Как определить источники угроз?

Сергей Вихорев, Роман Кобцев

Прежде чем приступить к созданию системы информационной безопасности, необходимо оценить какие угрозы наиболее актуальны. Данная статья является введением в обширную проблему методологии оценки угроз информационной безопасности.

К тому, что мало-мальски солидная защита информации должна носить комплексный характер, люди уже постепенно привыкли. Однако, организация обеспечения безопасности информации должна не просто носить комплексный характер, но еще и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты. Все больше в прошлое уходит бесполезное нагромождение различных средств защиты как реакция на первую волну страха перед компьютерными преступлениями.

Сегодня комплексная система безопасности информации это не просто комплекс средств, а комплекс мер, направленных на предотвращение потери информации.

Компании больше не хотят выбрасывать деньги на ветер, они хотят покупать только то, что им действительно необходимо для построения надежной системы защиты информации и при этом с минимальными расходами. А чтобы не стрелять из пушки по воробьям или не бросаться с пистолетом на танк необходимо знать о характере возможных опасностей. Еще В.Г.Белинский отмечал, что «найти причину зла -- почти тоже, что найти против него лекарство». Например, нужно ли на компьютер руководителя организации нагромождать кучу средств защиты от НСД, если он и в отдельном кабинете стоит, и кабинет закрыт, а вокруг еще и часовые стоят?

С другой стороны, не мешало бы поговорить о том, как изучать опасности. Можно, например, с криком «Ура» броситься на все грабли сразу, и затем каждую новую «шишку на лбу» «заклеивать» новыми сканерами, межсетевыми экранами и VPN. В результате, конечно, можно получить надежную, проверенную защиту, с которой ваш бизнес может спать спокойно, если, конечно, после всего этого у вас еще останутся средства на продолжение экономической деятельности. Можно поучиться на чужих ошибках. Но, во-первых, учиться на чужих ошибках у нашего народа вообще не принято, а во-вторых, кто же про свои ошибки расскажет? Остается сначала представить все возможные варианты, а затем отобрать наиболее применимые к конкретному случаю. Здесь опять-таки альтернатива: либо использовать накопленный банк данных уже случившихся вариантов проявлений угроз (и не быть до конца уверенным, что все варианты уже проверены), либо попытаться создать методологический инструмент формирования поля возможных проявлений угроз, основанный на изучении всех влияющих факторов и позволяющий рассмотреть даже самые маловероятные варианты. Например, в США только после трагических событий 11 сентября 2001года в гражданских самолетах стали ставить бронированные двери в кабины пилотов, в то время как в СССР, такую угрозу предвидели еще на заре становления гражданской авиации.

Однако не будем лукавить и утверждать, что в природе нет методик проведения анализа рисков. Например, в нашей компании консалтинг в области информационной

безопасности является серьезным направлением, и нами был самым тщательным образом изучен опыт коллег в данном вопросе. Но все имеющиеся на сегодняшний день методики (к сожалению, преимущественно иностранные) позволяют получить только лишь качественную оценку. Это, например, такие методики как Guide to BS 7799 risk assessment and risk management. – DISC, PD 3002, 1998.,Guide to BS 7799 auditing.o – DISC, PD 3004, 1998 (на основе стандартов BS 7799 и ISO/IEC 17799-00). В данных методиках оценка безопасности информации проводится по 10 ключевым контрольным точкам, которые представляют собой либо обязательные требования (требования действующего законодательства), либо считаются основными структурными элементами информационной безопасности (к примеру, обучение правилам безопасности). Эти контрольные точки применимы ко всем организациям. К ним относятся:

- документ о политике информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты;
- средства защиты от вирусов;
- планирование бесперебойной работы организации;
- контроль копирования ПО, защищенного законом об авторском праве;
- защита документации организации;
- защита данных;
- контроль соответствия политике безопасности.

Процедура аудита безопасности ИС включает в себя проверку наличия перечисленных ключевых точек, оценку полноты и правильности их реализации, а также анализ их адекватности существующим рискам. Такой подход может дать ответ только на уровне «это хорошо, а это плохо», а вопросы «на сколько плохо или хорошо», «до какой степени критично или некритично» остаются без ответа. Поэтому сегодня возникла необходимость выработки такой методики, которая выдавала бы руководителю количественный итог, полную картину ситуации, цифрами подтверждая рекомендации специалистов, отвечающих за обеспечение безопасности информации в компании. Рассмотрим, что же легло в основу такой методики.

