УДК 536.37

СТЕНД ДЛЯ ИССЛЕДОВАНИЯ ДИНАМИКИ ИЗМЕНЕНИЯ ТЕПЛОВЫХ ПОЛЕЙ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ АППАРАТУРЕ ПРИ ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

А.И. КУХАРЕНКО, Г.В. ДАВЫДОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 20 сентября 2018

Аннотация. В работе представлена схема и принцип работы стенда, предназначенного для исследования динамики изменения тепловых полей в информационно-коммуникационной аппаратуре при оценке защищенности информации от утечек по физическим каналам связи. Предоставлены результаты апробации стенда при исследовании нагрева электронных компонентов на тестовой печатной плате, также показан результат воздействия провоцирующего электромагнитного сигнала на модуль с каналом связи IEEE 802.11g (Wi-Fi). Определены численные границы обнаружения нагрева электронных компонентов, представленные в виде минимальной подводимой мощности нагрева. Предложены мероприятия по снижению влияния на термографическое изображение рассеивающих свойств поверхностей проверяемых объектов, дрейфа температуры окружающей среды, высоких шумов изображения, а также инерционности тепловых процессов.

Ключевые слова: инфракрасное излучение, защита информации, тепловизор, недекларированные возможности, провоцирующее воздействие.

Abstract. The paper presents the scheme and the work principle of the stand, designed to study the dynamics of the change in thermal fields in information and communication equipment, used for assess the protection of information from leaks via physical communication channels. The results of approbation of the stand during the study of heating of electronic components on a test printed circuit board are presented, as well as the result of the effect of the provoking electromagnetic signal on the module with the IEEE 802.11g (Wi-Fi) communication channel. The numerical limits of detection of heating of electronic components are determined, represented in the form of the minimum necessary heating power. It are proposed the measures to reduce the effect on the thermographic image of the scattering properties of the surfaces of the objects under test, the drift of the ambient temperature, high image noise and the inertia of the thermal processes.

Keywords: infrared radiation, data protection, thermal camera, undeclared capabilities, provoking effect.

Doklady BGUIR. 2018, Vol. 116, No. 6, pp. 93-100
Stand for researching the dynamics of changing the thermal fields in the information and communication equipment at the evaluation of the data protection
A.I. Kukharenko, H.V. Davydau

Введение

Проведение исследований в области защиты информации необходимо для обеспечения безопасности критически важного оборудования и информационно-коммуникационной аппаратуры. Такие устройства представляют большой интерес для проведения атак на инфраструктуру и уязвимы к утечкам информации по физическим каналам ее передачи. Использование таких каналов может приводить к утечкам речевой информации, перехвату передаваемой информации, копированию цифровых файлов или утечке ключей шифрования. Более того, использование при атаках независимых физических каналов передачи данных позволяет избежать оставления следов в сетевой инфраструктуре, мониторинг которой может

раскрыть атакующего, а также преодолевать защитный периметр и получать информацию с компьютера, физически не подключенного к сети передачи данных. Поэтому проведение исследований и разработка методов обнаружения атак весьма актуальны в современном мире.

В данной работе описывается стенд, разработанный для проведения таких исследований. Ключевым отличием от стандартных методов обнаружения каналов утечки информации является применение метода наблюдения за тепловым излучением, исходящим от электронных компонентов печатной платы тестируемого устройства. Инфракрасное излучение от компонентов, попав в объектив тепловизионной камеры, в дальнейшем оцифровывается, и информация о нем фиксируется. Инфракрасное излучение, порожденное тепловыми колебаниями атомной решетки корпусов электронных компонентов устройства является маркером для выявления характерного поведения частей устройства. Любое оборудование, любая микросхема греются во время работы, так как они потребляют энергию, и переход этой энергии в тепло является естественным следствием выполненной работы.

