БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 3 (106). – 9–25

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УДК 621.391 DOI: 10.17212/2782-2230-2022-3-9-25

ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ АНАЛИЗАТОРОМ СПЕКТРА PROTEK 3201N ДЛЯ РЕШЕНИЯ ЗАДАЧ РАДИОМОНИТОРИНГА*

С.В. БЫКОВ[1], И.В. ИСАКОВ[2], Б.С. ШВЕНК[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: bykov_72@ngs.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: einbesserwisser@yandex.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: shcwenkbogdan@mail.ru*

Электроизмерительные приборы, относящиеся к анализаторам спектра, позволяют оперативно получать информацию о распределении энергии электрических и электромагнитных сигналов в определенной полосе частот. Диапазон частот сигналов, которые могут быть измерены анализаторами спектра, зависит от конкретной модели прибора. Расширение диапазона частот сигналов, измеряемых анализатором спектра, увеличивает его стоимость. Но в зависимости от алгоритма обработки сигналов, анализаторы спектра с одинаковым диапазоном частот также могут значительно различаться по стоимости. Рассматриваемый в настоящей статье анализатор спектра PROTEK 3201N стоит около 50 000 рублей при том что близкий по характеристикам анализатор спектра GW Instek GSP-7730 стоит около 150 000 рублей. Учитывая разброс цен, анализатор спектра PROTEK 3201N можно рассматривать как оптимальный вариант для реализации системы измерения параметров высокочастотных электрических и электромагнитных сигналов. Одной из областей применения данного оборудования является радиомониторинг в пределах контролируемой зоны. Под радиомониторингом понимается комплекс мероприятий по определению частоты и уровню электромагнитных сигналов и их идентификация. Суть идентификации состоит в определении принадлежности обнаруженных электромагнитных сигналов штатным радиопередающим устройством или устройством, осуществляющим несанкционированный доступ к информации из контролируемой зоны. Одним из возможных способов идентификации является детальный анализ формы спектра электромагнитного сигнала. Это может быть обеспечено изменением шага сканирования диапазона частот радио-

* Статья получена 09 июля 2022 г.

приемным устройством. Именно анализаторы спектра обладают максимально развитым функционалом изменения шага сканирования без изменения частотного диапазона, в котором производится радиомониторинг.

Ключевые слова: Анализатор спектра, интерфейс RS-232, кодировка ASCII, радиомикрофон, радиомониторинг, контролируемая зона, программно-аппаратный комплекс, набор команд

ВВЕДЕНИЕ

В настоящее время практически все электроизмерительные приборы имеют в своем составе интерфейсы для подключения к персональным компьютерам. Наличие такого функционала позволяет реализовать процесс измерения параметров сигнала более гибко и упростить процесс обработки, сохранения и отображения результатов измерений. Как правило, производитель оборудования в техническом описании приводит перечень команд, позволяющих производить конкретные операции по измерению параметров сигналов. При этом для каждой отдельной области применения электроизмерительных приборов характерно использование определенной группы команд из полного набора.

1. ПРЕДПОЛАГАЕМАЯ ОБЛАСТЬ ПРИМЕНЕНИЯ АНАЛИЗАТОРА СПЕКТРА PROTEK 3201N

Существующие анализаторы спектра могут решать широкий круг задач по определению параметров высокочастотных электрических и электромагнитных сигналов. Одной из актуальных задач является создание программно-аппаратных комплексов радиомониторинга. Такие комплексы предназначены для обнаружения и идентификации сигналов от радиомикрофонов. Под радиомикрофонами понимаются электронные устройства, скрытно устанавливаемые в помещениях и передающие акустическую информацию за пределы контролируемой зоны по радиоканалу. Радиомониторинг – это комплекс мероприятий по исследованию электромагнитных сигналов радиодиапазона в районе контролируемой зоны с целью определения их параметров (несущая частота, полоса рабочих частот, тип модуляции и т. п.) и идентификации как легальных радиопередающих устройств (точки доступа WiFi, связные радиостанции, базовые станции мобильной связи и т. п.) или радиомикрофонов. Одно из определений контролируемой зоны – это территория, на которой исключается несанкционированный доступ к элементам информационной системы посторонними лицами. Подобные комплексы в настоящее время выпускаются, но имеют высокую стоимость.