Эгоизм правит миром, и поэтому вся деятельность всех организаций по обеспечению информационной безопасности направлена только на то, чтобы не допустить убытков от потери конфиденциальной информации. Соответственно, уже предполагается наличие ценной информации, из-за потери которой компания может понести убытки и благодаря нехитрым логическим измышлениям мы получаем цепочку:

источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака).

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». «Угроза» -- намерение нанести физический, материальный или иной вред общественным или личным интересам, возможная опасность (С. И. Ожегов, Словарь русского языка), иначе говоря, понятие *угроза* жестко связано с юридической категорией «ущерб» -- фактические расходы,

понесенные субъектом в результате нарушения его прав (например, разглашения или использования нарушителем конфиденциальной информации), утраты или повреждения имущества, а также расходы, которые он должен будет произвести для восстановления нарушенного права и стоимости поврежденного или утраченного имущества (ГК ФР, часть I, ст.15). Анализ негативных последствий реализации *угроз* предполагает обязательную идентификацию возможных *источников угроз*, *уязвимостей*, способствующих их проявлению и методов реализации. И тогда цепочка вырастает в схему, представленную на рис. 1.

Модель реализации угроз ИБ

Рис. 1.

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, при необходимости, 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. Угроз не так уж и много:

- 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

Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению (Рис. 2).

Рис. 2. Структура классификации «*Источники угроз*»

Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям (рис. 3).

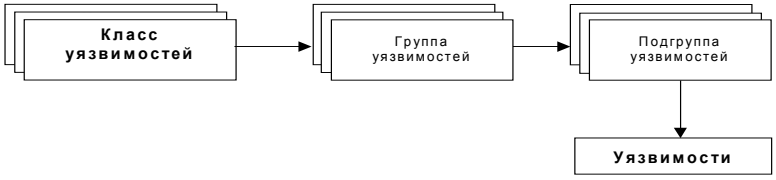

Рис. 3. Структура классификации «*Уязвимости*»

Методы реализации можно разделить на группы по способам реализации (рис. 4). 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».

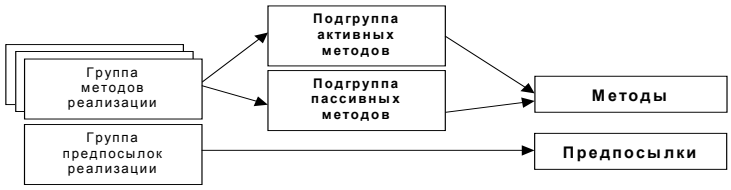

Рис. 4. Структура классификации «Методы реализации»

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.