Измерение тепловых полей радиоэлектронных компонентов, размещенных на печатной плате устройства, может быть использовано не только для поиска каналов утечки информации, но и для диагностики радиоэлектронной аппаратуры, поиска неисправностей, выявления некорректной работы компонентов или обнаружения потенциальных точек отказа и утечек информации в аппаратуре. Для обеспечения применимости в различных условиях и обеспечения точных измерений, при сборке стенда и во время его работы должны применяться методы по снижению влияния на термографическое изображение таких негативных факторов, как дрейфа температуры окружающей среды, рассеивающих или отражающих свойств поверхностей проверяемых объектов, высоких шумов инфракрасного изображения, а также инерционности тепловых процессов. Во время проведения апробации и исследований на стенде была выявлена необходимость снижения влияния негативных физических факторов на проводимые измерения [1].

Для уменьшения влияния паразитных факторов необходимо экранировать объект проверки и тепловизор от тепловых фоновых шумов. Эти шумы включают в себя тепловое излучение от экспериментатора, световое излучение, поступающее в помещение через окна, конвекционные тепловые потоки, излучение от самого тепловизора.

Для исключения влияния на результаты измерений инфракрасного излучения от экспериментатора или от людей, находящихся в комнате, необходимо тестируемое устройство и тепловизор размещать в отдельной комнате или за закрытой не пропускающей инфракрасное излучение ширмой. На результаты проверки вычислительной техники оказывают влияние вибрации испытуемого объекта и тепловизора, они приводят к смещению изображения объекта и усложнению цифровой обработки изображений. Негативное влияние могут оказывать конвекционные потоки и сквозняки, поэтому необходимо плотно закрывать двери и окна в комнате, где проводятся проверки. Многократно переотраженное световое и инфракрасное излучение, попадающее в комнату через окна, также негативно влияет на точность измерений. Окна в комнате, если они есть, должны быть зашторены. Тепловое излучение от самого тепловизора можно частично заблокировать с помощью однородного теплоизоляционного экрана, в котором проделано отверстие с диаметром, равным диаметру объектива. В таком случае от тестируемого устройства отражается только инфракрасное излучение от германиевой линзы объектива, не внося существенных помех в работу стенда.

Стенд для оценки защищенности информации

Оценка защищенности информации в тестируемых устройствах основана на поиске каналов утечек информации, выполненных аппаратно в виде недекларированных возможностей [2]. Недекларированными возможностями являются как функциональные возможности программного обеспечения, так и выполненные аппаратно возможности устройства, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Для обнаружения скрытых объектов съема и передачи информации используется термографический способ. Он основан на использовании последовательности термографических изображений и применением к ним методов

статистического анализа для выявления областей изображения, в которых произошло значимое изменение температуры. Одновременное использование при проверке тестовых устройств термографических измерений и факторов воздействия на проверяемое устройство позволяет увеличить вероятность обнаружения скрытых объектов съема и передачи информации и сократить время проверки.

К факторам воздействия на тестируемое устройство относятся провоцирующее воздействие и временной фактор. Провоцирующее воздействие представляет собой электромагнитное воздействие, создаваемое с помощью антенн и генератора электромагнитных сигналов. Временной фактор делится на кратковременный, заключающийся в воздействии на проверяемое устройство провоцирующим сигналом на протяжении интервала времени, необходимого для преодоления тепловой инерции, и долговременный, заключающийся в увеличении общего времени проверки устройства для повышения вероятности обнаружения периодически активизирующихся скрытых объектов съема и передачи информации.

Состав стенда

Для эффективной реализации принципа обнаружения недекларированных возможностей измерительное оборудование должно состоять из следующих элементов:

– тракта провоцирующих электромагнитных сигналов;

– тракта измерения ИК излучения;

– компьютера для управления с установленным программным обеспечением.

Схема стенда показана на рис. 1.

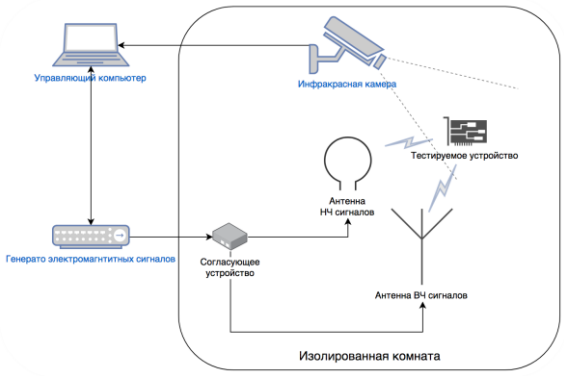

Рис. 1. Схема стенда для оценки защищенности информации

ство, антенну на диапазон частот от 10 до 30 МГц и антенну на диапазон от 30 до 3000 МГц.

