На рис. 2 показана зависимость сигнала на выходе кольцевого микрорезонатора на базе волновода с горизонтальной щелью, заполненной ЭОП, от напряженности внешнего электрического поля. Чувствительность и измерительный диапазон датчика на основе волновода с горизонтальной щелью с заполнением ЭОП представлены в табл. 2.

Таблица 2 – Параметры датчика на основе волновода с горизонтальной щелью с заполнением ЭОП с высотой щели 400 нм

Радиус резонатора, мкм	16	32	64
Диапазон измерений, В/мкм	1 … 47	1 … 24	1 … 12
Чувствительность, нА/(В/м)	0,237	0,474	0,982

Как видно из рисунка и таблицы, датчики на основе горизонтальных щелевых волноводов более чувствительны к электрическому полю, чем вертикальные щелевые волноводы. При изменении напряженности электрического поля на 1 В/м ток фотодиода в таком датчике изменяется примерно на 1 нА (чувствительность датчика равна 1 нА/(В/м)). Таким образом, датчик позволяет отслеживать изменение интенсивности электрического поля порядка 30–50 В/м. Однако ширина диапазона измерений значительно уже в сравнении с датчиком с вертикальной щелью (порядка 2×10^7 В/м). Таким образом, волноводы с вертикальной щелью можно использовать для грубого определения напряженности электрического поля, а резонаторы с горизонтально-щелевыми волноводами – для более точного ее измерения.

Датчик позволяет измерять переменные электрические поля с частотой до 10 МГц. Чувствительность датчика ограничена параметрами фотоприемника, в частности, величиной темного тока. При использовании фотоприемника, рассмотренного в работе, датчик позволяет измерять изменения напряженности электрического поля порядка 30 В/м. Чувствительность датчика с ЭОП на порядок хуже, чем у аналогичного устройства с использованием ЖК [3]. Это объясняется тем, что изменения показателя ЭОП под воздействием электрического поля на несколько порядков меньше, чем у ЖК. Однако устройство с ЭОП позволяет измерять поля с частотой до 10 МГц, тогда как датчик с ЖК – лишь до десятка кГц. Тем не менее, разрешение предложенного устройства значительно выше, чем разрешение датчиков на основе нерезонансных структур и сравнимо с разрешением датчиков, использующих резонансные структуры (антенны, кольцевые резонаторы).

Литература

1. Passaro, V.M.N. Electromagnetic field photonic sensors / V.M.N. Passaro, F. Dell'Olio, F. De Leonardis // Progress in Quantum Electronics. – 2006. – Vol. 30. – P. 45–73.

2. Goncharenko, I. Electric field sensing with liquid-crystal-filled slot waveguide microring resonators / I. Goncharenko, M. Marciniak, V. Reabtsev // Applied Optics. – 2017. – V. 56, no. 27. – P.7629–7635.

3. Zhang, X. Integrated photonic electromagnetic field sensor based on broadband bowtie antenna coupled silicon organic hybrid modulator / Xingyu Zhang [et al.] // J. Lightwave Technology. – 2014. – V. 32, no. 20. – P. 3774–3784.

4. Pregla, R. The method of lines for the analysis of dielectric waveguide bends / R. Pregla // Journal of Lightwave Technology. – 1996. – Vol. 14, no.4. – P. 634–639.

УДК 003.26.004.7.004.9

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ УПРАВЛЕНИИ КРИТИЧЕСКИ ВАЖНЫМИ ОБЪЕКТАМИ

Завадская Т.Е.

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

Эффективность любой автоматизированной системы в значительной степени определяется состоянием защищенности (безопасностью) перерабатываемой в ней информации. Этот постулат справедлив, прежде всего, для автоматизированных систем, функционирующих в составе энергетических объектов.

Безопасность информации – состояние защищенности информации, носителей и средств, обеспечивающих ее получение, обработку, хранение, передачу и использование, от различного вида угроз.

Угроза – потенциально возможное событие, действие или процесс, которое посредством воздействия на компоненты информационно-управляющей сети может привести к гибели людей, нанесению материального, морального или иного ущерба ресурсам объекта.

