конкретный фильтр, можно заметить, насколько эффективно использование нескольких типов фильтров для одного и того же изображения, т.к. особенности видимых границ объектов воспринимаются разными фильтрами по-разному. Объединение результатов способствует уменьшению общего количества шума в результатах.

Следующим этапом является обработка изображения с точки зрения перспективной развёртки, с целью получения «вида сверху» участка дороги, обозримого в поле зрения видеорегистратора. Для этого необходимо с учётом местоположения видеорегистратора в автомобиле произвести преобразование на основе трапеции перспективы. Для получения конкретных координат удобно воспользоваться имеющимся снимком прямолинейного участка пути. Тогда, сопоставив ребра трапеции с линиями дорожной разметки, можно получить достаточно точные координаты требуемой проекции.

Использовав впоследствии полученную матрицу трансформации для участков пути с изгибом, можно извлекать сведения о радиусе поворота на основе данных о кривизне дорожной разметки. Применив данную развёртку наряду с объединенными фильтрами изображений, мы получим множество точек, которые можно аппроксимировать в кривую на основе данных об их распределении. Метод основан на технике фреймов, когда для каждого горизонтального сегмента изображения выполняется поиск точки с пиковым распределением количества видимых точек. В случае, если несколько фреймов расположено рядом, то это будет оказывать влияние на последующий поиск фреймов, повышая коэффициент вероятности для близлежащих участков. Для реализации данного алгоритма были задействован метод polyfit библиотеки numpy. Полученная кривая достаточно репрезентативно позволяет судить о радиусе кривизны дороги и смещении АТС относительно центра полосы движения.

Зная стандарт ширины полосы движения и ширину видимого участка полосы движения в пикселях на полученном изображении, можно рассчитать соотношение, определяющее, сколько метров реального пространства приходится на видимые пиксели. Для данных тестового видеоряда соотношение получилось равным 0,0052 м/пиксель для горизонтального направления и 0,0414 для вертикального. Эти данные позволяют рассчитать смещение АТС относительно центра полосы движения, а также радиус кривизны поворота текущего участка пути.

Используя эти данные, можно обеспечить практически в режиме реального времени АТС сведениями о его локализации относительно дороги и элементов дорожной разметки.

Таким образом установлено, что на основе данных видеорегистратора и техник компьютерного зрения, существует реальная возможность частичного решения задачи локализации АТС.

Дальнейшее развитие данной модели может лежать в плоскости адаптации алгоритма к различным условиям освещенности местности и обработки прочих объектов, попадающих в поле зрения видеорегистратора.

Литература

1. Camera Calibration With OpenCV [Электронный ресурс]. Режим доступа: https://docs.opencv.org/2.4/doc/tutorials/calib3d/camera_calibration/camera_calibration.html. Дата доступа: 06.04.2020.

2. Advanced Lane Finding Project [Электронный ресурс]. Режим доступа: https://github.com/ kav137/ CarND-Advanced-Lane-Lines.

3. Sobel Derivatives [Электронный ресурс]. Режим доступа: https://docs.opencv.org/2.4/doc/tutorials/imgproc/imgtrans/sobel_derivatives/sobel_derivatives.html.

УДК 004.056

ЗАЩИЩЁННОСТЬ ИНФРАСТРУКТУРЫ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Глинская Е.В.

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

После определения угроз информационной безопасности следует перейти к подробной оценке защищённости системы передачи данных от информационных угроз.

Данная методика предполагает несколько последовательных этапов определения защищённости инфраструктуры передачи данных, которые следует выполнять в определённом порядке по ряду соображений, изложенных непосредственно в описании этапов.

Этап 1. Составление списка сетей передачи данных.

Поскольку угрозы информационной безопасности определяются на высоком уровне разработки системы, в них может быть не отражено реальное разделение инфраструктуры передачи данных [1].

На данном этапе необходимо разобрать всю систему передачи информации ВС, так же как и систему передачи информации от ВС к назем-

ным службам и обратно. Разделение следует производить на основании:

– Физических показателей: подсистема представляет собой ряд соединённых на физическом уровне (проводами, физическими адресами беспроводных устройств) узлов.

– Логических показателей: подсистема представляет собой объединение узлов, выполняющих одну функцию, информация, передающаяся в системе, служит конкретной цели.