В состав тракта провоцирующих электромагнитных сигналов входит несколько антенн, предназначенных для передачи на проверяемый объект провоцирующих электромагнитных сигналов в широком диапазоне частот от 10 МГц до 3 ГГц. Диапазон частот выбран так, чтобы перекрывать диапазоны частот большинства используемых для коммуникации протоколов связи. Для улучшения этой характеристики возможно расширение как нижней границы диапазона частот, так и верхней границы. Для перекрытия выбранного диапазона эффективно применять две антенны. На нижний диапазон частот от 10 до 30 МГц используется антенна Rohde&Schwarz HE300 Antenna Module 4067.6306.00, на верхний диапазон от 30 до 3000 МГц используется Rohde&Schwarz HE300 Antenna Module 4067.6458.00. Для подключения двух антенн к одному волновому тракту используется согласующее устройство. Разделение входных сигналов по частоте в нем выполняется за счет использования фильтра нижних и фильтра верхних частот с частотой среза 30 МГц. Применение двух антенн позволяет обеспечить линейную передаточную характеристику, менее сложную и дорогую конструкцию антенн по сравнению с одной широкополосной антенной, перекрывающей весь диапазон частот. Согласующее устройство подключается к антеннам и генератору электромагнитных сигналов с помощью радиочастотных коаксиальных кабелей, имеющих волновое сопротивление 50 Ом.

Генератор электромагнитных сигналов Keysight N5172B обеспечивает стабильную генерацию электромагнитных волн с возможностью регулировки несущей частоты в диапазоне от 10 МГц до 3 ГГц или шире и с возможностью выбора различных типов модуляций и манипуляций несущей частоты. Управление генератором электромагнитных сигналов может производиться как с панели прибора, так и с помощью подключения к компьютеру с установленным специальным программным обеспечением, производящим

ство, поступает через кабели в антенны и с их помощью излучается в пространство, тем самым воздействует на проверяемый объект.

Измерительный тракт включает в себя тепловизор FLIR Tau 2, регистрирующий излучение от проверяемого объекта. Регистрация тепловых полей электронных компонентов проверяемого объекта осуществляется с помощью неохлаждаемого тепловизора, работающего в длинноволновом инфракрасном диапазоне 8,5–13,5 мкм или шире, имеющего разрешение 640×480 пикселей, обеспечивающего чувствительность не хуже чем 50 мК. Тепловизор передает в реальном времени термографическое изображение на компьютер для дальнейшей обработки.

Измерение малых температурных колебаний электронных компонентов проверяемых устройств требует правильного подбора средств регистрации ИК излучения. Одним из важных параметров при выборе инфракрасной камеры является фокусное расстояние. Производители инфракрасных камер, подходящих для измерений, предоставляют широкий выбор оптики для них, и неверный выбор может существенно ограничить возможности стенда.

В публикации [3] был обоснован выбор фокусного расстояния тепловизора. Для измерения температурных колебаний компонентов современного электронного устройства необходимо иметь высокую пространственную разрешающую способность инфракрасной камеры. Под пространственной разрешающей способностью понимается линейный размер изображения, выраженный в миллиметрах, приходящийся на один пиксель камеры на минимальной дистанции фокусировки объектива. Такая точность необходима для контроля за электронными компонентами, имеющими малые размеры.

Резисторы поверхностного монтажа имеют широкий диапазон размеров. На сегодняшний день используются миниатюрные резисторы типоразмера SMD01005, имеющие размеры, близкие к 400 мкм в длину и 200 мкм в ширину.

На пространственную точность влияют количество пикселей тепловизора, минимальная дистанция фокусировки объектива, фокусное расстояние, поле зрения, разрешение на пиксель.

