повторное получение ВАХ после смены угла облучения по азимуту на 1–5 градусов (дискретность может варьироваться) с помощью датчика гироскопа;

повторение всего цикла измерений по азимуту по достижении 360 градусов, т. е. после полного круга азимута со сменой угла места на 1–5 градусов.

В результате полученные данные можно представить в виде трех графиков для каждого коэффициента полинома, аппроксимирующего ВАХ нелинейного объекта, которые и будут составлять ИП. Пример такого ИП в виде трехмерного графика для квадратичного коэффициента полинома, аппроксимирующего ВАХ диода Д220, представлен на рис. 1. По осям X и Y отложены соответственно градусы угла азимута и угла места, по оси Z значение квадратичного коэффициента. На рис. 2 представлен тот же ИД, но в виде изображения, на котором номера строк и столбцов – это углы места и азимута, а яркость соответствует числовому значению расчетного квадратичного коэффициента.

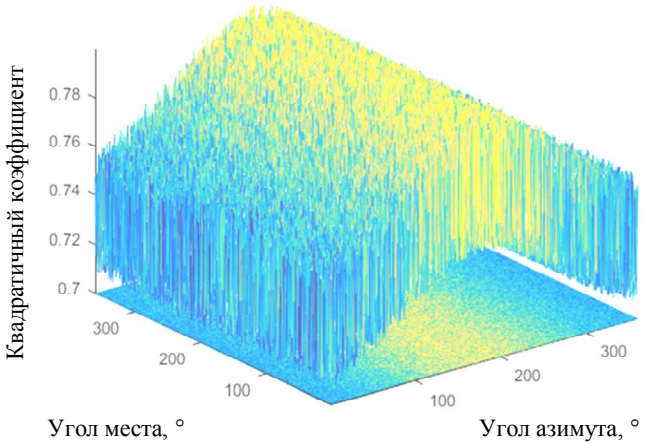

Рис. 1. Идентификационный портрет диода Д220
по квадратичному коэффициенту в виде графика

В результате цифровой обработки данных, полученных при оперативном обследовании, алгоритм поиска определяет степень подобия идентификационных портретов и принимает решение по отнесению исследованного объекта к определенному классу РЭС, который визуализируется в графическом интерфейсе пользователя на персональном компьютере в режиме реального времени, что снижает нагрузку на

оператора, повышает уровень обнаружения и достоверности идентификации, а следовательно, снижает вероятность объявления ложной тревоги.

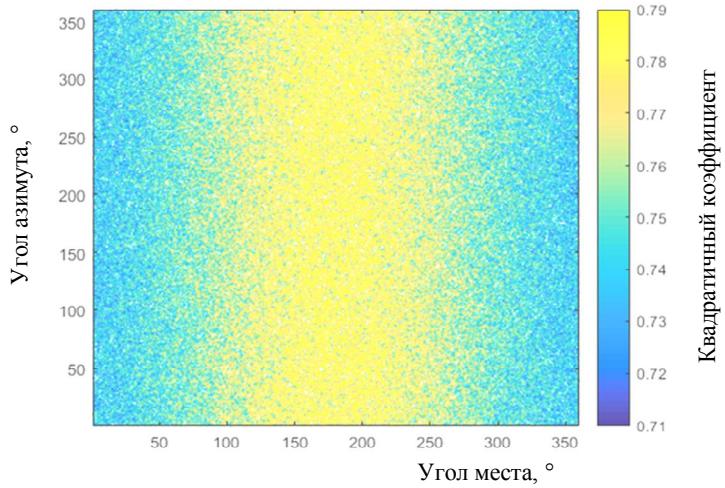

Рис. 2. Идентификационный портрет диода Д220
по квадратичному коэффициенту в виде изображения

УДК 004:34

Т.Г. Чудиловская

ОБЛАЧНЫЕ СЕРВИСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последние годы стремительно развиваются технологии облачных вычислений (англ. cloud computing), которые предлагают удаленный (в том числе через интернет) доступ пользователей к хранилищам данных, вычислительным ресурсам и программным приложениям.

Национальный институт стандартов и технологий США выделяет три модели облачных вычислений: IaaS (инфраструктура как сервис), PaaS (платформа как сервис) и SaaS (программное обеспечение как сервис).

