СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА ОЦЕНКИ ЗАЩИЩЁННОСТИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Савельев И.А.[1], Антипенко А.О.[2]

Наличие специального (выделенного) помещения для обработки, хранения и передачи конфиденциальной информации, например, переговорной комнаты, стало нормой не только в больших корпорациях, но и в организациях средней величины. Для выявления технических каналов утечки информации проводится специальное исследование, а перед ним строится модель угроз. В работе рассматривается совершенствование процесса оценки защищённости помещения от технических каналов утечки информации путём его автоматизации с помощью разработанного программного средства, что даёт существенную выгоду как во временном выражении, так и в денежном, а также исключает вероятность ошибок на этапе вычислений. Кроме того, в ходе исследования была разработана вероятностная модель реализации угроз конфиденциальным данным на основе модели анализа иерархий Саати.

***Ключевые слова**: модель угроз, автоматизация, специальное исследование, метод анализа иерархий Саати, оптимизация, мобильные приложения, методы и средства обеспечения безопасности, отношение сигнал/шум, информационная безопасность, защита акустической информации, система защиты переговоров.*

DOI: 10.21681/2311-3456-2017-3-35-42

Введение

Специальная комната для переговоров стала неотъемлемым местом совещания по конфиденциальным вопросам сотрудников не только в больших корпорациях, но и в средних предприятиях из-за существенного снижения стоимости оборудования, позволяющего вести несанкционированный съём конфиденциальной информации. Специальное исследование, которое проводится в обязательном порядке для подобных помещений, позволяет выявить «уязвимые места», которые могут привести к утечке информации. После проведения специального исследования и получения его итогов формируются предложения об установке или модернизации уже имеющейся системы защиты информации.

Специальное исследование является сложным комплексом мероприятий, которые предполагают выявление с помощью контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и оценку соответствия уровня защиты информации требованиям нормативных документов [1].

Основными техническими каналами утечки информации при обработке конфиденциальных данных (далее по тексту - КД) в автоматизированной системе конфиденциальных данных (далее по тексту - АСКД) будем считать видовой, побочных электромагнитных излучений и наводок (далее по тексту - ПЭМИН) и акустический (виброакустический). Единственным каналом, съём информации с которого может производиться не только без специального оборудования, но и в случайном порядке, является акустический (виброакустический) канал – особое внимание в работе уделено именно ему.

Реализация угрозы утечки акустической информации возможна при наличии функции голосового ввода или вывода акустическими средствами АСКД КД (с помощью колонок, микрофонов), а также при непосредственном разговоре носителей КД (работников компании) в защищаемом помещении. Несанкционированный съём акустической информации может быть осуществлён как без применения специальных технических средств (нарушитель может, находясь в смежном с защищаемым помещением или коридоре, приложить ухо к недостаточно толстой перегородке и подслушать переговоры по конфиденциальным вопросам), так и с использованием таковых (возможно применение от банальных диктофонов до сложных лазерных систем).

1 Савельев Иван Андреевич, кандидат технических наук, доцент кафедры «Информационная безопасность» ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва, Россия. E-mail: IASavelev@fa.ru

2 Антипенко Антон Олегович, ведущий специалист отдела корпоративной защиты АО «Газпром электрогаз», г. Москва, Россия. E-mail: a.antipenko@elektrogaz.ru

Предлагаемый подход ориентирован на снижение как временных, так и финансовых затрат фирмы, проводящей специальное исследование, путём автоматизации процесса оценки защищённости помещения от технических каналов утечки информации (далее по тексту – ТКУИ).

Для оценки защищённости помещения от ТКУИ строится модель угроз, а затем, исходя из неё, выбирается наиболее опасный ТКУИ. После проводится специальное исследование выделенного помещения по выбранному ТКУИ, на выходе из которого получают соотношения «сигнал/шум» в выбранных контрольных точках и некоторую другую информацию. Эти данные вносятся в программу, которая не только рассчитывает защищённость помещения, но и даёт практические советы по устранению обнаруженных несоответствий.

1. Построение модели угроз и выбор наиболее опасного технического канала утечки информации

Эксперт, по результатам построения модели угроз, заполняет специальную таблицу, при этом её заполнение является чисто субъективной оценкой эксперта тех или иных параметров защищённости исследуемого помещения. В основе модели угроз лежит базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК России. В качестве основных каналов утечки примем ПЭМИН, акустический (виброакустический) и видовой, угрозы, соответствующие своим каналам утечки, возьмём непосредственно из модели ФСТЭК. Таким образом, таблица модели угроз будет выглядеть так, как показано в таблице 1.

