внешних специализированных приложениях. Программа имеет простой и интуитивно понятный интерфейс.

Рис. 3. Сцинтилляционный блок БДЭГ 2-38 помещенный в прокачиваемый герметизированный сосуд Маринелли (слева). БДЭГ 2-38 изображен справа

Нами разработана методика определения эффективности сорбции материала при различных скоростях прокачки жидкости с радиоизотопом при использовании на примере Cs-137. Методика основана на относительном измерении удельной известной активности раствора до фильтрации и после нее. Так как удельная активность жидкости до фильтрации известна и геометрия система не изменяется, то удельная активность раствора после фильтрации вычисляется, при заранее установленной величине фона [2]. Как правило, проводится измерение удельных активностей, когда скорость фонового счета на несколько порядков ниже скорости полезного счета. Так же, при вычислениях учитываются отсчеты лежащие в определенных энергетических воротах, соответствующих гамма- линии радиоизотопа. Такая энергетическая дискриминация позволяет пренебрегать фоновыми отсчетами в подавляющем большинстве измерений. Учет фона и размещение свинцовой защиты для зоны детектирования производится в диапазоне удельных активностей 10-100 Бк/л.

1. Лаборатория синтеза и исследования свойств ионообменных волокон. Электронный ресурс: http://ifoch.bas-net.by/structure/laboratory-of-syntheses-and-investigation-of-ion-exchange-fibers.html.
2. Дементьев, В.А. Измерение малых активностей радиоактивных препаратов. – Москва: Атомиздат, 1967. – 140 с.

УДК 004.056.55

МАТЕМАТИЧЕСКАЯ ПОСТАНОВКА ЗАДАЧИ УПРАВЛЕНИЯ РИСКАМИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В СИСТЕМЕ С КОНТРОЛИРУЕМЫМ ПЕРИМЕТРОМ

Медведев Н.В.
Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Введение. Актуальность проблемы несанкционированного доступа (НСД) возрастает пропорционально количеству информации, которая хранится и обрабатывается с помощью информационных систем (ИС). С ростом потоков информации увеличивается и количество пользователей ИС, и как следствие, возрастают риски доступа к данным лиц, не имеющих на то права. Программные продукты, автоматизирующие процесс оценивания риска, не в полной мере позволяют достоверно оценить уровень риска конкретного объекта для обеспечения его информационной безопасности (ИБ). Это связано с определением в них значений вероятностей угроз экспертным путем на основании статистических данных об инцидентах в области ИБ, с отсутствием возможности учесть специфику объекта защиты. Задачей настоящей публикации является математическая постановка математической задачи управления рисками несанкционированного доступа к информации для ее последующего строгого решения.

Обзор критериев анализа рисков и показателей. Под *риском* понимается ситуация, когда внешняя или внутренняя угроза использует уязвимости системы для нарушения её функционирования или совершения иных вредоносных действий. Анализ рисков производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Цель анализа рисков заключается в определении характеристик рисков корпоративной информационной системы и её ресурсов. Результаты анализа рисков используются в рамках мероприятий по экспертизе средств защиты как один из критериев оценки уровня защищённости системы.

При проведении анализа рисков учитываются следующие основные факторы:

- ценность программно-аппаратных и информационных ресурсов системы;
- значимость угроз и уязвимостей;
- эффективность существующих или планируемых средств обеспечения информационной безопасности.

Показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами (преимущественно для стоимостных

характеристик), так и качественными (в частности, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды).

В настоящее время теория и практика выработали множество методов для определения величины информационных рисков. Все эти методы можно объединить в две группы:

1) качественные методы анализа риска;

2) количественные методы анализа риска.

Качественный анализ информационных рисков в инновационной деятельности предприятия позволяет создать структуру рисков. Качественный анализ риска заключается в выявлении источников и причин риска, этапов и работ по проекту, при выполнении которого возникает риск. Он состоит из ряда этапов: определение потенциальных зон риска; выявление рисков; прогнозирование практических выгод и возможных негативных последствий проявления выявленных рисков.

Результаты качественного анализа, в свою очередь, служат исходной базой для проведения количественного анализа.

Выделяют следующие методы качественного анализа рисков:

1. Метод экспертных оценок.
2. Метод рейтинговых оценок.
3. Контрольные списки источников рисков.

В настоящее время известно множество табличных методов оценки информационных рисков компании.

