УДК 004.056.53

Г.А. Вашакидзе, студент; В.В. Паслен, к.т.н., доцент; И.Л. Щербов старший преподаватель, А.Е. Якушина старший преподователь.
Донецкий национальный технический Университет
E-mail: gur.vash@yandex.ru

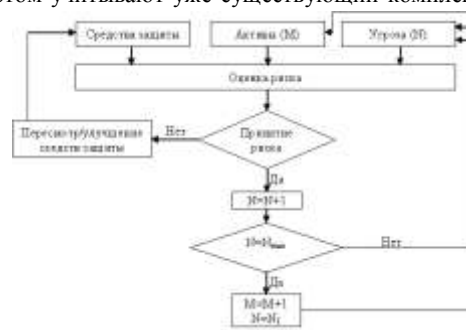
МЕТОДИКА ПРИНЯТИЕ РЕШЕНИЯ ПО ОЦЕНКИ РИСОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В повседневной жизни как отдельно взятого человека, так и государства в целом все значительнее возрастает зависимость процессов жизнедеятельности человека от окружающего его информационного пространства. Данная зависимость приводит к возникновению новых видов угроз – кибернетических преступлений.

Разработка эффективных моделей и методов управления безопасностью информационно-телекоммуникационных систем (ИТС) с целью противодействия кибернетической преступности, является актуальной задачей. Решение данной задачи базируется на требованиях международных стандартов и рекомендаций.

Международным союзом электросвязи в рекомендации МСЭ-Т X.805 предложена архитектура защиты для систем, обеспечивающих связь между оконечными устройствами. Данная архитектура позволяет произвести детализацию составных частей ИТС, с целью упрощения принятия решения, направленного на эффективное управление, контроль и использования сетевой инфраструктуры, услуг и приложений, позволяет более качественно провести оценку риска безопасности ИТС.

С этой целью, исходя из рекомендаций международного стандарта ISO/IEC 27005 «Менеджмент риска информационной безопасности», в начальной стадии принятия решения производится учет активов, уязвимость которых может повлиять на степень защищенности ИТС. Для этого необходимо рассмотреть выделяемые плоскости защиты ИТС. На следующем этапе определяются угрозы для идентифицированных активов. При этом учитывают уже существующий комплекс реализованных мер по защите ИТС.



В случае успешной реализации угрозы активам может быть нанесен ущерб, который может привести к потере свойств информации или управляемости ИТС.

Используя полученные данные, можно получить количественную оценку уязвимости конкретного актива от вероятных угроз. В дальнейшем вопрос принятия риска в упрощенной форме сводится к алгоритму, представленному на рисунке.

Проведенный анализ стандартов и рекомендаций, анализ воздействия угроз на активы ИТС, а также предложенный алгоритм оценки риска приводит к выводу о необходимости скорейшего внедрения данных документов в повседневную деятельность, с целью повышения защищенности ИТС государства.