МЕНЕДЖМЕНТ ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ АВС-АНАЛИЗА

Юрий Копытин
Одесская национальная академия связи им. А.С. Попова (Украина)

Проблем утраты таких важных свойств информации, как конфиденциальность, целостность и доступность, избежать невозможно. Однако ими можно управлять путем менеджмента рисков - полного процесса идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий [1]. Для осуществления менеджмента информационными рисками используют специально разработанные стандарты, методики и рекомендации. Наиболее известные: ISO/IEC 17799 (BS7799), ISO/IEC 27001, ISO/IEC TR 13335-3, BSI, NIST 800-30, MITRE и др..

Цель доклада – продемонстрировать целесообразность использования АВС-анализа в вопросах выбора защитных мер при проведении менеджмента информационными рисками.

Процесс менеджмента информационным риском состоит из следующих основных этапов: 1) идентификации активов; 2) оценки активов и установления зависимостей между активами; 3) оценки угроз и уязвимостей; 4) идентификации существующих/планируемых мер безопасности; 5) оценки рисков; 6) выбора защитных мер; 7) оценки остаточных рисков.

На первом этапе производится идентификация активов информационной системы. К ИТ активам относятся: информация/данные, аппаратные средства, программное обеспечение и т.д. Полный перечень активов в [2].

На втором этапе определяется ценность идентифицированных активов (выраженная в деньгах), а также устанавливаются зависимости одних активов от других, поскольку наличие таких зависимостей может оказать влияние на оценку активов.

На третьем этапе производится идентификация угроз и уязвимостей, вызывающих эти угрозы, характерных данной информационной системе. Для описания угроз и уязвимостей используют классификации угроз и уязвимостей (OCTAVE (США), BSI (Германия), DSECCT (Россия), ISO/IEC TR 13335-3 и др.).

На четвертом этапе создается перечень действующих и планируемых мер безопасности с указанием статуса их реализации и использования.

На пятом этапе определяется величина риска каждого информационного актива. Величина риска

может быть представлена в качественных, количественных, одномерных и многомерных терминах [3]. Результаты анализа величины рисков могут быть использованы при оценке остаточного риска, выборе мер по предотвращению или устранению рисков, оценке затрат на обеспечение поддержания безопасного состояния.

На шестом этапе производится выбор защитных механизмов. Автором доклада предлагается методика определения уровня опасности угроз с использованием АВС-анализа для выбора эффективных защитных механизмов.

Метод «АВС-анализа» можно применять практически в любых областях деятельности с целью выявления первоочередных проблем, которые необходимо устранить, определив их приоритетность.

Согласно [4] АВС-анализ представляет собой следующую последовательность действий: 1) определение цели анализа; 2) определение объектов анализа; 3) определение факторов для дифференциации объектов анализа; 4) формирование информационного массива для анализа; 5) оценка объектов анализа по выделенным факторам; 6) ранжирование показателей; 7) разделение объектов на группы; 8) интерпретация результатов анализа.

Целью АВС-анализа является определение уровня опасности угроз информационной системе для дальнейшего выбора эффективных защитных механизмов.

Объектами анализа выступают активы информационной системы, идентифицированные на первом этапе.

В качестве анализируемого фактора выступает выведенный коэффициент опасности угрозы K_{on}, вычисляемый по формуле:

$$\boldsymbol{K}_{on} = \frac{\sum_{i=1}^{N} \boldsymbol{Y}_i}{\boldsymbol{N} * 10} \qquad (1)$$

где: $\boldsymbol{Y}_i$ - значения базовых показателей от 1 до 10, $\boldsymbol{N}$ - количество базовых показателей.

К базовым показателям относятся: возможность предотвращения угрозы, возможность обнаружение угрозы, частота появления, потенциальная опасность, простота реализации, потенциальное наказание в рамках существующего законодательства, степень защищенности от угрозы и т.п. Количество показателей выбирается в зависимости от степени детализации.

Информационный массив для анализа создается на основе присвоения идентифицированным на третьем этапе угрозам и уязвимостям числовых значений базовых показателей.

В дальнейшем производится: оценка вклада каждого объекта по выбранному фактору; ранжирование объектов в порядке уменьшения анализируемого фактора; вычисление нарастающего общего вклада объекта к общему количеству объ-

ектов в процентах и вклада объекта в общий результат в процентах.

Разделение полученных результатов осуществляется на три группы (A,B,C) при помощи одного из методов. Например: эмпирического метода, метода сумм, метода петли. Группу А составляют очень опасные угрозы; группу В - опасные угрозы; группу С -неопасные. При этом под: неопасными угрозами понимаются те, которые легко предотвращаются или обнаруживаются, нейтрализуются и устраняются; опасными - те, для которых процессы предотвращения, обнаружения и нейтрализации, с точки зрения технологии, не отработаны; очень опасными - те, которые обладают максимальными оценками по всем показателям и реализация процессов противостояния сопряжена с огромными затратами [5].

Суть проведенного АВС-анализа сводится к тому, что максимальный эффект при выборе защитных механизмов достигается при первоочередном закрытии угроз, относящихся к группе А.

На седьмом проводится измерение остаточных рисков, которые всегда имеют место, поскольку система не может быть абсолютно безопасной. Эти риски оцениваются организацией как приемлемые или неприемлемые.

В заключение отметим, что использование АВС – анализа на этапе выбора защитных мер безопасности предоставляет возможность: значительно повысить качество менеджмента информационных рисков; выбрать оптимальные меры безопасности, которые обеспечивают защиту от опасных угроз для конкретного объекта; осуществить легко, быстро и удобно адаптацию систем защиты к изменяющимся условиям.

Литература:

1. ISO/IEC 13335-1:2004 “Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management (IDT)”.
2. ISO/IEC TR 13335-3:1998 “Information technology - Guidelines for the management of information technology security - Part 3: Techniques for the management of information technology security”.
3. *В.В. Домарев*. Безопасность информационных технологий. Системный подход. - ТИД «ДС», 2004. - 992 с.
4. *Фишер Андрей*. Методы выделения групп в АВС анализе [Електронний ресурс]: - Режим доступа: http://www.transmap.ru/articles/view/169
5. *Черней Г.А.* Оценка угроз безопасности автоматизированным информационным системам [Електронний ресурс]: - Режим доступа: http://security.ase.md/publ/ru/pubru01.html