Риск в основном оценивают вероятностной характеристикой (безразмерной величиной от 0 до 1), но могут использовать и частоту реализации риска. Частота реализации - это число случаев возможного проявления опасности за определенный период времени.

Математическая постановка задачи. Исходные данные:

$U = \{u_1, u_2, \ldots, u_n\}$ – множество угроз

$K = \{k_1, k_2, \ldots, k_m\}$ – множество контрмер

Таблица 1 – Матрица покрытия.

	u_1	…	u_n
K_1	d_{11}	…	d_{1n}
…	…	…	…
k_m	d_{m1}	…	d_{mn}

Пусть C = {c₁, …, cₘ} – множество затрат на средства защиты, где C_i – стоимость i-го средства защиты. Таким образом, необходимо решить задачу минимизации стоимости набора, при условии закрытия всех угроз:

$$f(k) = \sum_{i=1}^{m} c_i k_i \rightarrow min,$$

Условия ограничения к задаче:

$$\sum_{i=1}^{m} d_{i,j} k_i \geq 1, \forall\, j \in \{1, \ldots, n\},$$

$$d_{i,j} = \begin{cases} 1, & \text{если } i - \text{ая контрмера закрывает } j - \text{ую угрозу,} \\ 0 & \text{иначе.} \end{cases}$$

$$k_i = \begin{cases} 1, & \text{если средство защиты содержится в наборе,} \\ 0 & \text{иначе.} \end{cases}$$

Решение поставленной задачи. Возьмем за основу дуэльную ситуацию, пусть имеется множество способов атаки, с помощью которых нарушитель может получить доступ к защищаемой информации (множество актуальных угроз) $U = \{u_1, \ldots, u_n\}$, а $K = \{k_1, \ldots, k_m\}$, множество мер, применимых для защиты от актуальных угроз. Пусть $a'_{i,j}$, $a''_{i,j}$ прогнозируемый и остаточный ущерб до и после применения[6]. Рассмотрим матрицу A' размера $m \times n$, состоящую из элементов вида $a'_{i,j}(t) = A'(i,j)$; $i = \overline{1,m}$; $j = \overline{1,n}$; $a'_{i,j}$ – ущерб от j-й угрозы при использовании i-й контрмеры.

Таблица 2 – Матрица прогнозируемых ущербов.

	u_1	…	u_n
k_1	$a'_{1,1}$	…	a'_{1n}
…	…	…	…
K_m	$a'_{m,1}$	…	a'_{mn}

Таблица 3 – Матрица остаточных ущербов.

	u_1	…	u_n
k_1	$a''_{1,1}$	…	a''_{1n}
…	…	…	…
K_m	$a''_{m,1}$	…	a''_{mn}

Пусть $a''_{i,j}$ – остаточный ущерб при использовании i-ой контрмеры для j-ой угрозы, b_i – разница между прогнозируемым ущербом до применения меры защиты и остаточным ущербом, p_i – вероятность реализации угрозы, y – суммарный остаточный ущерб после применения мер защиты:

$$y_i = \sum_{j=1}^{n} a''_{i,j};\ i = \overline{1,m};$$

$$b_i = \sum_{j=1}^{n} (a'_{i,j} - a''_{i,j});\ i = \overline{1,m}.$$

Следовательно, получаем итоговую функцию

$$F(k) = \sum_{i=1}^{m} \left(\frac{c_i + y_i}{b_i}\right) k_i\, p_i \rightarrow min\,.$$

Обеспечив минимум функции F(k), мы сумеем добиться минимизации рисков НСД для ИС с защищаемым периметром.

1. Клейнрок Л. Вычислительные системы с очередями. - М.: Мир, 1979. – 600 с.
2. Медведев Н.В. Исследование процесса функционирования информационных каналов мобильных робототехнических комплексов. // Электромагнитные волны и электронные системы. – 2015. – № 8. – С. 29–36.

