АВТОМАТИЗАЦИЯ РАСЧЕТА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ PON

Кириллов В. И., Коврига Е. А.
Кафедра метрологии и стандартизации, кафедра систем телекоммуникаций,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: kirillov@bsuir.by, misterbaxx@qip.ru

Разработана блок-схема модели сценария атаки на информацию, передаваемую по пассивным волоконно-оптическим сетям PON, в соответствии с которой на основе конкретизации существующих общих методик предложена методика определения экономической эффективности защиты информации в сетях PON, а также проведена автоматизация расчетов для удобства разработчиков в среде C++ Builder 2009.

На основе анализа и обобщения источников [1-5] авторами была составлена блок-схема модели сценария атаки на информацию, передаваемую по пассивным волоконно-оптическим сетям PON (рис. 1).

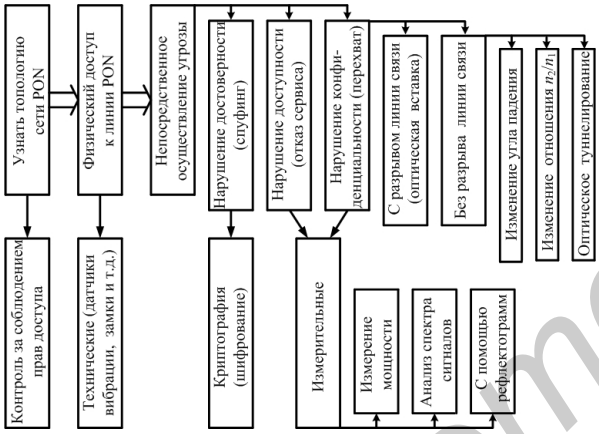

Рис. 1 – Обобщенная модель сценария атаки на информацию, передаваемую по пассивным волоконно-оптическим сетям PON

На рис. 1 все этапы сценария атаки и соответствующие им методы защиты связаны между собой, при этом применение только одного из вариантов защиты не может гарантировать стопроцентную защиту информации. Однако необходимо понимать, что использование всего комплекса защитных мероприятий на каждой ветви «дерева PON» очень затратно и абсолютно неоправданно. Поэтому построение сетей абонентского доступа PON должно анализироваться в зависимости от назначения и степени важности передаваемой информации (сети государственного значения, военных ведомств, организаций, домашние сети и т.д.). Согласно такому разделению и должен выбираться экономически оправданный комплекс защитных мер.

Обобщив методики, приведенные в [6-8], и конкретизировав их в соответствии с полученной моделью сценария атаки на информацию, передаваемую по пассивным волоконно-оптическим сетям PON (рис. 1), предложим методику определения экономической эффективности защиты информации в сетях PON.

Пусть для конкретной сети доступа экспертами даны следующие параметры:

1. Стоимость организации защитных мер: а) стоимость организации контроля соблюдения прав доступа d_1, у.е.; б) стоимость оснащения линий PON техническими средствами d_2, у.е.; в) стоимость оснащения сети измерительными средствами d_3, у.е.; г) стоимость криптографической защиты передаваемых данных d_4, у.е;
2. Потенциальная величина ущерба при выполнении каждой из трех возможных угроз: а) конфиденциальности u_1, у.е.; б) доступности u_2, у.е.; в) достоверности u_3, у.е.;
3. Вероятность перехода злоумышленника к следующему этапу сценария атаки либо к осуществлению самой угрозы при: а) несоблюдении прав доступа p_1; б) отсутствии технических средств защиты p_2; в) отсутствии измерительных средств защиты p_3; г) отсутствии криптографических средств защиты p_4.

Определим вероятную стоимость величины ущерба u, ед.: $u = u_1p_1p_2p_3 + u_2p_1p_2p_3 + u_3p_1p_2p_4$. Как видно из рис. 1, нарушение доступности и конфиденциальности наступят при одновременной успешной реализации злоумышленником трех шагов сценария атаки с вероятностями p_1, p_2 и p_3 соответственно, а нарушение достоверности — при одновременной успешной реализации злоумышленником трех шагов сценария атаки с вероятностями p_1, p_2 и p_4 соответственно.

Аналогичным образом определим вероятную стоимость защитных средств d, ед.: $d = (d_1+d_2+d_3)(1-p_1p_2p_3)+(d_1+d_2+d_3)(1-p_1p_2p_3)+(d_1+d_2+d_4)(1-p_1p_2p_4)$. Вместо стоимости ущерба от каждой из видов угроз подставим суммарную стоимость всех мер, необходимых для защиты от данного вида угроз, а вместо вероятности

наступления угрозы — вероятность ее ненаступления (по формуле полной группы событий).

Как правило, о целесообразности применения выбранной системы защиты информации начинают говорить, если вероятная стоимость величины ущерба превышает вероятную стоимость защитных средств ($u > d$) [7].