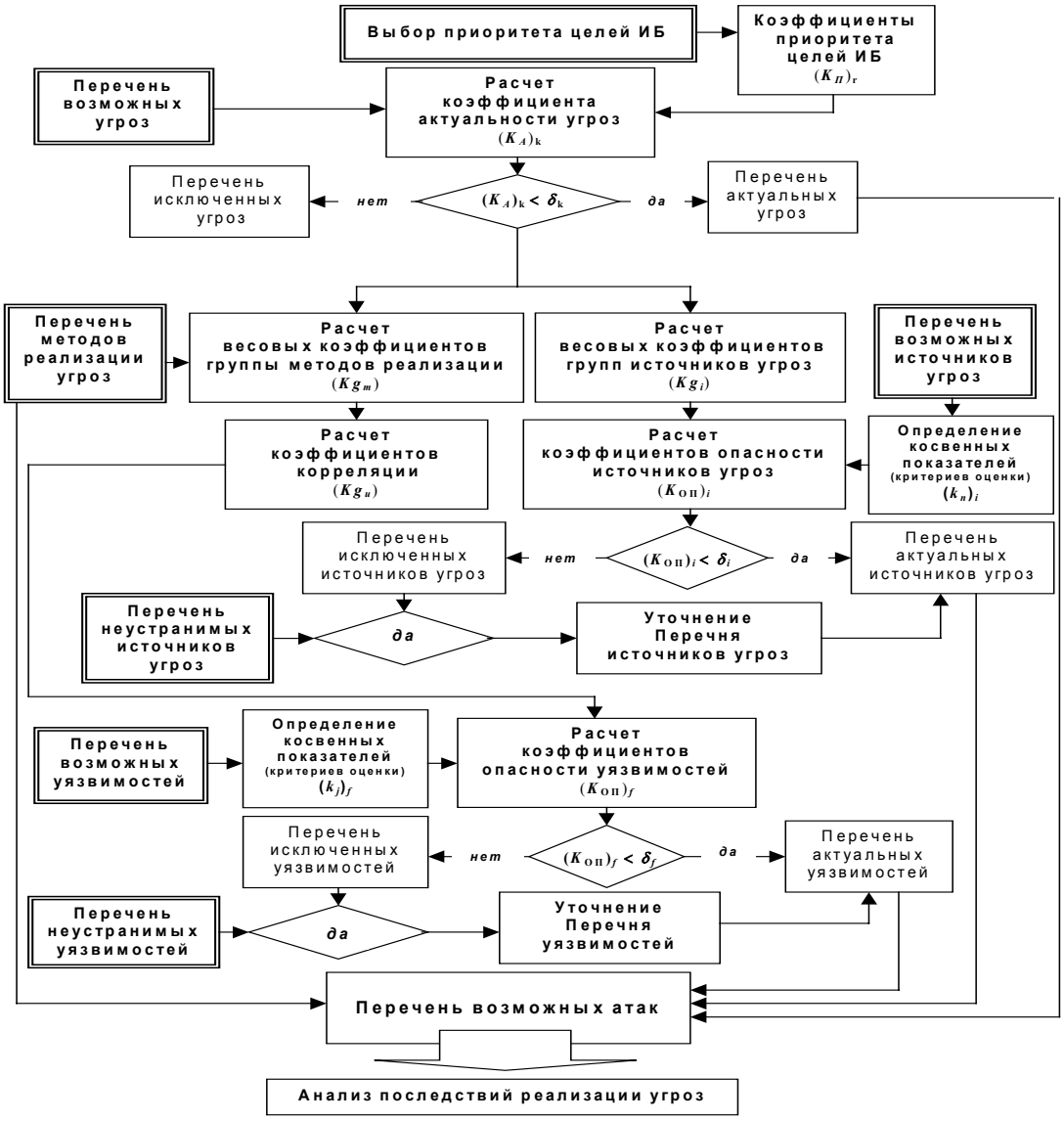

Рис. 5. Алгоритм проведения анализа и оценки

Исходными данными для проведения оценки и анализа (рис. 5) служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых АС и условий расположения и эксплуатации объекта. Благодаря такому подходу возможно:

- установить приоритеты целей безопасности для *субъекта отношений*;
- определить Перечень актуальных *источников угроз*;
- определить Перечень актуальных *уязвимостей*;
- оценить взаимосвязь *угроз*, *источников угроз* и *уязвимостей*;
- определить Перечень возможных атак на *объект*;
- описать возможные последствия реализации *угроз*.

Результаты проведения оценки и анализа могут быть использованы при выборе адекватных оптимальных методов парирования угрозам, а также при аудите реального состояния информационной безопасности объекта для целей его страхования.

При определении актуальных угроз, экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей из которой определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент опасности этих атак как произведение коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее.

Предложенная классификация может служить основой для выработки методики оценки актуальности той или иной угрозы, а уже по выявлению наиболее актуальных угроз могут приниматься меры по выбору методов и средств для их парирования.

Как отмечал С. Дали, «не бойся совершенства, тебе его не достичь» -- все сказанное является нашим сугубо субъективным мнением и не является панацеей при построении системы безопасности информации. Однако нужно всегда стремиться к совершенству и принцип системного подхода к решению вопросов информационной безопасности позволяет заложить комплекс мероприятий по парированию угроз безопасности информации уже на стадии проектирования защищенной сети, тем самым избавив себя от излишних затрат в дальнейшем.

Сергей Вихорев (vsv@elvis.ru), Роман Кобцев, сотрудники ОАО «Элвис Плюс» (Москва)