Таблица 1. Общий вид модели угроз

Угроза	***Актуальность угрозы***	***Коэффициент реализуемости угрозы***
Угрозы утечки по акустическому (виброакустическому) каналу		
Перехват с использованием аппаратуры, регистрирующей акустические волны	Неактуальная/актуальная	[0; 1]
Перехват с использованием аппаратуры, регистрирующей виброакустические волны	Неактуальная/актуальная	[0; 1]
Перехват с использованием аппаратуры, регистрирующей электромагнитные излучения и электрические сигналы	Неактуальная/актуальная	[0; 1]
Перехват с использованием специальных электронных устройств съёма речевой информации, внедрённых в ВТСС	Неактуальная/актуальная	[0; 1]
Перехват с использованием специальных электронных устройств съёма речевой информации, внедрённых в помещения	Неактуальная/актуальная	[0; 1]
Перехват с использованием специальных электронных устройств съёма речевой информации, подключённых к каналам связи	Неактуальная/актуальная	[0; 1]
Утечка с помощью средств перехвата пейджинговых сообщений и сотовой связи	Неактуальная/актуальная	[0; 1]
Угрозы утечки по видовому каналу		
Перехват за счёт просмотра КД с помощью оптических средств с дисплеев и других средств вычислительной техники	Неактуальная/актуальная	[0; 1]
Просмотр КД с использованием специальных электронных устройств съёма, внедрённых в служебные помещения	Неактуальная/актуальная	[0; 1]
Просмотр КД с использованием специальных электронных устройств съёма скрытно используемых физическими лицами при посещении ими служебных помещений	Неактуальная/актуальная	[0; 1]
Угрозы утечки по каналу ПЭМИН		
За счёт побочных электромагнитных излучений ЭВТ	Неактуальная/актуальная	[0; 1]
За счёт наводок по цепям питания	Неактуальная/актуальная	[0; 1]
За счёт радиоизлучений, модулированных информационным сигналом	Неактуальная/актуальная	[0; 1]
С помощью средств съёма наведённых информативных сигналов с цепей электропитания	Неактуальная/актуальная	[0; 1]

Любая угроза может быть либо неактуальной, либо актуальной. Критерием актуальности угрозы служит возможность реализации данной угрозы в конкретной АСКД, а также её опасность для КД. В качестве коэффициента реализуемости угрозы берётся показатель, определяемый экспертным путём, который характеризует вероятность реализации конкретной угрозы безопасности КД в текущей обстановке. Коэффициент реализуемости каждой угрозы выражается экспертом численно в интервале от нуля до единицы – ноль присваивается, если эксперт считает реализацию данной угрозы невозможной, единица в случае, если эксперт считает вероятность реализации данной угрозы гарантированной. При неактуальности угроза отбрасывается, коэффициент реализуемости не считается.

Модель угроз заполняется экспертом в диалоговом режиме с помощью разработанного программного средства, написанного на языке программирования C/C++ с использованием технологий Qt, позволяющих запускать программу не только в среде операционной системы Windows, но и в других – Mac OS, Linux, Android и iOS, при этом интерфейс приложения масштабируется в зависимости от разрешения дисплея устройства. На рисунке 1 представлен скриншот диалогового окна «Заполнение модели угроз» в операционной системе семейства Windows.

В целях повышения уровня объективности специального исследования предлагается для определения модели угроз привлекать нескольких экспертов – каждый эксперт составляет отдельную модель, проставляя, в соответствии со своим опытом, коэффициенты реализуемости угрозам, и далее, с помощью математического метода взвешенных экспертных оценок Саати, который позволяет определить наилучшую альтернативу из возможных, составляется итоговая (общая) модель угроз. Использование метода Саати начинается с построения иерархической структуры рассматриваемой проблемы. Она, в общем случае, должна состоять из трёх уровней – цель, критерии и альтернативы. На выбор альтернативы напрямую влияет относительный вес каждого критерия, определяемый на этапе построения модели [3].