Среда облачных вычислений – это совокупность вычислительных ресурсов в виде виртуальной машины, предоставляемых пользователю с помощью общих сервисов доступа. Физический уровень облачной системы состоит из аппаратных ресурсов, которые необходимы для

обеспечения предоставляемых сервисов, и, как правило, включает серверы, системы хранения и сетевые компоненты.

Использование облачных технологий обладает весомыми преимуществами: возможностью передавать в аутсорсинг высокотехнологические работы по эксплуатации ИТ-инфраструктуры; доступностью широкого набора информационных технологий и ресурсов без приобретения специализированного программного обеспечения и оборудования, а также затрат на обучение и содержание персонала.

Вместе с тем использование облачных технологий имеет и свои недостатки. Система облачных вычислений может подвергаться различным видам угроз безопасности, включая угрозы целостности, конфиденциальности и доступности ее ресурсов, данных и виртуальной инфраструктуры, которые могут быть использованы нецелевым образом, например в качестве площадки для распространения новых атак.

Фактически задачу защиты облака можно разделить на две составляющие: обеспечение безопасности функционирования оборудования и обеспечения безопасности данных. Провайдер должен реализовать защиту своего аппаратно-программного комплекса от несанкционированного вторжения, модификации кода, взлома ИТ-системы, чтобы обеспечить защиту данных клиента. Клиент, в свою очередь, при необходимости размещения каких-либо важных и секретных данных может использовать технологии шифрования для защиты от несанкционированного доступа к ценной информации.

При этом важно учитывать, что возможности пользователя по управлению системой безопасности зависят от выбора сервисной модели. В модели IaaS провайдер контролирует лишь физическую и виртуальную среду, в которой работают виртуальные машины клиентов; он не занимается обслуживанием операционных систем и приложений, функционирующих внутри самих виртуальных машин. На стороне заказчика можно построить свои собственные технические средства обеспечения безопасности. Клиент может иметь полный контроль над реальной конфигурацией сервера, что гарантирует ему больший контроль рисков безопасности окружения и данных. В PaaS поставщик управляет лишь аппаратной платформой и операционной системой, что ограничивает способности предприятия заказчика в управлении рисками на этих уровнях. В модели SaaS провайдер облачной услуги полностью контролирует физическую и логическую инфраструктуру, занимается его разработкой и обслуживанием, оставляя пользователю лишь возможность загружать свои данные и работать с ними.

В сложившихся условиях специалистами все большее внимание уделяется вопросам разработки средств защиты, позволяющих противодействовать угрозам информационной безопасности со стороны злоумышленников, на основе единого концептуального подхода, сочетающего в себе преимущества разных методов защиты информации.

Активное распространение облачных сервисов и очевидная выгода от работы на этом направлении привела к появлению концепции «всё как сервис» (Everything as a Service, XaaS). Среди набора услуг, предоставляемых провайдерами, в последнее время набирают популярность облачные сервисы для информационной безопасности, или безопасность как услуга (Security as a Service, SecaaS). Безопасность как сервис – это обеспечение безопасности, осуществляемое удаленно на базе системы, находящейся в собственности поставщика услуги, с оплатой по факту использования.

Преимуществами сервисов безопасности являются:

быстрое развертывание. Чтобы начать пользоваться сервисом, не требуется дополнительного программного обеспечения или аппаратных устройств;

аутсорсинг административных задач;

использование лицензионного программного обеспечения;

стабильное обновление антивирусов, black-list (черных списков) и других ресурсов защиты;

снижение издержек на поддержание работоспособности аппаратного и программного обеспечения;

гибкая система оплаты за потребленные ресурсы;

отсутствие необходимости содержать штат специалистов определенной квалификации в области информационной безопасности;

доступность при наличии подключения к сети Интернет;

надежность и устойчивость сервиса благодаря технологии отказоустойчивости и уровня надежности.

В зависимости от выбора программного продукта Security as a Service включает в себя целый набор программ и сервисов для обеспечения комплексной безопасности: антиспам-защиту, антивирусную защиту, защиту от атак «отказ в обслуживании» (DoS/DDoS), оценку безопасности, защиту мобильных устройств (поддержка IOS/Android), управление, обнаружение и предотвращение вторжений.