Для упрощения и большей наглядности в среде C++ Builder 2009 авторами была написана программа автоматизированного расчета экономической эффективности защиты информации в сетях PON.

После запуска окно программы имеет следующий вид (рис. 2).

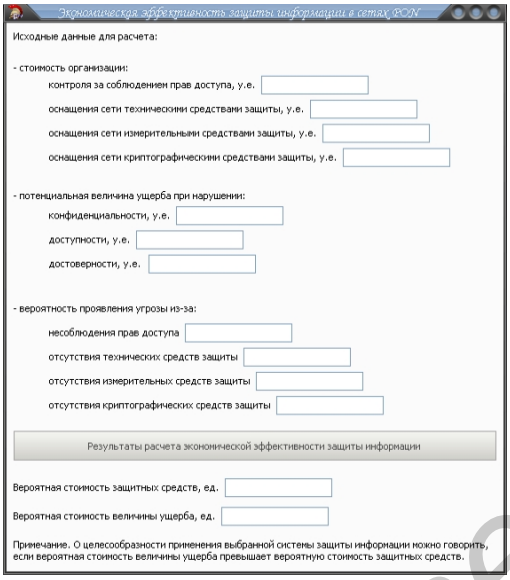

Рис. 2 – Окно программы после запуска

Далее вводим необходимые исходные данные, жмем кнопку «Результаты расчета экономической эффективности защиты информации» и получаем результат (рис. 3).

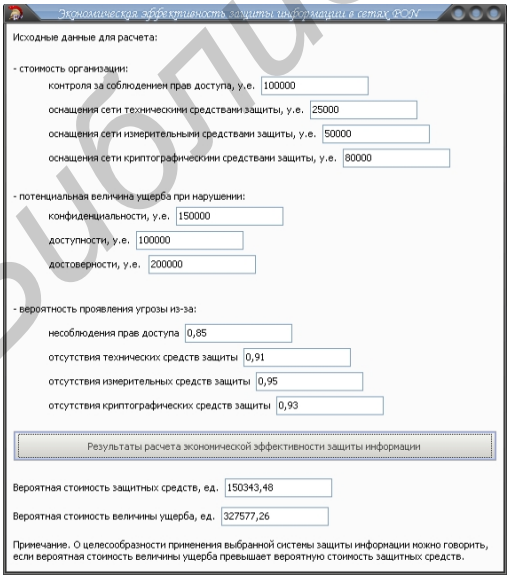

Рис. 3 – Результаты расчета экономической эффективности защиты информации в сетях PON

При вводе исходных данных осуществляются следующие проверки:

а) при оставлении пустыми полей исходных данных и попытке нажать кнопку «Результаты расчета экономической эффективности защиты информации» пользователю выдаются предупреждающие сообщения (рис. 4) до тех пор, пока все поля не будут заполнены;

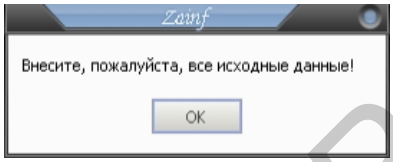

Рис. 4 – Предупреждающее сообщение о нехватке исходных данных

б) при попытке пользователя ввести в поля для определения вероятностей значения, меньшие 0 и большие 1, и дальнейшей попытке нажать кнопку «Результаты расчета экономической эффективности защиты информации», выдаются предупреждающие сообщения (рис. 5) до тех пор, пока все поля не будут заполнены верно.

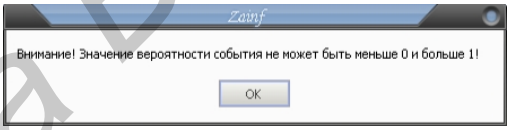

Рис. 5 – Предупреждающее сообщение о несоответствии значений вероятностей

1. Куприянов, А.И. Основы защиты информации: учеб. пособие / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – М.: Издательский центр «Академия», 2006. – 256 с.
2. Хорошко, В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – Киев: Юниор, 2003. – 504 с.
3. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК-Пресс, 2012. — 592 с.
4. Гришачев, В. Фотоника в системах безопасности и защиты информации / В. Гришачев // Волоконно-оптические линии связи, 2011. — №6. — С. 58-63.
5. Булавкин, И.А. Вопросы информационной безопасности сетей PON / И.А. Булавкин // Технологии и средства связи, 2006. — №2. — С. 104-108.
6. Цуканова, О.А. Экономика защиты информации: учеб. пособие / О.А. Цуканова, С.Б. Смирнов. — СПб.: СПб ГУИТМО, 2007. — 59 с.
7. Ажмухамедов, И.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования. Монография / И.М. Ажмухамедов. — Астрахань, 2012. — 344 с.
8. Галкин, А.П. Защита технических каналов связи предприятий и учреждений от несанкционированного доступа к информации: учеб. пособие / А.П. Галкин, В.С. Эмдин. — СПб.: СПб ГУТ им. проф. М.А. Бонч-Бруевича, 2003. — 100 с.