3. Методика определения угроз безопасности информации в информационных системах (утверждена 17 февраля 2015 г. заместителем директора ФСТЭК России).
4. Казарин О.В. Особенности анализа рисков утечки конфиденциальной информации по технически каналам при создании радиоэлектронных средств. / О.В. Казарин // Вопросы кибербезопасности Специальная техника. – 2015. – № 4. – С. 62–69.
5. Троицкий И.И., Репин М.М. Организация работы по защите информации на этапе испытаний опытного образца радиоэлектронной техники // Безопасные информационные технологии: сборник трудов Второй всероссийской научно-технической конференции / под ред. Матвеева В.А. – М: Изд-во НИИ радиоэлектроники и лазерной техники, – 2011 – С. 136–138.
6. Феер К. Беспроводная цифровая связь: методы модуляции: пер. с англ. / под. ред. В. И. Журавлёва. – М.: Радио и связь, 2000.
7. Машкина И.В., Рахимов Е.А., Васильев В.И. Методика построения модели комплексной оценки угроз информации, циркулирующей на объекте информатизации / И.В. Машкина, Е.А. Рахимова, В.И. Васильев //Известия ТРТУ. Материалы VIII научно-практической конференции «Информационная безопасность». – Таганрог: ТРТУ, 2006. – С. 70–76.

УДК 621.317.328:621.372.8

ДАТЧИК ЭЛЕКТРИЧЕСКОГО ПОЛЯ НА ОСНОВЕ ЩЕЛЕВЫХ ВОЛНОВОДНЫХ КОЛЬЦЕВЫХ РЕЗОНАТОРОВ С ЖК ЗАПОЛНЕНИЕМ

Гончаренко И.А., Ильюшонок А.В., Рябцев В.Н.
Университет гражданской защиты МЧС Беларуси
Минск, Республика Беларусь

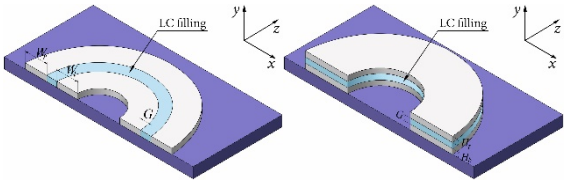
Современные промышленные технологии сопровождаются побочным возникновением электростатических полей при работе электротехнического оборудования, а также целенаправленной их генерацией для технологических процессов. Систематическое воздействие на организм человека сверхдопустимых уровней электрического поля отрицательно воздействует на здоровье человека, может привести к необратимым изменениям в организме. Определение величины напряженности электростатических полей требуется в нефтяной, химической, текстильной и электронной промышленностях (т.е. там, где возникает вероятность появления электрических зарядов, приводящих к взрыву или пожарам), а также в области изучения атмосферного электричества, экологии, медицине и др. В связи с этим приобретают большое значение проблемы, связанные с разработкой новых средств обнаружения и получения информации о параметрах электростатических полей.

Сравнительный анализ показывает, что актуально измерение напряженности электростатического поля в диапазоне от 0,3 до 3000 кВ/м.

В традиционных датчиках электрического поля используются антенны, проводящие электроды или металлические соединения. Наличие металлов в датчиках может приводить к искажениям измеряемых полей. В отличие от них волноводные оптические датчики практически не вызывают возмущение электрического поля, а оптические волокна, соединяющие сенсорное устройство с измерительным блоком, естественным образом устойчивы к электромагнитному воздействию [1].

В данной работе приведена структура, принципы функционирования и измерительный диапазон датчика электрических полей на базе микрокольцевых резонаторов на основе щелевых волноводов с ЖК заполнением.

Мы рассматриваем две структуры микрокольцевого резонатора на основе волноводов с вертикальной и горизонтальной щелью с ЖК заполнением, показанные на рис. 1. Кольцевой микрорезонатор имеет набор резонансных длин волн. Излучение, распространяющееся по входному волноводу на длинах волн, совпадающих с резонансными, поступает в кольцевой волновод. Оставшаяся часть излучения на других длинах волн распространяется дальше, практически не ответвляясь в микрорезонатор. Ответвленное в кольцевой волновод излучение переходит из него в выходной волновод. Таким образом, в выходной волновод поступает излучение узких спектральных диапазонов, центральные длины волн которых соответствуют резонансным длинам волн микрорезонатора. Ширина этих диапазонов задается коэффициентом связи кольцевого и прямых волноводов, а также параметрами самого микрорезонатора.



а *б*

Рисунок 1 – Структуры микрокольцевого резонатора на основе волноводов с вертикальной (*а*) и горизонтальной (*б*) щелью с ЖК заполнением

Если щелевой волновод с ЖК заполнением внести во внешнее электрическое поле, показатель преломления ЖК, заполняющего щель, изменится пропорционально величине электрического поля. Это в свою очередь приведет к изменению эффективного показателя преломления щелевого волновода. В результате изменится оптическая длина кольцевого резонатора и сместится его