Например, анализатор спектра реального времени и мониторинговый приемник SpectrumJet 3.0 без персонального компьютера стоит от 963 000 рублей [1]. При этом данное оборудование может использоваться не только для проведения поисковых мероприятий на реальных объектах, но и для обучения студентов на специальностях, связанных с обеспечением информационной безопасности; в практике применения оборудования, обеспечивающего проведение операций радиомониторинга. В связи с этим на кафедре «Защита информации» НГТУ были начаты работы по разработке программно-аппаратного комплекса радиомониторинга. Выбор в качестве радиоприемного устройства анализатора спектра PROTEK 3201N обусловлен более низкой ценой по сравнению с аналогичным оборудованием, компактными размерами, высокой скоростью передачи данных по интерфейсу RS-232, возможностью организовать автономную работу за счет наличия встроенного отсека для электрических аккумуляторов [9]. Предполагалось, что при несколько худших характеристиках (диапазон рабочих частот, скорость анализа выбранного диапазона частот) стоимость будет значительно ниже. Кроме того, предполагалось реализовать возможность демонстрации особенностей работы комплексов радиомониторинга разного типа и большинства возможных алгоритмов идентификации обнаруженных электромагнитных сигналов.

По типам комплексы радиомониторинга подразделяются [2, 3, 4]:

– на комплексы пошагового анализа;

– комплексы с анализом интегрального уровня сигнала в полосе промежуточной частоты радиоприемного устройства;

– комплексы с цифровой обработкой сигнала в полосе промежуточной частоты радиоприемного устройства.

Самые простые и дешевые – комплексы пошагового анализа. При проведении радиомониторинга компьютер перестраивает сканирующий приемник в заданном диапазоне с установленным оператором шагом. Если на какой-либо частоте уровень сигнала превышает пороговый, проверяется принадлежность радиосигнала в соответствии с настройками комплекса. Главный недостаток программно-аппаратных комплексов этого типа – большое время, необходимое для проверки. Например, для проверки диапазона частот 40...2000 МГц с акустическим зондированием необходимо от 40 мин до 1,5 ч. Комплексы радиомониторинга, относящиеся ко второй группе, осуществляют проверку интегрального уровня сигналов в полосе промежуточной частоты (ПЧ) [8] приемника (рис. 1). Для реализации подобного алгоритма необходимы сканирующие приемники с выходом ПЧ (или доработанные). При проведении радиомониторинга сканирующий приемник перестраивается с шагом, равным полосе ПЧ. В каждом шаге производится детектирование уровня сигна-

лов. Если, как показано на рис. 1, *а*, интегральный уровень сигналов ниже порогового, комплекс перестраивается дальше. Если интегральный уровень сигнала выше порогового (рис. 1, *б*), комплекс перестраивает приемник в пределах полосы ПЧ с меньшим шагом для точного определения значений частот. При настройке на каждую частоту в пределах полосы ПЧ, уровень которой превышает пороговый, также производится проверка принадлежности радиосигнала в соответствии с настройками комплекса. Использование данного способа значительно уменьшает время радиомониторинга до 10...20 мин.

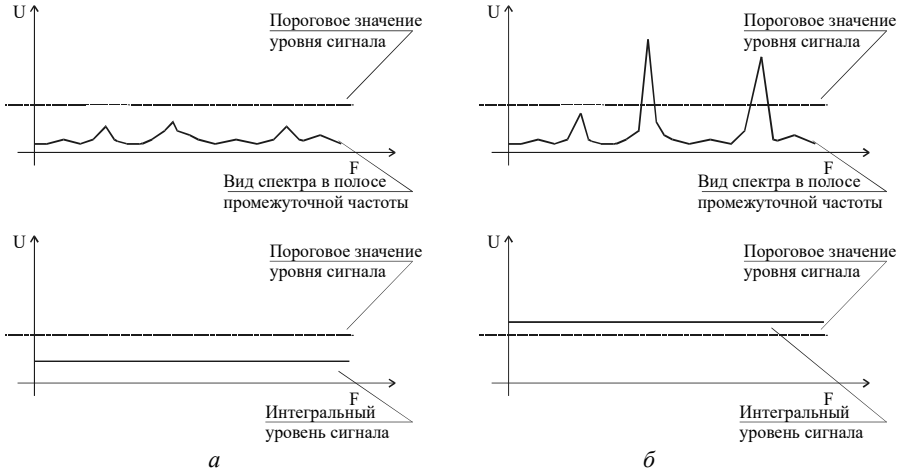


Рис. 1. Особенности работы комплексов радиомониторинга с анализом интегрального уровня в полосе промежуточной частоты