Следующим этапом исследования выступает построение иерархической структуры конкретно нашей проблемы - в этом случае целью будет выявление наиболее опасного ТКУИ в представлениях отдельного эксперта, угрозы, представленные в общей модели угроз (таблица 1) будут являться критериями, а коэффициент реализуемости, который эксперт присвоил определённой угрозе – весом критерия. Альтернативами будут являться ТКУИ – акустический (виброакустический), видовой и ПЭМИН – обозначенные в общей модели угроз. В конечном итоге все

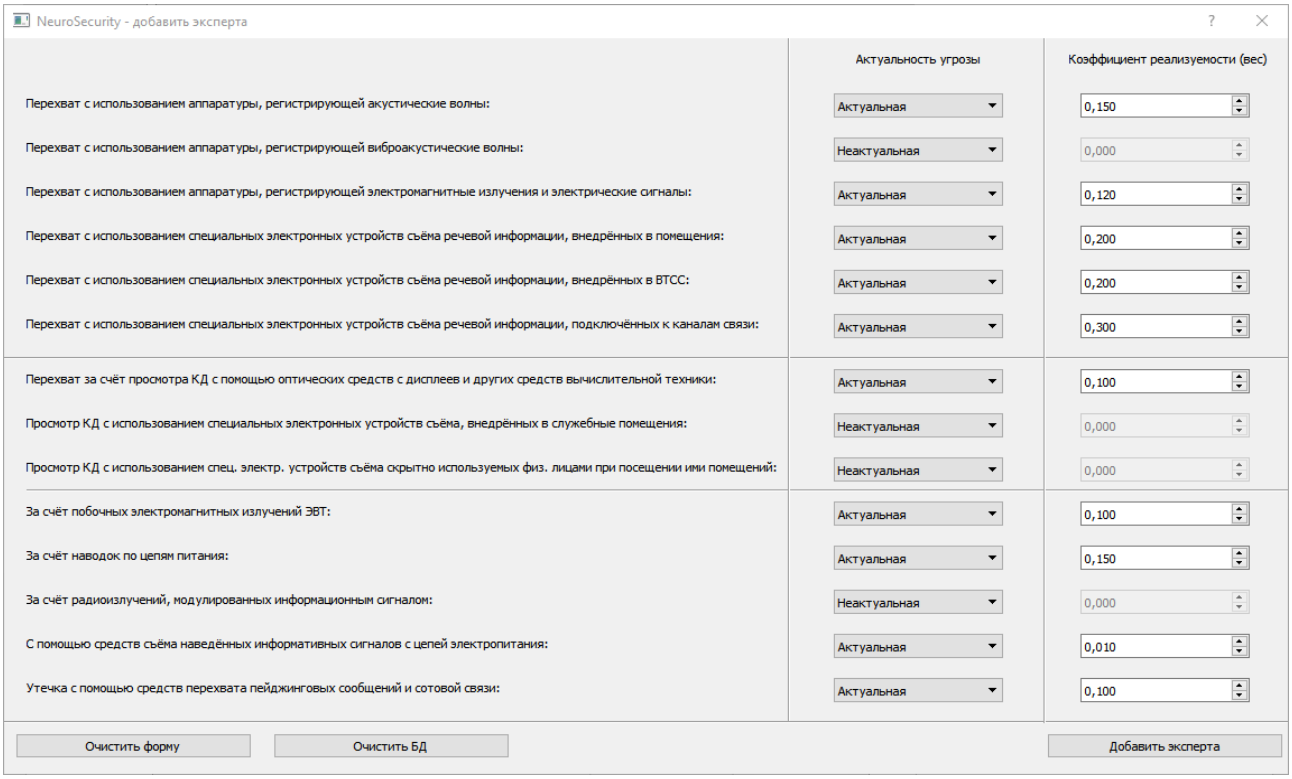

Рис. 1. *Заполнение модели угроз*

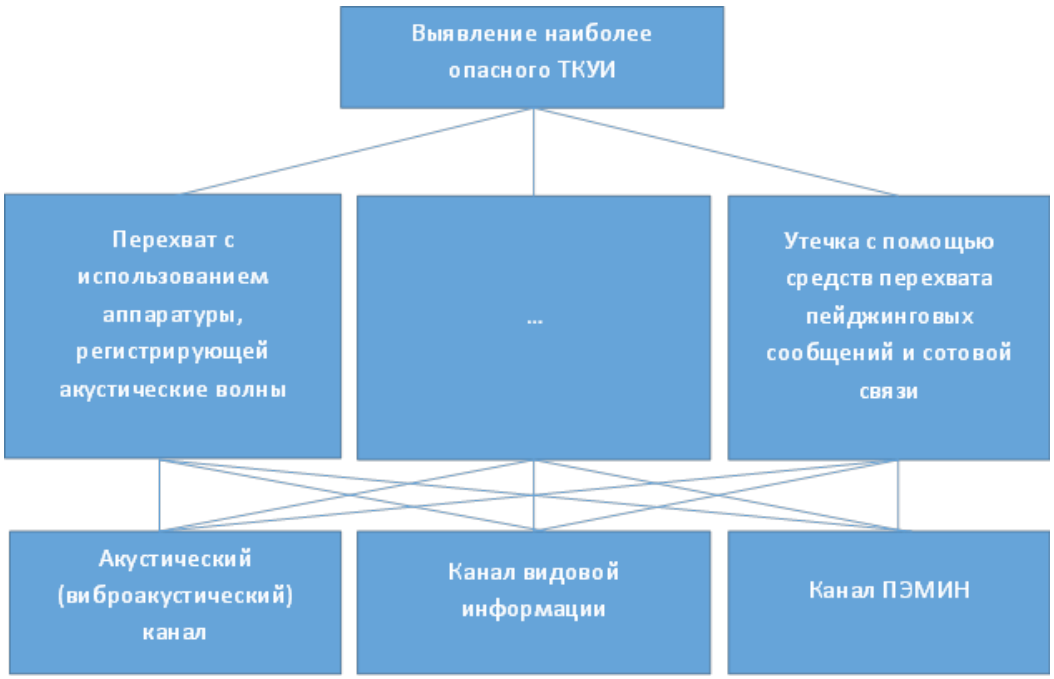

***Рис 2**. Иерархическая структура проблемы выявления наиболее опасного ТКУИ*

критерии поделены на три группы в соответствии со своим ТКУИ, а иерархическая модель проблемы приобретает вид, представленный на рисунке 2. Подчеркнём, что на программном уровне реализовано масштабирование коэффициентов, которое позволяет держать сумму всех весов критериев в единице (обязательное условие применения метода взвешенных экспертных оценок Саати). Самым опасным ТКУИ будем считать канал, имеющий наибольший вес, вычисляемый путём сложения относительных весов групп угроз определённого ТКУИ. В программном обеспечении предусмотрена возможность использования нескольких экспертов – в этом случае происходит подсчёт «голосов» за самый опасный ТКУИ. Таким образом подпрограмма «Модель угроз объекта» предусматривает не только составление этой самой модели, но и выявление наиболее опасного ТКУИ.

Предложенный подход с применением нескольких экспертов для составления общей модели угроз позволяет выбрать именно тот технический канал утечки, который в наибольшей степени уязвим для злоумышленников, позволяя компании сэкономить на установке и эксплуатации неактуальных для её условий средств защиты, и, тем самым, оптимизировать затраты фирмы на защиту своей конфиденциальной информации.

В результате работы подпрограмма «Модель угроз объекта» выводит на дисплей информацию о наиболее опасном ТКУИ, после чего эксперт проводит соответствующее специальное исследование, специфичное для выбранного канала.

На рисунке 3 представлен скриншот результатов работы подпрограммы с рекомендацией проводить специальное исследование акустического (виброакустического) канала утечки информации.

2. Оценка защищённости помещения

За основу алгоритмов оценки защищённости помещения от акустического и виброакустического каналов утечки информации взяты методики расчёта значений показателя защищённости информации, изложенные в работах С. В. Дворянкина,