– При этом следует обратить внимание на следующие моменты:

– Замкнута ли система передачи данных, или имеет шлюз, через который информация переходит из одной подсистемы в другую?

– Находятся ли все каналы передачи данных системы в помещении одного уровня доступа?

– Имеет ли система или её узлы резервирование по мощностям или по физическим каналам передачи?

– Имеет ли канал передачи физическую защиту в электромагнитной или шумовой области?

– Передаёт ли система информацию только одного типа, или является многозадачной?

Ответы на эти вопросы потребуются на последующих этапах. Результатом этапа 1 должен стать список сетей передачи данных с их детальными характеристиками.

Этап 2. Соотнесение списка сетей категориям.

Данные этапа 1 необходимо систематизировать, разбив все сети передачи данных на ряд категорий, представленных в таблице 1.

Таблица 1 – Категории сетей передачи данных

Сеть физически обособлена?	Сеть логически обособлена?	Категория сети передачи данных
Да	Да	1
Нет	Да	2
Да	Нет	3
Нет	Нет	4

Для каждой категории сети передачи данных в соответствие следует поставить общий коэффициент защиты. Соответственно, ниже следуют описания категорий:

– Категория 1: полностью закрытая сеть. Отсутствие переходов на физическом уровне обеспечивает защиту, а передача информации только одного типа – удобство шифрования и способность определения строгих норм безопасности на уровне всей сети. Базовый коэффициент защищённости сети $К_б = 1$.

– Категория 2: сеть пользуется транзитными механизмами при передаче информации, но источник и приёмник информации всё ещё логически объединены. Это значит, что существует возможность шифровать всю идущую информацию, оставляя открытой только небольшую сетевую часть потока данных, нужную для прохождения через маршрутизаторы. Для данной категории базовый коэффициент защищённости будет составлять $К_б = 1{,}1$.

– Категория 3: физически обособленная сеть, по которой передаётся информация разных типов. При этом за счёт жёсткой привязки источников и приёмников информации можно достичь защищённости от несанкционированного вторжения. В таком случае $К_б = 1{,}15$.

– Категория 4: распределённая сеть общего пользования. По сети, устройства которой подключаются в динамическом порядке и находятся в разных по уровню доступа местах, ходит информация разных классов защиты и разной степени важности. В данном случае проблема шифрования осложнена разнородностью сети, как в плане оборудования, так и в плане информации. Коэффициент защищённости такой сети $К_б = 1{,}2$.

Здесь более высокий коэффициент означает меньшую защищённость инфраструктуры передачи данных.

Данные коэффициенты будут использоваться в качестве весовых коэффициентов для расчёта защищённости сети, но для этого сначала их необходимо дополнительно скорректировать. Это происходит на следующем этапе.

Этап 3. Введение коэффициентов для категорий.

Помимо введённых на этапе 2 категорий существует ряд независимых параметров, определяющих степень защищённости любой сети [2]. Эти параметры являются ответами на вопросы, поставленные на этапе 1. Они определяют дополнительные весовые коэффициенты, которые суммируются с базовым коэффициентом защищённости. Вводимые коэффициенты представлены в таблице 2.

Таблица 2 – Корректирующие коэффициенты

Свойства безопасности	Изменения $K_б$ в зависимости от свойства	
	Выполняется	Не выполняется
Замкнутость системы	–0,1	+0,05
Изолированность сети	–0,1	+0,05
Резервирование	–0,05	+0,1
Защита	–0,15	+0,1
Многозадачность	+0,1	–0,05

После проверки коэффициента $K_б$ на соответствие каждому из указанных в таблице 2 свойств безопасности результирующий коэффициент обозначается базовым коэффициентом сети – $K_{бс}$. Чем он ниже – тем лучше безопасность данной конкретной сети передачи данных.

Этап 4. Выбор угроз, разделение по категориям.

После определения базового коэффициента сети необходимо определить параметры, к которым он будет применяться.

Для определенной инфраструктуры можно раскрыть некоторые рассмотренные там угрозы, поскольку их расширение позволит более полно оценить защищённость инфраструктуры передачи данных, что и является целью данной методики. Несмотря на то, что составление списка угроз не является частью данной методики, для грамотной оценки проведения этой процедуры следует знать этот список.

