичные случаи имеют место в ИТ-подразделениях: для управления и мониторинга сетевого оборудования и серверов, отладки проблем и ведения базы данных конфигураций используются сетевые операционные центры.

Создание таких центров позволяет предприятию сосредоточить внимание и ресурсы на главных целях и задачах бизнеса, а также улучшить внутреннюю организацию служб, для которых эти центры создаются, и тем самым снизить затраты на их поддержание. Особенностью такого подхода является то, что созданный центр может являться подразделением внутри компании или самостоятельным юридическим лицом. В последнем случае используется модель аутсорсинга: заключается договор о предоставлении качественных услуг, в котором максимально подробно фиксируются все бизнес-процессы, ключевые показатели деятельности, взаимоотношения между поставщиком услуг (общий центр обслуживания) и их пользователями (подразделениями компании), денежные вознаграждения и штрафы, выступающие мощным стимулом к повышению качества и эффективности работы. Качество услуг, предоставляемых таким центром, может быть оценено на всех уровнях компании — от высшего руководства до отдельных ее подразделений [4].

Создание единого центра управления проблемами ИБ позволит унифицировать процессы ИБ, выведенные в ОЦИБ, сформировать по единым корпоративным стандартам отчетность, обеспечить непрерывное взаимодействие между подразделениями ИБ, сформировать основу для быстрого принятия решений по проблемам ИБ.

Основными предпосылками для создания ОЦИБ в организации являются следующие:

- наличие разнообразных источников, а также средств сбора и обработки данных аудита, относящихся к обеспечению ИБ;
- большое количество непосредственно данных аудита ИБ, требующих анализа;
- необходимость корреляции и статистической обработки данных аудита и оценки выполнения требований внутренних нормативных документов и положений законодательной базы;
- разрозненные интерфейсы управления и мониторинга средств обеспечения ИБ;
- нерациональное взаимодействие между сотрудниками подразделений ИБ;
- отсутствие унифицированного средства формирования отчетов;

· избыточность штата специалистов, выполняющих однородные функции.

Цели создания ОЦИБ:

· качественное улучшение работы подразделений ИБ за счет использования единого инструмента для управления проблемами ИБ;

· консолидация данных аудита ИБ различных уровней для упрощения их администрирования, мониторинга и анализа;

· предоставление отчетности по событиям и инцидентам ИБ и оценка эффективности средств защиты;

· снижение информационных рисков;

· обеспечение соответствия требованиям нормативных документов.

3. Реализация ОЦИБ

Создание подобного центра для решений проблем ИБ является целесообразным и логичным. Подразделения ИБ выполняют разнообразные функции. В работе может использоваться целый ряд различных технических средств: межсетевые экраны, системы обнаружения вторжений, сканеры уязвимостей, системы контроля доступа, системы управления информационными рисками. Каждое из средств имеет собственный интерфейс управления, интерфейс мониторинга и журнал регистрации событий. Найти реальную атаку в сотнях мегабайт фиксируемых событий практически нереально. Но даже в случае успешного обнаружения угрозы, необходимо оповестить об этом и других заинтересованных лиц — владельцев атакуемой системы или ее администратора, группу реагирования на инциденты и т. п. [5].

Использование разнородных систем для управления ИБ является накладным с точки зрения ресурсов и может быть связано с рядом функциональных ограничений. У одной системы не хватает механизма сопоставления разнородных событий безопасности, у другой — отсутствует эффективный механизм хранения гигабайтов собранных данных, третья — не обладает системой генерации высокоуровневых отчетов, понятных руководству. Чтобы избежать описанных неприятностей, необходимо единое средство, реализующее систему управления информационной безопасностью, которое позволит связать все используемые защитные средства в единый управляемый комплекс [5]. Данная автоматизированная система также должна обеспечивать взаимодействие между подразделениями ИБ на организационном уровне.

Основным предназначением ОЦИБ является комплексное управление проблемами ИБ организации, которое выражается в выявлении проблем и выработке ответной реакции на инциденты ИБ. Поскольку ОЦИБ является автоматизированной системой, то в его состав входят технические средства обеспечения ИБ, которые используют в своей работе некоторые методы поддержки принятия решений и персонал, который выполняет операции, направленные на обеспечение выполнения целей и задач ИБ. Таким образом, в ОЦИБ можно выделить три основных уровня:

· уровень организационной поддержки ОЦИБ;

· уровень методов поддержки принятия решения;

· уровень технического обеспечения ОЦИБ.