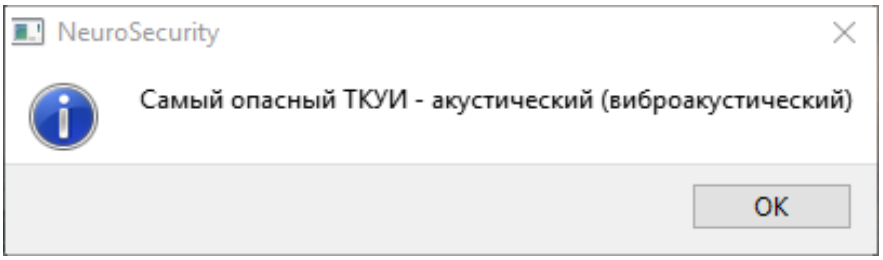

***Рис. 3**. Результат работы подпрограммы «Модель угроз объекта»*

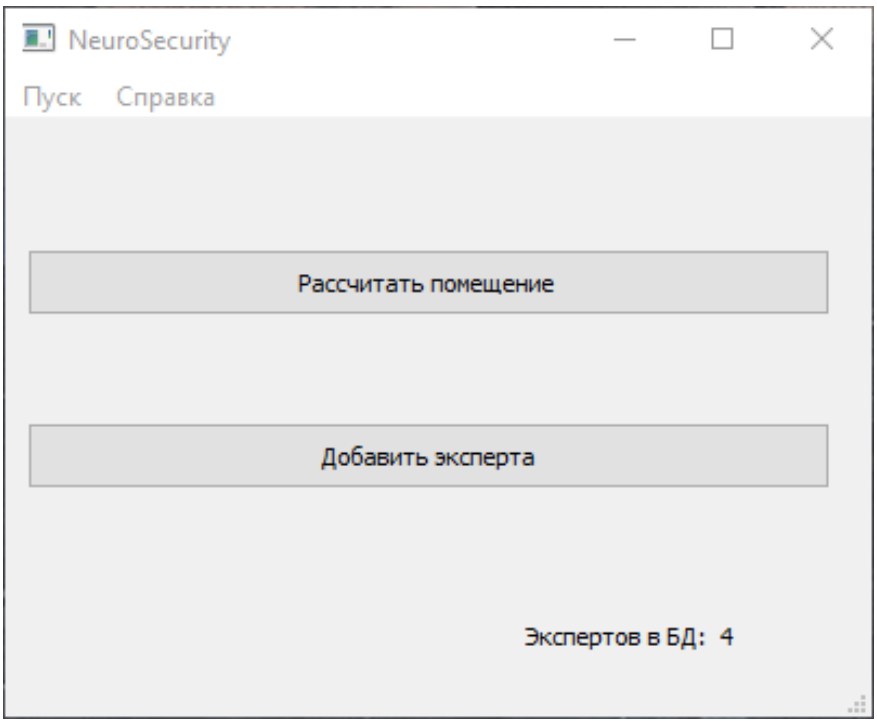

***Рис. 4**. Главное окно программы в ОС семейства Windows*

В. К. Железняка и Г. А. Бузова [1, 4-6] (на основе метода Н. Б. Покровского, для определения показателя разборчивости речи), а также методика, приведённая в Сборнике временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам ФСТЭК России (для определения защищённости помещения от утечки речевой информации по акустическому и вибрационному каналу).

Совершенствование процесса оценки защищённости помещения от ТКУИ предлагается проводить через его автоматизацию с помощью разработанного программного средства, написанного на языке программирования C/C++ с использованием технологий Qt, позволяющих запускать программу не только в среде операционной системы Windows, но и в других – Mac OS, Linux, Android и iOS, при этом интерфейс приложения масштабируется в зависимости от разрешения дисплея устройства.

Фактически программа состоит из двух подпрограмм – подпрограммы «Модель угроз объекта» и подпрограммы «Расчёт помещения». На рисунке 4 представлен скриншот главного окна программы.

Программа является помощником специалиста по технической защите информации в построении модели угроз и в определении защищённости выделенного помещения от ТКУИ. На основе анализа полученных результатов способна выдавать практические советы по улучшению показателей защищённости выделенного помещения.

Алгоритм работы специалиста с подпрограммой «Расчёт помещения» выглядит следующим образом:

1) Получив рекомендацию подпрограммы «Модель угроз объекта» эксперт проводит соответствующее специальное исследование. Исследование проводится с помощью специализированного оборудования, например, для акустического (виброакустического) канала утечки информации применяются системы «Спрут» или «Шёпот». После проведения исследования эксперт получает в распоряжение его результаты в каждой контрольной точке – измерения тестового сигнала, шума, соотношение сигнал/шум, а также коэффициенты затухания и спектральный уровень шума;

2) Результаты проведения специального исследования, полученные на этапе 1, эксперт вносит в подпрограмму «Расчёт помещения». В базу данных подпрограммы внесены основные объекты и стройматериалы, которые чаще всего подвергаются исследованию – начиная от различных дверей и окон, заканчивая кирпичной кладкой определённой толщины. На рисунке 5 представлен скриншот интерфейса ввода в подпрограмму результатов специального исследования. В левой части эксперт выбирает исследуемую ограждающую конструкцию, а в правой вносит результаты проведённого для неё специального исследования. Кроме того, эксперт должен выбрать требуемый уровень защищённости (критерий эффективности защиты выделенного

