

К ВОПРОСУ ПОВЫШЕНИЯ ОБОСНОВАННОСТИ ПЛАНИРОВАНИЯ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Л.Л. УТИН, М.А. САБЕРИАН

*Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
ullktn@mail.ru, maryam.saberian@yandex.ru*

Разработка программно-аппаратных систем поддержки принятия решений в области информационной безопасности является одним из приоритетных направлений научных исследований Республики Беларусь. Одной из составных задач, решаемых данными системами является повышение качества планирования применения средств защиты информации. В докладе предлагается к обсуждению направления повышения качества решения данной задачи.

Ключевые слова: планирование применения средств защиты, моделирование радиоизлучений средств вычислительной техники, поддержка принятия решений.

В настоящее время выбор организационных и технических мер защиты информации от утечки по каналам побочных электромагнитных излучений и наводок осуществляется, как правило, путем привлечения экспертов в области обеспечения информационной безопасности [1]. Такой подход позволяет наиболее полно учесть требования отечественного законодательства, однако обладает множеством недостатков, одним из которых является недостаточное внимание к исследованиям условий функционирования средств вычислительной техники внутри объектов информатизации типа «защищаемое помещение». В результате требования, предъявляемые к защите информации, как правило, являются завышенными. Основной причиной сложившегося положения дел является отсутствие в Республике Беларусь сертифицированных средств поддержки принятия решений в области обеспечения информационной безопасности. Разработка подобных средств является важной актуальной научной и практической задачей.

Проведенный анализ диссертационных работ, защищенных в Республике Беларусь за прошедшие годы, показал, что в данном направлении отдельными авторами предлагаются достаточно оригинальные решения позволяющие повысить обоснованность применения активных и пассивных средств защиты информации. Например, в работе [2] предложено на этапе планирования применения средств защиты информации, использовать разработанный программный комплекс имитационного моделирования зон радиоизлучений ЭВМ, размещаемых в защищаемых помещениях. Основу данного комплекса составляет методика оптимизации размещения ЭВМ в защищаемом помещении, позволяющая минимизировать уровень радиоизлучений ЭВМ за пределы контролируемой зоны.

Разработанный программный продукт позволяет [3]:

- отображать суммарную зону электромагнитных излучений ЭВМ и других электронных устройств, находящихся в помещении;
- определять расстояние до точки, в которой еще возможен перехват информативных излучений ЭВМ радиоприемной аппаратурой злоумышленников с учетом затухания электромагнитного поля при прохождении его через различные препятствия;

- находить место для размещения ЭВМ в защищаемом помещении, на котором ее излучения за пределы контролируемой зоны будут минимальны;
- отображать потенциально опасные направления распространения излучений за пределы контролируемой зоны;
- отображать зону помех активных средств защиты информации, планируемых к применению в помещении, а также визуализировать степень маскирования информативных излучений ЭВМ;
- осуществлять подбор места расположения генераторов шума для минимизации мощности излучаемых помех, при максимизации удаления средств защиты от рабочих мест персонала;
- подбирать минимальные размеры пассивных средств защиты информации, визуализировать эффективность их применения.

В целом применение данного программного продукта позволяет уже на этапе планирования оценить целесообразность применения тех или иных средств защиты и сократить финансовые затраты на их приобретение за счет оптимизации размещения ЭВМ в защищаемом помещении по критерию минимизации зоны ее радиоизлучений. Однако, в ходе анализа предложенного программного комплекса, был выявлен ряд недостатков, которые могут лечь в основу для дальнейшего совершенствования процесса планирования применения средств защиты информации. Основные недостатки и пути их решения предлагаются к обсуждению.

Список литературы

1. Утин Л.Л., Кред Х.М. Особенности оценки утечек информации через побочные электромагнитные излучения и наводки // Инженерный вестник. 2010. №2(30). С.27–31.
2. Кред, Х.М. Программный комплекс имитационного моделирования зон радиоизлучений средств вычислительной техники в защищаемых помещениях. Дис... канд. техн. наук. Минск, 2013.
3. Утин Л. Л., Григорьев В. Л., Кред Х. М. Усовершенствованная методика построения зоны излучения персональных электронных вычислительных машин // Доклады БГУИР. 2010. №7(53). С.53–58.