Для тепловизора FLIR Tau 2, имеющего размер пикселя 17 мкм и разрешение 640×512 пикселей, оптимальным выбором объектива с высоким разрешением и не вносящим искажения в изображение близко расположенного предмета оказался объектив с фокусным расстоянием, равным 19 мм. Выбор длиннофокусных объективов приводит к потере разрешающей способности камеры. Короткофокусные объективы хоть и имеют повышенную разрешающую способность, однако не подходят из-за малого расстояния до объекта измерения и связанных с этим искажений изображения. Искажения возникают по причине различной высоты электронных компонентов на печатной плате. Высокие компоненты, находящиеся ближе к объективу, имеют больший видимый размер и могут закрывать мелкие объекты, находящиеся рядом ниже.

Компьютер с помощью установленного на нем программного обеспечения выполняет управление генератором электромагнитных сигналов, принимает и обрабатывает термографические изображения с инфракрасной камеры, по результатам обработки этих данных помогает принять решение о защищенности информации в проверяемом устройстве.

Обработка поступающей с тепловизора информации

Влияние на термографическое изображение рассеивающих свойств поверхностей проверяемых объектов, дрейф температуры окружающей среды, высокие шумы изображения, а также различная инерционность процессов в каждом конкретном случае вынуждают

отказаться от измерения абсолютных значений температуры в каждой точке и перейти к статистической оценке термографических изображений. Применяется статистический анализ для определения характеристик шума термографического изображения и детектирования выхода значений температур за диапазон допустимых значений. Перед проверкой выполняется накопление и усреднение распределения теплового поля по проверяемому объекту, формируется базовое радиометрическое изображение путем нахождения среднего значения для каждого пикселя изображений. Далее ведется сравнение базового радиометрического изображения с текущим путем нахождения разности этих двух изображений для каждого пикселя. Эта разность сравнивается с пороговым значением. Когда текущее распределение теплового поля проверяемого объекта превышает пороговое значение, принимается решение о наличии изменений в режиме работы электронных компонентов, что автоматически фиксируется в результатах проверки с указанием режимов, при которых было обнаружено это изменение.

Обнаружение радиоприемных устройств в проверяемом объекте основано на приеме входным каскадом радиоприёмного устройства провоцирующего гармонического сигнала на частоте работы радиоприёмного устройства и усилении его до уровня, необходимого для дальнейшей обработки. При усилении радиоприёмным устройством провоцирующего гармонического сигнала температура его повышается, что может быть зафиксировано с помощью тепловизора и управляющего компьютера.

Обнаружение радиопередающих устройств основано на повышении температуры выходного каскада радиопередатчика при работе на передачу и ее фиксировании с помощью тепловизора и управляющего компьютера.

Если в проверяемый объект встроена недекларированная возможность в виде передатчика, то такие скрытые устройства обычно работают на передачу лишь короткое время в течение суток или другого отрезка времени, накапливая информацию для передачи. Поэтому целесообразно не прерывать проверку при смене провоцирующих воздействий и проводить ее более 24 ч.

С помощью генератора провоцирующих электромагнитных сигналов были сформированы радиосигналы с различными видами модуляции и протоколами связи:

– гармонический сигнал с развёрткой частоты по логарифмическому закону;

– гармонические сигналы с амплитудной, частотной, фазовой модуляцией;

– гармонический сигнал с квадратурной модуляцией;

– гармонический сигнал с амплитудной импульсной модуляцией одиночными импульсами с большой скважностью;

– гармонический сигнал с квадратурной манипуляцией;

– сигнал спутниковой системы IRIDIUM;

– сигналы мобильной связи GSM, UMTS (3G), CDMA;

– сигналы Bluetooth и Wi-Fi.

Такое разнообразие сигналов необходимо для увеличения вероятности провоцирующего воздействия на проверяемый объект. Сигналы включают в себя большинство распространенных в настоящее время протоколов связи, а также различные виды широкополосных сигналов.

Результаты апробации стенда

Для обнаружения малых изменений в работе электронного устройства с помощью инфракрасной камеры необходимо знать численные значения мощностей рассеяния на различных электронных компонентах, обнаруживаемых на данном стенде. Для этого была разработана специальная тестовая плата. Тестовая плата представляет собой модель проверяемого устройства, на которую, на каждый из компонентов, можно в контролируемых условиях подавать необходимую мощность, в реальном времени следить за нагревом электронных компонентов и проводить измерения температуры с помощью инфракрасной камеры.