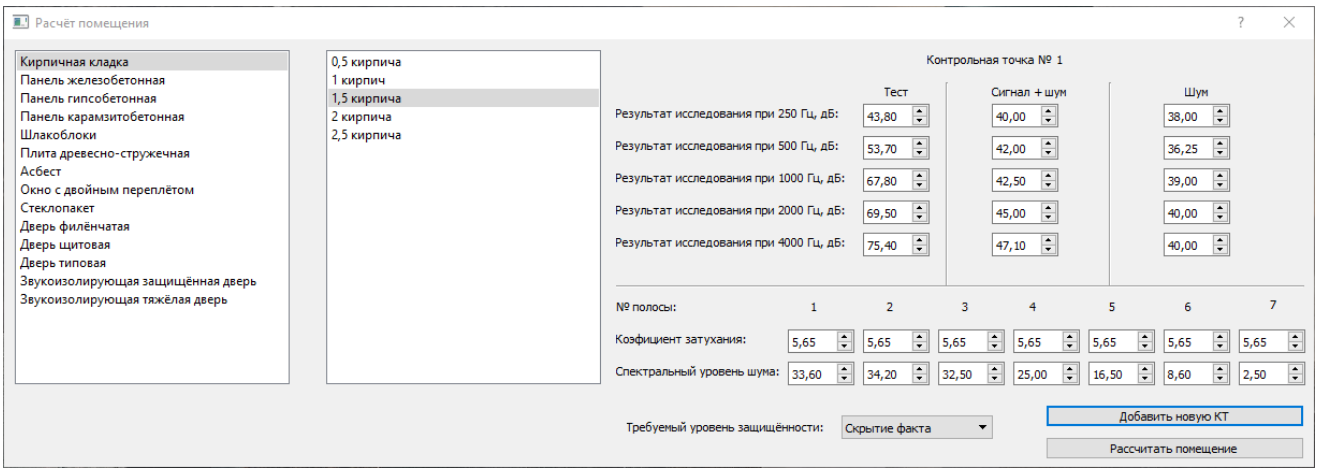

Рис.5. *Ввод результатов специального исследования в подпрограмму «Расчёт помещения»*

помещения) - скрытие факта ведения переговоров, скрытие предмета переговоров, либо же скрытие содержания переговоров. Подпрограмма поддерживает внесение неограниченного количества контрольных точек;

3) Анализируя совокупность результатов проведения специального исследования, введённых на предыдущем этапе, подпрограмма рассчитывает защищённость выделенного помещения от конкретного ТКУИ;

4) После проведения вычислений на этапе 3 подпрограмма выводит эксперту окно с результатами, представленное на рисунке 6. В левой части окна эксперт может либо выбрать полный (общий) отчёт по всем контрольным точкам, либо изучить каждую контрольную точку отдельно. В центральной части окна для эксперта отображается информация о полученном коэффициенте словесной разборчивости для контрольной точки и некоторая техническая информация, а также, в случае неудачного результата, выводятся рекомендации по устранению обнаруженных несоответствий.

Фактически специалист по результатам работы подпрограммы «Расчёт помещения» получает в отчёте полную информацию как о соответствии помещения нормам в целом, так и о каждой контроль точки в отдельности. Начинающему специалисту по информационной безопасности будут полезны рекомендации, которые подпрограмма предлагает для устранения обнаруженных несоответствий – это позволяет использовать разработанное программное средство для обучения молодых кадров.

3. Экономическое обоснование

Для подтверждения экономической целесообразности применения разработанного программного средства был проанализирован рынок специальных исследований выделенных помещений. В поле зрения по-

