

МЕТОДЫ, ПРИМЕНЯЕМЫЕ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ СЕТЕЙ ТЕЛЕКОММУНИКАЦИЙ

Федоренко В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Утин Л.Л. – канд. техн. Наук

Аннотация. В данной статье рассмотрены современное состояние и подходы к оценке информационной безопасности сетей телекоммуникации. Дан краткий анализ задач оценки информационной безопасности.

В последние годы в сфере связи и информатизации ведется работа по построению современных сетей телекоммуникаций, которые необходимо осуществлять с учетом требований безопасности их функционирования. В основе формирования требований, определяющих необходимый уровень информационной безопасности (далее – ИБ), лежит анализ сетей как объектов оценки ИБ. Однако в настоящее время общей методологии и конкретных методик оценки ИБ не существует. В связи с этим важным является анализ различных подходов к решению аналогичных задач в информационно-вычислительных системах.

В области оценки ИБ в настоящее время развиваются два основных направления [1,2]:

- первое направление основывается на использовании для оценки ИБ совокупности строго определенных требований, которым должны удовлетворять сети телекоммуникаций (качественные подходы);

- второе направление оценки ИБ технологий телекоммуникаций основывается на определении числовых характеристик безопасности используемых технологий телекоммуникаций (количественные подходы).

При оценке ИБ сетей телекоммуникаций вводится понятие риска, под которым понимается вероятный ущерб, зависящий от защищенности сети. Оценка рисков ИБ сетей выполняется либо количественно (риск измеряется в денежных единицах), либо – качественно (по уровням риска: высокий, средний, низкий). Двумя ключевыми элементами при оценке риска является определение последствий угроз и вероятности его нанесения.

В настоящее время известно множество направлений качественной оценки рисков, большинство из которых построено на использовании таблиц. Такие методы сравнительно просты в использовании и достаточно эффективны. Однако не стоит говорить о «лучшем» методе, так как для различных случаев они будут разными. Важно из имеющегося многообразия методов выбрать именно тот, который обеспечивал бы воспроизводимые результаты для данной сети телекоммуникаций.

Некоторые качественные подходы оценивают результаты анализа риска ИБ сетей телекоммуникаций эффективнее всего, выражая его математически в виде скалярной величины с описанием условий для каждой точки. Другие подходы предлагают графическое изображение дерева решения, которое показывает распределение вероятностей самых общих случаев [3,4].

Однако ни одно из указанных направлений не способно в отдельности обеспечить получение объективной, оценки безопасности сети телекоммуникаций. Задача выбора эффективной критериальной основы оценки безопасности технологий телекоммуникаций заключается в определении рационального сочетания этих направлений и в правильном выборе показателей безопасности. Для разработки рационального плана обеспечения безопасности необходимо оценить и вероятность осуществления каждой угрозы безопасности. Общей целью большинства предложенных стратегий оценки риска является получение количественной оценки риска. В качестве наиболее приемлемого метода используется вычисление ожидаемой величины потерь для каждой угрозы. При этом целью применения мер противодействия является уменьшение риска: либо за счет уменьшения вероятности осуществления угрозы, либо за счет уменьшения эффекта воздействия угрозы.

Анализ рассмотренных методик показывает, что для выбора технических средств обеспечения ИБ необходимо располагать достаточно представительными данными по угрозам безопасности и их последствиям. В связи с этим важной задачей является организация сбора и анализа информации о воздействиях угроз и их последствиях, охватывающего большое число объектов различных сетей.

Список использованных источников:

1. Новиков, А.А., Устинов, Г. Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие для вузов. — М.: Радио и связь, 2003. — 296 с.
2. Петренко, С.А., Симонов, С. В. Управление информационными рисками, экономически оправданная безопасность. М.: АйТи: ДМК Пресс, 2004. — 392 с.
3. Dang Depeng, Meng Zhen. Assessment of information security risk by support vector machine. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2010, 3(38), p.46–49.
4. Джураев, Р.Х., Шомаксудов, Б. Ю. Анализ методов обеспечения целостности информации в сетях передачи данных // Труды ICEIC-2008. Ташкент: 24–27 июнь, 2008, С. 304–306.