На уровне технического обеспечения ОЦИБ находятся программные и аппаратные средства построения ОЦИБ. К этому уровню относятся источники данных аудита ИБ, различные СЗИ, серверы и специализированное ПО, которые используются для реализации ОЦИБ, активное сетевое оборудование и каналы связи. Основная задача данного уровня — реализовать функциональные возможности ОЦИБ (Рис. 2).

На уровне методов поддержки принятия решений происходит вся интеллектуальная обработка данных информационной безопасности, анализ тенденций и выработка рекомендаций по необходимым управляющим воздействиям. На данном уровне работают математические и статистические методы и алгоритмы обработки информации. Уровень методов поддержки принятия решений базируется на уровне технического обеспечения ОЦИБ. Основная задача уровня методов поддержки принятия решений — своевременно предоставить корректную информацию на уровень организационной поддержки ОЦИБ.

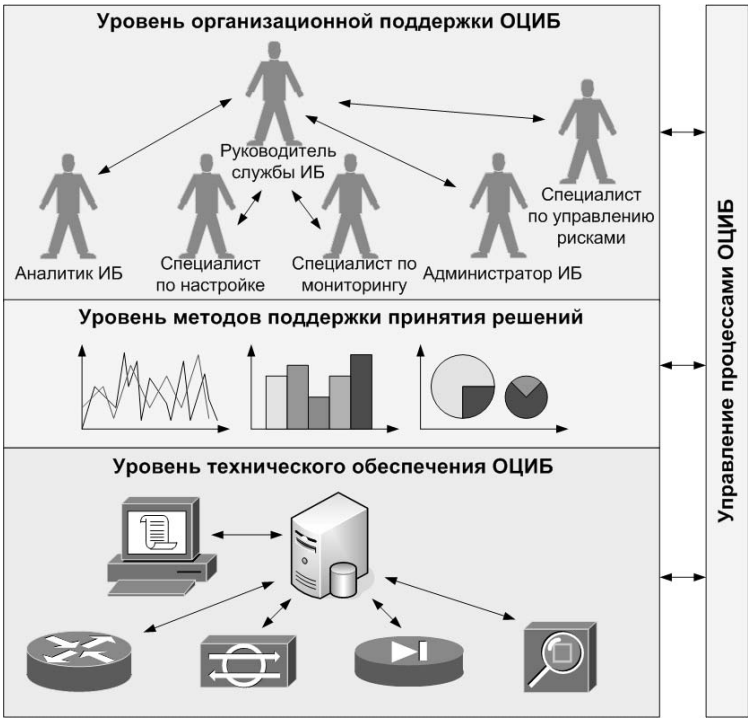

Рис. 2. Структура ОЦИБ

На организационном уровне происходит работа команды специалистов по ИБ. Специалисты по ИБ во главе с руководителем службы ИБ ответственны за обеспечение ИБ организации. В своей работе они предоставляют исходные данные для уровня методов поддержки принятия решений и пользуются его результатами работы. Основная задача данного уровня — способствовать процессу обеспечения ИБ организации, используя средства других двух уровней.

Процессы реализации ОЦИБ на каждом из уровней требуют определенных управляющих воздействий — данные воздействия имеют место на вспомогательном уровне управления процессами ОЦИБ.

4. Заключение

ОЦИБ — это централизованная компонента, предназначенная для комплексного управления проблемами ИБ организации. Идеология ОЦИБ обосновывает необходимость создания, цели и задачи, стоящие перед ОЦИБ. С практической точки зрения, идеология ОЦИБ, предоставляет возможность для экономического обоснования внедрения ОЦИБ в организациях.

Трехуровневая модель ОЦИБ формализует подход к построению ОЦИБ. Выделение в рамках ОЦИБ нескольких уровней повышает прозрачность и понятность процесса разработки, внедрения и сопровождения ОЦИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Security Information Management [Электронный ресурс]: Netforensics / Московский инженерно физический институт. М., 2003. — Режим доступа к ресурсу: http://www.netforensics.com.
2. СТО БР ИББС-1.0-2006. Стандарт Банка России. Обеспечение информационной безопасности банковской системы Российской Федерации. Общие положения. Введ. 2006—01—01. М., 2006. — 27 с.
3. ГОСТ Р ИСО/МЭК 17799:2005. Информационная технология. Практические правила управления информационной безопасностью. Введ. 2005—29—12. М., 2006. — 62 с.
4. *Игнатьев М.* Общий Центр Обслуживания как инструмент повышения эффективности крупной компании // Нефтегазовая вертикаль. 2005. № 15. С. 12.
5. *Лукацкий А. В.* Безопасность сети оператора // Информкурьер-связь. 2005. № 2. С. 15.