Источниками угроз информации являются факторы внешней среды, человеческий фактор, аппаратные и программные средства, используемые при разработке и эксплуатации информационно-управляющих систем (ИУС) объекта. Порождаемое данными источниками множество угроз безопасности информации можно разделить на два класса: непреднамеренные (случайные) и преднамеренные.

Случайные угрозы связаны, главным образом, со стихийными бедствиями, сбоями и отказами технических средств, а также с ошибками в работе персонала и аппаратно-программных средств. Реализация этого класса угроз приводит,

как правило, к нарушению достоверности и сохранности (целостности) информации в ИУС, реже – к нарушению конфиденциальности, однако при этом могут создаваться предпосылки для злоумышленного воздействия на информацию.

Угрозы второго класса носят преднамеренный характер и связаны с незаконными действиями посторонних лиц и персонала ИУС. В общем случае, в зависимости от статуса по отношению к ИУС злоумышленником может быть: разработчик ИУС, сотрудник из числа обслуживающего персонала, пользователь или постороннее лицо. Большие возможности оказания вредительских воздействий на информацию ИУС имеют специалисты, обслуживающие эти системы. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

Реализация угроз безопасности информации приводит к нарушению основных свойств информации: достоверности, сохранности (целостности) и конфиденциальности. Результатом воздействия угроз является ухудшение качества функционирования аппаратно-программных средств и характеристик обрабатываемой информации, что в конечном итоге приводит к ухудшению качества функционирования ИУС, снижению эффективности решаемых ею задач и тем самым к нанесению ущерба ее пользователям или владельцам.

Преднамеренные угрозы в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

– шпионаж и диверсии;

– несанкционированный доступ к информации;

– электромагнитные излучения и наводки;

– несанкционированная модификация структур;

– вредительские программы.

Действия злоумышленника в рамках указанных пяти групп подпадают под определение терроризма и квалифицируют себя в качестве терроризма кибернетического. В соответствии с ним, терроризм – это сознательное и целенаправленное использование насилия или угрозы насилия для принуждения общества, государства, правительства к реализации политических, идеологических, религиозных, экономических целей организации или отдельной личности.

Особенную опасность для объектов энергетики представляет несанкционированная модификация алгоритмической, программной и технической структур информационно-управляющей системы.

Для достижения требуемой или максимальной достоверности обработки информации ИУС критически важных объектов энергетики используются специальные методы повышения надежности и живучести системы, основанные на введении в структуры обработки информации информационной, временной или структурной избыточности.

Надёжность ИУС – свойство системы выполнять заданные функции, сохраняя во времени значения установленных эксплуатационных показателей в заданных пределах, соответствующих заданным режимам и условиям использования, технического обслуживания, ремонта, хранения и транспортирования.

Живучесть (выживаемость) определяется как свойство объекта сохранять ограниченную работоспособность при воздействии на него угроз двух рассмотренных типов (в том числе при террористических актах). Разделяют структурную и функциональную живучесть.

Структурная избыточность характеризуется введением в состав АС дополнительных элементов (резервирование, реализация одной функции различными процедурами, схемный контроль и др.).

Временная избыточность связана с возможностью неоднократного повторения определённого контролируемого этапа (фазы) обработки информации.

Информационная избыточность характеризуется введением дополнительных источников разрядов в используемые аппаратно-программные средства и дополнительных операций в процедуры переработки информации, имеющих математическую или логическую связь с алгоритмом переработки, обеспечивающих в результате применения выявление и исправление ошибок определённого типа.

При эксплуатации ИУС существует возможность разрушения информационных массивов (ИМ), которая приводит к появлению ошибок в результатах, невозможности решения некоторых функциональных задач или к полному отказу ИУС.

Методы повышения сохранности информации в ИУС в зависимости от вида их реализации можно разделить на организационные и аппаратно-программные.

Совокупность методов и средств обеспечения безопасности информации ИУС критически важного объекта энергетики составляют, в соответствии с ГОСТ Р ИСО/МЭК 15408-2002, политику информационной безопасности такого объекта. Для отработки политики информационной безопасности необходимо имитационное моделирование работы программ и аппаратуры, реализующих рассмотренные методы противодействия угрозам. Натурное моделирование невозможно из-за его дороговизны, математическое – крайне затруднительно в силу слишком значительной размерности интегро-дифференциальных уравнений, составляющих основу модели. В настоящее

время активно разрабатываются моделирующие аналитико-имитационные комплексы средств защиты информации на основе реализации методов искусственного интеллекта.

