ресурсом – выходным концептом. Данные о значениях вероятностей преодоления барьеров получены из базы данных [2].

В программном модуле предусмотрена функция сохранения проекта на любом этапе работы с возможностью последующего дополнения и изменения. Также предусмотрена функция формирования отчета, содержащего сведения об используемых сервисах безопасности, значениях относительного риска нарушения ИБ сегментов сети и относительного полного риска.

Программный модуль позволяет оценить риски нарушения информационной безопасности при проектировании системы защиты информации, сравнить в количественном отношении различные варианты наборов средств защиты для построения СЗИ.

Программный модуль разработан в среде Borland C++.

СПИСОК ЛИТЕРАТУРЫ:

1. *Степанова Е. С., Машкина И. В., Васильев В. И.* Разработка модели угроз на основе построения нечеткой когнитивной карты в проекции на топологию сети // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 2. Таганрог: Изд-во ТТИ ЮФУ, 2010. С. 232–239.
2. National Vulnerability Database (NVD) Search Common Platform Enumeration. URL: http://web.nvd.nist.gov/view/cpe/search.

М. С. Чистяков, А. П. Дураковский

ОСНОВЫ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ СРЕДСТВ ИЗГОТОВЛЕНИЯ И РАЗМНОЖЕНИЯ ДОКУМЕНТОВ

Следует отметить, что в настоящее время в сфере создания защищенных автоматизированных систем и оценки защищенности средств вычислительной техники остро обозначается проблема применения автоматизированных комплексов оценки защищенности. Проблема состоит в том, что такие комплексы могут быть полезны лишь при участии опытного оператора на каждом этапе проведения исследований. Алгоритмы автоматической выборки и верификации сигналов далеки от совершенства. Таким образом, многие специалисты в области специальных исследований (СИ) предпочитают автоматическому более трудоемкий, но и более точный процесс проведения измерений и расчетов в полуавтоматическом режиме. Проведение СИ вручную и явилось основной целью данной работы. Не любое средство изготовления и размножения документов (СИРД) подвержено утечке информации по каналам ПЭМИН. Проведем некоторую классификацию.

Существует большой выбор критериев классификации СИРД, однако нас интересует лишь один, имеющий значение для оценки защищенности СИРД от утечки информации по каналу ПЭМИН. За критерий классификации возьмем возможность преобразования информации, представленной в виде некоторых физических параметров (области на листе бумаги), в некоторый внутренний код устройства (двоичный код в общем случае). Удобно использовать классификацию по типу внутреннего представления информации. Тогда все СИРД можно будет разбить на две большие группы: информация преобразуется во внутренний код и информация не преобразуется во внутренний код.

Таким образом, первым шагом при проведении СИ некоторого СИРД необходимо определить принцип его работы и, как следствие, целесообразность специальных исследований.