Этап 5. Для каждой обособленной подсети передачи данных должны быть прописаны свои угрозы.

Угрозы данных должны быть разделены по степени воздействия на информацию (если разные воздействия возможны).

После этого коэффициент реализации угрозы рассчитывается по следующей формуле:

$$K_{\text{Р}} = K_{\text{бс}} \cdot \frac{1}{N} \sum_{i=1}^{N} k_i \cdot n, \qquad (1)$$

где N – общее число источников угроз; k_i – возможность реализации угрозы конкретным типом нарушителя i, этот коэффициент равен 1, если рассматриваемый источник способен реализовать угрозу, и равен 0 в противном случае; n – весовой коэффициент; этот коэффициент равен 0,8 в случае, если рассматриваемый источник – внешний антропогенный нарушитель; коэффициент равен 1,2 – в случае, если угроза реализуется внутренним антропогенным нарушителем; для прочих типов нарушителя (техногенный, стихийный) весовой коэффициент равняется единице.

Этап 6. Определение защищённости сети.

После предыдущего этапа для каждой угрозы есть соответствующий ей коэффициент реализации $K_{\text{Р}}$.

Для оценки защищённости каждой из подсетей передачи данных требуется оценить значения $K_{\text{Р}}$ каждой из угроз, существующих для данной подсети:

– для угроз 1 типа система может считаться защищённой от данной конкретной угрозы, если соответствующий $K_{\text{Р}}$ меньше или равен 0,6;

– для угроз 2 типа система может считаться защищённой от данной конкретной угрозы, если соответствующий $K_{\text{Р}}$ меньше или равен 0,4;

– для угроз 3 типа система может считаться защищённой от данной конкретной угрозы, если соответствующий $K_{\text{Р}}$ меньше или равен 0,25.

Как можно заметить, чем критичнее угроза для системы, тем меньше должен быть коэффициент реализации, что с точки зрения практики означает, что возможность злоумышленнику реализовать данную угрозу должна быть минимальной. Если все $K_{\text{Р}}$ сети передачи данных соответствуют требуемым значениям – она может считаться *защищённой*. Если в сети присутствует $K_{\text{Р}}$ угрозы 1 типа, больший порогового значения, она считается *условно защищённой*. Для некоторых сетей, не связанных непосредственно с ОС РВ, отвечающих за контроль полёта, это приемлемо. При всех других комбинациях $K_{\text{Р}}$ сеть передачи данных считается *недоверенной*.

В целом, инфраструктура передачи данных считается защищённой, если состоит из защищённых и условно защищённых сетей, причём количество условно защищённых сетей не превышает 20 % от общего числа сетей в инфраструктуре.

Литература

1. Смит Д.Д. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов / Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон. – М. Издательский Дом «Технологии», 2004. – 208 с.

2. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета. / Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение». – 2016. – № 6. – С. 85–97.

УДК 621.317.328:621.372.8

ДАТЧИК НАПРЯЖЕННОСТИ ВЫСОКОЧАСТОТНЫХ ЭЛЕКТРИЧЕСКИХ ПОЛЕЙ НА ОСНОВЕ ОПТИЧЕСКИХ ВОЛНОВОДОВ С НЕСКОЛЬКИМИ ЩЕЛЯМИ

Гончаренко И.А., Ильюшонок А.В., Рябцев В.Н.

Университет гражданской защиты МЧС Беларуси
Минск, Республика Беларусь

Развитие методов измерений высокочастотных электрических полей становится важнейшим направлением в области электромагнитных исследований [1, 2]. Оптические датчики электрического поля имеют значительные преимущества перед их электронными аналогами благодаря малым размерам, меньшему весу, более высокой чувствительности, широкому спектральному диапазону, защищённость канала передачи данных от воздействия помех [9]. В работах [3, 4] нами предложены структура и принцип работы оптических датчиков электромагнитных полей на основе микрокольцевых резонаторов на базе оптических волноводов с горизонтальной и вертикальной щелью, заполненной жидким кристаллом (ЖК) или электрооптическим полимером (ЭОП). Датчик с заполнением ЖК обладает высокой чувствительностью, но позволяет измерять переменные электрические поля с частотами лишь до десятков кГц. Датчик с заполнением ЭОП позволяет измерять электрические поля с частотой более 1 МГц, но его чувствительность