Тестовая плата, изображенная на рис. 2, представляет собой двухстороннюю печатную плату с размерами 190×180 мм и толщиной текстолита 1,5 мм. На нее припаянны 10 образцов резисторов в разных корпусах, подключенных к источнику питания, подающего напряжение

независимо на каждый образец. Источник питания имеет возможность регулировки выходного напряжения. Плата жестко закреплена в массивном штативе для предотвращения смещения и вибраций во время измерений.

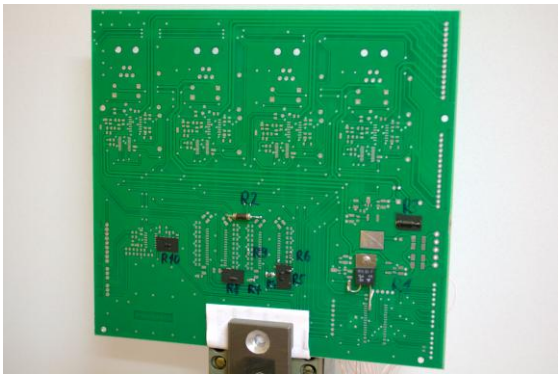

Рис. 2. Тестовая печатная плата

В стенде тепловизор FLIR Tau 2640, работающий в длинноволновом инфракрасном диапазоне 8–14 мкм, передает цифровые изображения через интерфейс CameraLink и через переходник подключен к персональному компьютеру. Инфракрасная камера закреплена на штативе, размещена на расстоянии 400 мм от тестовой платы и сфокусирована на нее.

Измерения [4] проводились с помощью штатного программного обеспечения тепловизора и заключались в определении минимального уровня мощности, подаваемой на образец в течение 1 с, при котором обнаруживалось изменение температуры. Самым заметным в ИК диапазоне оказался маломощный выводной резистор, обнаруживаемый при подаче на него мощности 0,0013 Вт. Для обнаружения SMD резистора размера 1206 понадобилась мощность от 0,0021 до 0,0030 Вт. Для обнаружения резистора в корпусе TO-220, имитирующего греющийся силовой транзистор, необходима была мощность 0,1707 Вт.

Замечена тенденция осложнения обнаружения нагрева SMD резисторов по мере уменьшения размеров корпусов, при этом наблюдаются отличия от расчетной мощности обнаружения. Это можно объяснить уменьшением количества пикселей, приходящихся на площадь резистора, а также иными коэффициентами термосопротивления к печатной плате. Разница между необходимой мощностью для обнаружения при разных теплоотводах составила 1,5 раза. В случае массивных корпусов замечена существенная тепловая инерционность.

Инерционность изменения температуры поверхности проверяемых объектов из-за изменений температуры кристаллов микросхем определяется теплопроводностью и теплоемкостью примененных материалов. Высокая теплопроводность кристаллического кремния внутри микросхемы, теплоотвод через припой, медные дорожки и слои заземления и питания на многослойных печатных платах существенно влияют на распределение температур на корпусах компонентов и вокруг их. Хороший теплоотвод на печатную плату сглаживает изменения температур исследуемых радиоэлектронных компонентов и вносит инерционность в получаемые радиометрические изображения. Изменение температур компонентов и печатной платы может составлять десятки градусов разницы между отключенным устройством и включенным, но эти изменения температуры долговременные и инерционные, занимают от нескольких минут до нескольких часов в зависимости от массы и теплоемкости устройства. Больший же интерес представляют не статические, инерционные изменения температур, а быстрые и динамические изменения температуры отдельных электронных компонентов. Такие изменения происходят за секунды, и могут составлять от менее чем 0,1 °С до нескольких градусов.

Были проведены исследования PCI-Express модуля с микросхемой, обеспечивающей связь по протоколу IEEE 802.11g (Wi-Fi). Производилось воздействие на компоненты провоцирующим электромагнитным сигналом. Результаты измерений показали, что температура части кремниевого кристалла, предположительно отвечающая за прием и передачу сигналов, поднималась при переключении от стационарного режима работы в режим поиска свободного от помех канала. Температура в первом случае составила 39,0 °С, во втором 39,3 ºС, зафиксировано увеличение температуры на 0,3 °С.