Утечка информации может происходить и в не действующих, но проложенных оптоволоконных сетях. Для этого злоумышленник искусственно вводит в кабель сигнал, который после будет модулирован акустическими волнами. При такой утечке, обнаружить её можно по наличию излучения, которого быть не должно.

Если утечка происходит в действующей сети, то утечку можно выявить анализом сигнала на модуляцию.

Кроме того, устанавливаются средства диагностики состояния в конце линии, которые проверяют потери интенсивности. Если потери больше 0,1 Дб, то считается, что есть вероятность попытки доступа к информации в ВОЛС. Потери возникают и без установленных средств разведки, но они значительно ниже.

На текущий момент, канал утечки информации для критически важных систем мало изучены. Разрабатываются как методы съёма информации, так и методы защиты. Это мощные программно-аппаратный продукт, способный обеспечить защищённость сети. Однако, даже в таком новом, с точки зрения физики, канале утечки, остаются старые проблемы, в первую очередь проблема НСД.

В общем, критически важные объекты обладают особо опасными каналами утечки. По возможностям утечки он вполне сопоставим с другими каналами, а по характеристикам (пропускная способность и прочее) гораздо опаснее. Можно сделать вывод, что исследования в указанной области являются настоятельной необходимостью.

Литература

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2017. 452 с.

2. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. М.: Издательство МГТУ им. Н.Э.Баумана, 2012. – 304 с.

3. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации. Учебное пособие. М.: Горячая линия – Телеком, 2014 г. – 280 с.

УДК 614.84

ВЛИЯНИЕ НА ДИЭЛЕКТРИЧЕСКУЮ ПРОНИЦАЕМОСТЬ ДРЕВЕСИНЫ РАСХОДА И СПОСОБА НАНЕСЕНИЯ ОГНЕЗАЩИТНОЙ КОМПОЗИЦИИ

Нератова В.В.[1], Антошин А.А.[2]

[1]Научно-исследовательский институт пожарной безопасности и проблем чрезвычайных ситуаций МЧС Республики Беларусь
Минск, Республика Беларусь
[2]Белорусский национальный технический университет
Минск, Республика Беларусь

Нанесение на древесные материалы огнезащитной пропитки способствует снижению горючих свойств древесины. В литературе [1, 2] приводится описание огнезащитных пропиток древесины, поверхностной и глубокой пропитки.

В работе [3] сообщаются результаты оценки влияния расхода огнезащитного состава на диэлектрическую проницаемость обработанной древесины. Исследования авторов [4] позволяют утверждать, что наиболее эффективным методом неразрушающего контроля свойств многих неоднородных материалов является электроемкостной метод. Согласно [5] емкость накладного измерительного конденсатора, заполненного исследуемым материалом, прямо пропорциональна его диэлектрической проницаемости. Следовательно, увеличение или уменьшение емкости накладного конденсатора, расположенного на поверхности образца древесины, говорит об изменении ее диэлектрической проницаемости. Однако в работах [3, 6] не приводится информация о влиянии способа нанесения огнезащитных составов на диэлектрическую проницаемость обработанной древесины.

В настоящей работе изучалось влияние на диэлектрическую проницаемость интервала времени между нанесением слоев огнезащиты при разном расходе наносимых растворов. При проведении измерений использовались сосновые бруски размером 7,5×6×3 см. Исследовалось 2 варианта нанесения огнезащитной композиции КМД-О-2. В 1 варианте нанесение композиции проводилось в два-четыре слоя с интервалом 60 минут при помощи кисти. Во 2 варианте нанесение композиции проводилось в два-четыре слоя с интервалом 24 часа при помощи кисти. Огнезащитная композиция наносилась на древесину с расходами: 0,0178 г/см^2, 0,022 г/см^2, 0,027 г/см^2, 0,031 г/см^2, 0,035 г/см^2, 0,04 г/см^2, 0,044 г/см^2 и 0,049 г/см^2. При расходе 0,0258 г/см^2 и 0,0426 г/см^2 огнезащитная композиция обеспечивает II и I группу огнезащитной эффективности соответственно.