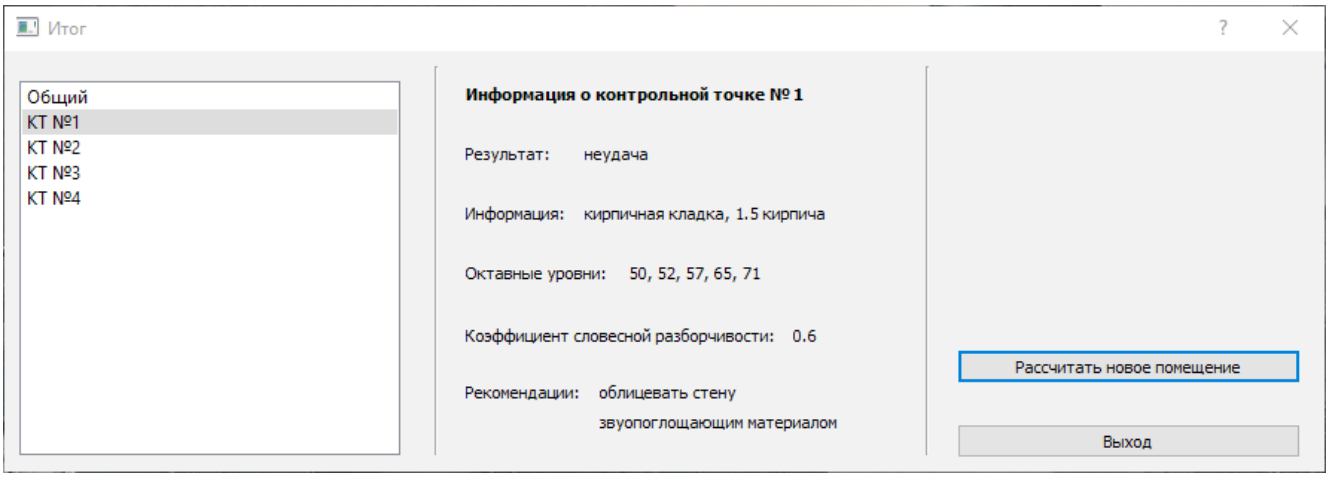

Рис. 6. *Результат работы подпрограммы «Расчёт помещения»*

пали такие компании как ООО «Сюртель», ЗАО НПО «Эшелон», ЗАО «Итеранет», ООО «Центр безопасности информации», ООО «ИС-Комьюнити» и ООО «Аналитические приборы и специальные технологии защиты».

По результатам анализа рынка была выявлена как средняя стоимость проведения специального исследования (60 тысяч рублей за помещение площадью 25 квадратных метров), так и среднее затрачиваемое время (при выборе 15 контрольных точек - 6 часов на измерение показателей и 2 часа на расчёты, итого 8 часов). Исходя из вышеизложенных данных проведение специального исследования обходится в 7,5 тысяч рублей/час, и непосредственно стоимость расчётов составляет 15 тысяч рублей. Отметим, что увеличение количества контрольных точек неизбежно ведёт к резкому возрастанию временных затрат на проведение специального исследования.

Разработанное программное средство позволяет снизить временные затраты на расчёт защищённости выделенного помещения в несколько раз. Например, при расчёте 15 контрольных точек эксперт сократит временные затраты со 120 минут «в ручном режиме» до 30 минут, кроме того, минимизируются возможные ошибки в расчётах – эксперт лишь переносит соответствующие позиции в программу, далее все расчёты происходят автоматически. Фактически стоимость расчётов снижается с 15 тысяч рублей до 3,75 тысяч рублей, то есть ровно в четыре раза.

Таким образом, при использовании разработанного программного средства можно радикально уменьшить время на расчёт защищённости помещения от ТКУИ, и, тем самым, снизить финансовые затраты на проведение специального исследования, что приведёт к увеличению прибыли предприятия (увеличение рентабельности за счёт снижения издержек, либо увеличение количества заказов за счёт снижения стоимости), проводящего специальное исследование. Кроме того, невозможно оценить ущерб, который может понести заказчик и исполнитель в случае «случайных» ошибок как при заполнении модели угроз, так и при подсчёте оценки защищённости выделенного помещения от ТКУИ.

Заключение

В данной статье была построена вероятностная модель реализации угроз конфиденциальным данным на основе метода анализа иерархий Саати, позволяющая привлекать сразу нескольких экспертов для снижения субъективности мнения и оценок отдельных из них. На основе данной модели разработано программное обеспечение в комплексе с программным обеспечением, реализующим расчёт рисков реализации угроз утечки конфиденциальных данных по ТКУИ. Были приведены экономические выкладки с результатами внедрения предлагаемого подхода.

Резюмируя вышеизложенное можно с уверенностью говорить о том, что разработанное программное обеспечение кардинальным образом снизит затраты фирмы, проводящей специальное исследование. Таким образом, была достигнута основная цель работы – усовершенствовать процесс оценки защищённости помещения от ТКУИ за счёт использования релевантных экспертных оценок, а также снизить экономические и временные затраты на оценку защищённости помещения от ТКУИ путём оптимизации процесса специального исследования.