Кроме основных сервисов услуга может предоставить и дополнительные, к которым можно отнести: шифрование данных, непрерывность бизнеса и восстановление после катастроф (предотвращение потери данных), управление учетными записями и доступом, управление событиями информационной безопасности, предотвращение утечек данных.

В настоящее время лидирующими продуктами Security as a Service являются McAfee Security-as-a-Service, Panda Security Cloud Protection, Symantec.cloud и Zscaler Cloud Services.

Задача обеспечения информационной безопасности становится все более сложной и ресурсоемкой. Грамотно применяя облачные сервисы для информационной безопасности, клиенты получают выстроенные процессы защиты, возможность оперативно подключать или отключать услугу, оплачивая только тот объем сервисов, который необходим в конкретный момент времени.

УДК 355.4

А.Н. Шедько

СОЗДАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В настоящее время проблема обеспечения безопасности критически важных объектов информатизации (КВОИ) в каждом государстве приобретает все более актуальный характер. И в Республике Беларусь, и в Российской Федерации также уделяется значительное внимание этой проблеме. В частности, отмечается, что информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Также определяется, что угрозы информационной безопасности предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Создание системы безопасности (СБ) КВОИ предлагается рассматривать на примере стационарной цифровой автоматической телефонной станции (АТС) узла электросвязи сети общего пользования, обеспечивающей предоставление услуг в населенном пункте Республики Беларусь с численностью не менее 20 тыс. человек (далее – районный центр).

Объекты информатизации (ОИ) данной АТС размещены в пределах области действия одного комплекса безопасности (КЗ) и используются как критичные активы, так и обрабатывается общедоступная (открытая) информация, хотя одно или несколько средств вычислительной техники из совокупности имеют открытые каналы обмена информацией за пределами КЗ с другими ОИ. Так как при этом обеспечивается доступность и целостность критичных активов путем реализации мер,

направленных на предотвращение умеренного ущерба, то данным КВОИ присвоен класс В2-у.

Согласно перечню показателей уровня ущерба национальным интересам Республики Беларусь в социальной и демографической сферах в случае возникновения угроз различного характера в отношении ОИ (его составляющих элементов) уровень ущерба определяется с учетом того, что АТС размещена в районном центре, и оценивается как умеренный при прекращении функционирования на период от 48 до 72 ч более одной сети электросвязи (стационарная или сотовая подвижная электросвязь, передача данных, в том числе с доступом в сеть Интернет).

Если АТС в целом невозможно отнести к КВОИ, то приказом ее руководителя создается комиссия по отнесению отдельных ОИ АТС к КВОИ, утверждается ее председатель и состав. Комиссией составляется перечень ОИ АТС с их описанием (состав комплекса технических средств (средств электронной вычислительной техники), структура используемого программного обеспечения (перечень), общая функциональная схема (схема сети), наличие и характер взаимодействия с другими объектами и т. д.), который утверждается руководителем АТС. Для каждого из перечня ОИ АТС комиссия устанавливает отраслевые критерии отнесения ОИ к КВОИ методом экспертных оценок: определяются отраслевые критерии, перечень которых утвержден, и соответствие данных ОИ отраслевым критериям отнесения ОИ к КВОИ в соответствии с методикой, также утвержденной.

Руководителю АТС представляется отчет по результатам оценки соответствия ОИ АТС отраслевым критериям отнесения ОИ к КВОИ и составляются заключения о соответствии отдельных ОИ АТС отраслевым критериям отнесения их к КВОИ по утвержденной форме. В частности, к КВОИ комиссией может быть отнесена локальная информационная сеть АТС. Указанные заключения с описанием ОИ прилагаются к мотивировочному ходатайству и направляются по подчиненности в вышестоящую организацию для принятия решения об отнесении ОИ АТС к КВОИ.

При рассмотрении практических аспектов создания СБ КВОИ уже упоминалось о том, что в рамках создания СБ КВОИ разрабатывается и внедряется система менеджмента информационной безопасности.

Кардинальной мерой повышения защищенности сетей связи могла бы стать замена телекоммуникационного оборудования иностранного производства на «доверенное» отечественное, сертифицированное. Однако данное мероприятие сложное в организационно-техническом плане, требует больших затрат. Приемлемой альтернативой является оснащение существующего оборудования связи специализированными техническими средствами защиты.