АУДИТ БЕЗОПАСНОСТИ: ТРИ ГЛАВНЫХ ЗАБЛУЖДЕНИЯ

Роман Кобцев, Сергей Вихорев
ОАО «ЭЛВИС-ПЛЮС»

Консалтинг и аудит в сфере ИТ 2004, обзор CNews

На фоне возрастающей значимости информации, все большее значение приобретает аудит безопасности. Чтобы объективно оценить необходимость аудита для конкретной информационной системы, необходимо четко представлять суть этого процесса и избавиться от традиционных заблуждений.

Распространенные ошибки

Под аудитом безопасности информации традиционно подразумеваются системный процесс получения и оценки объективных данных о текущем состоянии обеспечения ИБ на объектах, действиях и событиях, происходящих в проверяемой информационной системе. Целью является обследование процессов обеспечения безопасности информации при выполнении информационной системой своего главного предназначения — информационного обеспечения пользователей.

Эксперты подчеркивают, что безопасность информации нельзя ставить во главу угла и считать самоценной, как бы важна ни была ее роль. Главной задачей является все-таки обеспечение бизнеса необходимой ему информацией. Другое дело, что для эффективного ведения бизнеса информация должна быть целостной, конфиденциальной и доступной, а здесь уже без обеспечения безопасности информации не обойтись, но, тем не менее, это всего только «боевое обеспечение».

Даже близкие к сфере защиты информации люди зачастую допускают ошибки при рассмотрении как формы, так и содержания аудита безопасности. Наибольшее распространение получили три заблуждения, основой которых стала популяризация международных стандартов.

Первое заблуждение состоит в том, что многие считают, аудит — это стандарт ISO 17799. Однако если говорить о качественном аудите безопасности, то ISO 17799 скорее необходим для оценки уровня менеджмента безопасностью информации, потому что, во-первых, дает возможность оценки только состояния управления безопасностью информации, а во-вторых, не дает возможности оценки реального уровня защищенности информационной системы. Поэтому в рамках ISO 17799 остается неразрешенный вопрос, достаточно ли принятых мер защиты для обеспечения безопасности информации.

Второе заблуждение: аудит — это стандарт ISO 15408. Несмотря на то, что по популярности этот стандарт сегодня значительно опережает ISO 17799, он также не может в полной мере определить требования к аудиту, т.к. определяет только методологию формирования требований к безопасности информации для продуктов и технологий. Кроме того, он требует разработки профиля защиты и задания по безопасности для оценки правильности реализации функций безопасности. Таким образом, подобный подход не дает ответа на вопрос, все ли реальные угрозы на проверяемом объекте учтены и могут быть устранены.

Третье распространенное заблуждение: аудит — это сканирование и IDS. Между тем, сканирование скорее необходимо для подтверждения состояния безопасности, но не достаточно для качественного аудита, потому что все сканеры, как правило, ищут только заранее известные уязвимости, которые внесены в базы знаний. Кроме того, при сканировании всегда остается вероятность выведения из строя оборудования информационной системы. В результате всегда остается неразрешенный вопрос: если при сканировании не выявлены уязвимости, то их нет на самом деле или их не было на момент проверки.

Единый подход

Можно выделить несколько видов аудита в области безопасности информации, однако стоит отметить, что отличаются они только по цели, а методика их проведения абсолютно идентична. Традиционно выделяют следующие типы аудита:

- первоначальное обследование (первичный аудит)
- предпроектное обследование (технический аудит)

- аттестация объекта
- сюрвей
- контрольное обследование

Первоначальное обследование проводится на той стадии, когда заказчик принимает решение о защите своей информации. На этом этапе заказчику необходимо получить ответ на вопросы — что у него есть реально, насколько это соответствует определенным требованиям и критериям, и после этого получить общее видение проблемы и направление ее решения. Результатом этого аудита может явиться концепция информационной безопасности предприятия, т.е. та система взглядов, которая позволит выстроить грамотную защиту информации. На основе этих результатов может быть выработана политика безопасности — по сути, набор правил безопасности, выполнение которых можно требовать от всех участников информационного обмена.

После проведения первичного обследования, наступает этап технического аудита. На этой стадии в результате сравнения имеющейся или проектируемой информационной системы с моделью угроз данного объекта определяется, какие факторы являются наиболее критичными. Результатом технического аудита может явиться набор требований к системе информационной безопасности. Если говорить о программно-аппаратных средствах защиты, то это может быть профиль защиты или техническое задание. Кроме того, определяется комплекс организационных мероприятий, уровень защиты, и т.д.

В случае, когда заказчику необходимо убедиться, насколько разработанная исполнителем система удовлетворяет поставленным требованиям, наступает следующая стадия аудита — аттестация объекта. Результатом является определенный документ — аттестат соответствия ГОСТу. Хотя возможен и другой вариант, когда заказчику необходимо только заключение эксперта.