Заключение

В работе описан стенд для исследования распределения и динамики изменения тепловых полей в информационно-коммуникационной аппаратуре при оценке защищенности информации. Определены характеристики границы обнаружения минимального нагрева электронных компонентов и воздействия провоцирующего сигнала. Предложены мероприятия по снижению влияния на термографическое изображение рассеивающих свойств поверхностей проверяемых объектов, дрейфа температуры окружающей среды, высоких шумов изображения, а также инерционности тепловых процессов. Работа важна с точки зрения существующих в настоящее время потребностей в сфере защиты информации. Результаты исследования могут быть использованы для обеспечения защищенности информации в вычислительной технике, а также решения таких актуальных задач, как диагностика радиоэлектронной аппаратуры, поиск неисправностей, выявление некорректной работы компонентов в информационно-коммуникационной аппаратуре.

Список литературы

1. Давыдов Г.В., Кухаренко А.И. Снижение влияния внешнего излучения на измерения малых колебаний температуры с помощью тепловизора // Тез. докл. XV Бел.-рос. науч.-техн. конф. «Технические средства защиты информации». Минск, 6 июня 2017 г. С. 86.
2. Руководящий документ. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: утв. решением председателя Гос. техн. комиссии при Президенте Рос. Федерации от 4 июня 1999 г. № 114.
3. Давыдов Г.В., Кухаренко А.И. Влияние фокусного расстояния объектива тепловизора на способность измерять температуру малых объектов // Тез. докл. XV Бел.-рос. науч.-техн. конф. «Технические средства защиты информации». Минск, 6 июня 2017 г. С. 86–87.
4. Давыдов Г.В., Кухаренко А.И. Обнаружение рассеиваемой энергии электронными компонентами по их инфракрасному излучению // Материалы 10-й Междунар. науч.-техн. конф. «Новые направления развития приборостроения». Минск, 26–28 апреля 2017 г. С. 83–84.

References

1. Davydov G.V., Kuharenko A.I. Snizhenie vlijanija vneshnego izluchenija na izmerenija malyh kolebanij temperatury s pomoshh'ju teplovizora // Tez. dokl. XV Bel.-ros. nauch.-tehn. konf. «Tehnicheskie sredstva zashhity informacii». Minsk, 6 ijunja 2017 g. S. 86. (in Russ.)
2. Rukovodjashhij dokument. Zashhita ot nesankcionirovannogo dostupa k informacii. Ch. 1. Programmnoe obespechenie sredstv zashhity informacii. Klassifikacija po urovnju kontrolja otsutstvija nedeklarirovannyh vozmozhnostej: utv. resheniem predsedatelja Gos. tehn. komissii pri Prezidente Ros. Federacii ot 4 ijunja 1999 g. № 114. (in Russ.)
3. Davydov G.V., Kuharenko A.I. Vlijanie fokusnogo rasstojanija ob'ektiva teplovizora na sposobnost' izmerjat' temperaturu malyh ob'ektov // Tez. dokl. XV Bel.-ros. nauch.-tehn. konf. «Tehnicheskie sredstva zashhity informacii». Minsk, 6 ijunja 2017 g. S. 86–87. (in Russ.)
4. Davydov G.V., Kuharenko A.I. Obnaruzhenie rasseivaemoj jenergii jelektronnymi komponentami po ih infrakrasnomu izlucheniju // Materialy 10-j Mezhdunar. nauch.-tehn. konf. «Novye napravlenija razvitija priborostroenija». Minsk, 26–28 aprelja 2017 g. S. 83–84. (in Russ.)

Сведения об авторах

Кухаренко А.И., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Давыдов Г.В., к.т.н., доцент, заведующий НИЛ 5.3 НИЧ Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Kuharenko A.I., PG student of information security department of Belarusian state university of informatics and radioelectronics.

Davydau H.V., PhD, associate professor, head of SRL 5.3 of R&D department of Belarusian state university of informatics and radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6,
Белорусский государственный
университет информатики и радиоэлектроники
тел. +375-17-293-89-39;
e-mail: nil53@bsuir.edu.by
Давыдов Геннадий Владимирович

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian state university
of informatics and radioelectronics
тел. +375-17-293-89-39;
e-mail: nil53@bsuir.edu.by
Davydov Gennadij Vladimirovich