Рецензент: *Дворянкин Сергей Владимирович, доктор технических наук, профессор, заместитель заведующего кафедры «Информационная безопасность» ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва. E-mail: SVDvoryankin@fa.ru*

Литература:

1. А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. «Технические средства и методы защиты информации», Москва: «Горячая линия-Телеком», 7-е издание, 2012.442 с;
2. М. Шлее. «Qt 5.3: профессиональное программирование на C++», Санкт-Петербург: «БХВ-Петербург», 2015.928 с;
3. Т. Саати. Об измерении неосязаемого. Подход к относительным измерениям на основе главного собственного вектора матрицы парных сравнений // Журнал «Cloud of Science». 2015. Т.2. №1. С. 5-39;
4. А.П. Дураковский, И.В. Куницин. Оценка защищённости речевой информации. Часть 1. Выявление акустических и вибрационных каналов утечки речевой информации. М.: НИЯУ МИФИ, 2015. 52 с.
5. С.В. Дворянкин, Ю.К. Макаров, А.А. Хорев. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Журнал «Защита информации. Инсайд». 2007. №2. С. 18-25;
6. В.К. Железняк, Д.С. Рябенко, С.В. Лавров, А.П. Провозин. Методологическое исследование защищённости информации объектов информатизации // Журнал «Вестник Полоцкого государственного университета. Серия С: Фундаментальные науки». 2014. №12. С. 21-29.

УДК 004.056

INCREASING PROCESS OF EVALUATION SECURITY OF ALLOCATED ROOM FROM TECHNICAL CHANNELS OF LEAKAGE INFORMATION

I. Savelyev[3], A. Antipenko[4]

The presence of a special (dedicated) rooms for processing, storage and transmission of confidential information, for example, meeting rooms have become the norm not only in large corporations, but also in organizations of medium size. To identify technical channels of leakage information is carried out a special study, and before him build a model of threats. The paper discusses improving the process of assessing the security of the premises from technical channels of information leakage by automating it with the help of developed software tools that offer significant benefit in terms of time expression, and in money, and also eliminates the possibility of errors during calculations. In addition, the study developed a probabilistic model of realization of threats to confidential data on the basis of the model of analysis of hierarchies Saaty.

***Keywords**: threat model, automation, a special study, Saati hierarchy's analysis method, optimization, mobile apps, methods and security features, signal/noise ratio, information security, protection of the acoustic information, the protection system of negotiations.*

References:

1. A.P. Zajcev, R.V. Meshcheryakov, A.A. Shelupanov. «Tekhnicheskie sredstva i metody zashchity informacii», Moskva: «Goryachaya liniya-Telekom», 7 edition, 2012. 442 p.;
2. M. Shlee. «Qt 5.3: professional'noe programmirovanie na C++», Sankt-Peterburg: «BHV-Peterburg», 2015. 928p.;
3. T. Saati. Ob izmerenii neosyazaemogo. Podhod k otnositel'nym izmereniyam na osnove glavnogo sobstvennogo vektora matricy parnyh sravnenij // ZHurnal «Cloud of Science». 2015. T.2. №1. pp. 5-39;
4. A.P. Durakovskij, I.V. Kunicin. Ocenka zashchishchyonnosti rechevoj informacii. Chast' 1. Vyyavlenie akusticheskih i vibracionnyh kanalov utechki rechevoj informacii. M.: NIYAU MIFI, 2015. 52 p.;
5. S.V. Dvoryankin, Y.K. Makarov, A.A. Horev. Obosnovanie kriteriev ehffektivnosti zashchity rechevoj informacii ot utechki po tekhnicheskim kanalam // Zhurnal «Zashchita informacii. Insajd». 2007. №2. pp. 18-25;
6. V.K. Zheleznyak, D.S. Ryabenko, S.V. Lavrov, A.P. Provozin. Metodologicheskoe issledovanie zashchishchyonnosti informacii ob'ektov informatizacii // Zhurnal «Vestnik Polockogo gosudarstvennogo universiteta. Seriya S: Fundamental'nye nauki». 2014. №12. pp. 21-29.

3 Ivan Savelyev, Ph.D., assistant professor, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: IASavelev@fa.ru

4 Anton Antipenko, a leading specialist of corporate security department of JSC «Gazprom elektrogaz», Moscow, Russia. E-mail: a.antipenko@elektrogaz.ru