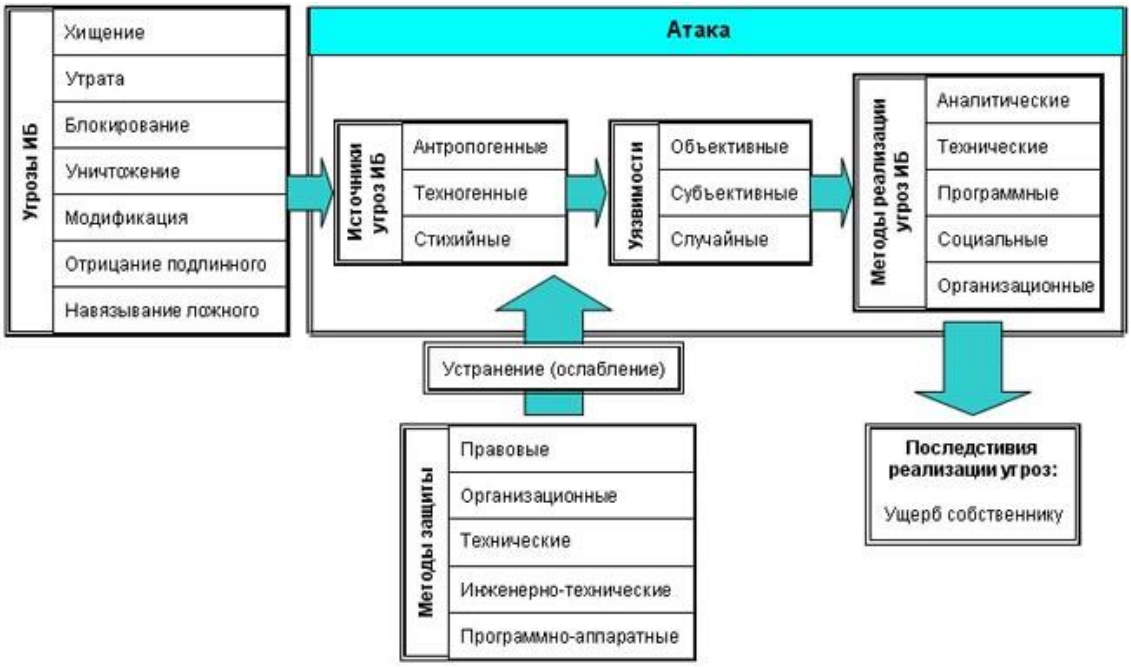
Если собственник информации осознал ценность своей информации, а после первичного обследования пришел к выводу, что в результате потери информации возможны значительные финансовые потери, он может задуматься над возможностью компенсации ущерба. И одним из вариантов является страхование информационных рисков. И в таком случае проводится следующая форма аудита безопасности — сюрвей. Особенностью сюрвея является то, что результаты обследования передаются третей стороне — страховой компании, для определения размера страхового взноса. Результатом является сюрвей-рипорт (экспертное заключение).

Последняя форма аудита — контрольное обследование — проводится в основном в двух критических ситуациях. Во-первых, если произошло событие, приведшее к потере (утрате, искажению и т.д.) информации, и необходимо выяснить причины. И, во-вторых, в случае планового контрольного обследования с целью проверки соблюдения правил безопасности информации.

Угрозы и уязвимости

Сегодня угрозу безопасности информации отождествляют обычно либо с характером (видом, способом) дестабилизирующего воздействия на информацию, либо с последствиями (результатами) такого воздействия. Однако практика свидетельствует, что о том, что такого рода сложные термины могут иметь большое количество трактовок и возможен иной подход к определению угрозы безопасности информации, базирующийся на понятии «угроза». Анализ негативных последствий реализации угроз предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации.

Модель реализации угроз ИБ



В ходе анализа необходимо убедиться, что все возможные источники угроз и уязвимости идентифицированы и сопоставлены друг с другом, а всем идентифицированным источникам угроз и уязвимостям (факторам) сопоставлены методы реализации. При этом важно иметь возможность не меняя самого методического инструментария, вводить новые виды источников угроз, методов реализации, уязвимостей, которые станут известны в результате развития знаний в этой области.

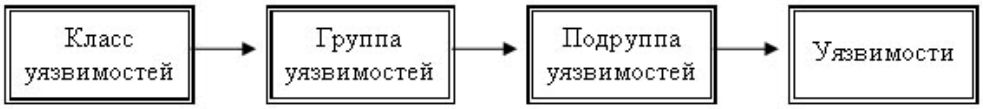
Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, независящим от субъекта проявлений. Наиболее распространенные типы угроз возникают в следующих ситуациях:

- при обеспечении конфиденциальности информации:
  - хищение (копирование) информации и средств ее обработки
  - утрата (неумышленная потеря, утечка) информации
- при обеспечении целостности информации:
  - модификация (искажение) информации
  - отрицание подлинности информации
  - навязывание ложной информации
- при обеспечении доступности информации:
  - блокирование информации
  - уничтожение информации и средств ее обработки

Классификации источников угроз

Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению. Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям.

Классификации уязвимостей



Методы реализации можно разделить на группы по способам реализации. При этом необходимо учитывать, что само понятие «метод» применимо только при рассмотрении реализации угроз антропогенными источниками. Для техногенных и стихийных источников это понятие трансформируется в понятие «предпосылка».

Классификации методов реализации

Классификация возможностей реализации угроз (атак) представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получения промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае такого несовпадения атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, то есть как «подготовка к совершению» противоправного действия. Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

Сам подход к анализу и оценке состояния безопасности информации основывается на вычислении весовых коэффициентов опасности для источников угроз и уязвимостей, сравнения этих коэффициентов с заранее заданным критерием и последовательном сокращении (исключении) полного перечня возможных источников угроз и уязвимостей до минимально актуального для конкретного объекта.