Fig. 1. Features of the operation of radio monitoring complexes with the analysis of the integral level in the intermediate frequency band

Комплексы радиомониторинга третьей группы имеют еще меньшее время сканирования. Это достигается цифровой обработкой сигналов. Сканирующий приемник также перестраивается с шагом, равным полосе ПЧ. При превышении интегральным уровнем сигнала порогового значения производится последующая обработка (например, операция быстрого преобразования Фурье – БПФ). Время, необходимое на проведение БПФ, меньше, чем время, необходимое для проверки полосы ПЧ с меньшим шагом, как в комплексах, относящихся ко второй группе.

В качестве алгоритмов идентификации обнаруженных электромагнитных сигналов могут использоваться [2–4]:

- акустический тест;
- наличие сигналов на частотах, соответствующих 2-й и 3-й гармоникам проверяемого сигнала;
- появление новой частоты, не зарегистрированной ранее.

Суть применяемых методов в следующем. При проведении *акустического теста* комплекс при помощи акустических колонок формирует акустические сигналы с заранее известными параметрами. Если сканирующий приемник настроен на частоту радиомикрофона, то в демодулированном сигнале будут присутствовать сигналы, близкие по параметрам (форме сигнала во времени). После сравнения формы демодулированных сигналов с формируемой формой сигнала во времени вычисляется коэффициент корреляции при разных типах демодуляторов (WFM, NFM). Определяя задержку распространения акустического сигнала от колонок до радиомикрофона, можно оценить расстояние до него. Недостаток данного метода в том, что происходит демаскирование факта проведения радиомониторинга и радиомикрофоны с дистанционным управлением могут быть выключены. Радиомикрофоны, используемые для несанкционированного доступа к информации (НСД), как правило, прячут в предметах интерьера. При этом акустический путь тестового сигнала от колонок до радиомикрофона может сильно отличаться от геометрического. В связи с этим расстояние до радиомикрофона будет измерено неверно.

Полупроводниковые элементы, используемые для генерации и усиления радиосигналов, являются нелинейными элементами. В связи с этим происходит искажение формы синусоидального сигнала, используемого в качестве несущей частоты радиомикрофона [7]. Таким образом, в эфир помимо основного сигнала будут *излучаться сигналы на 2-й, 3-й и т. д. гармониках*. В штатных устройствах, передающих данные по радиоканалу (вещательные станции, телевизионные передатчики и т. п.), принимаются специальные меры по подавлению кратных гармоник. Но применять эти меры в радиомикрофонах затруднительно, так как резко увеличиваются габаритные размеры радиомикрофонов, что усложняет их маскирование в предметах интерьера. При проверке радиосигнала по данному признаку компьютер поискового комплекса перестраивает сканирующий приемник на частоты, равные удвоенному и утроенному значению несущей. На данных частотах производится оценка уровня сигнала. Если он выше некоторого порогового значения, принимается решение о принадлежности данного сигнала устройству НСД к информации. При использовании данного метода факт проведения радиомониторинга не демаскируется. Но с учетом наличия в эфире большого числа радио-

сигналов очень высока вероятность, что на частотах, равных удвоенной и утроенной частоте проверяемого сигнала, окажутся сигналы от посторонних передатчиков.

Для эффективной проверки принадлежности обнаруженного сигнала для радиомикрофона по факту *появления нового сигнала* нужно создать образец, с которым будет происходить сравнение. В комплексах радиомониторинга этот образец называется файлом панорамы или файлом образца. Для создания файла панорамы (файла образца) необходимо запустить комплекс на анализ радиообстановки и проводить анализ в течение нескольких циклов. При регистрации данных в файле панорамы используется несколько методов обработки: обновление, усреднение, накопление. При обновлении в каждом цикле проверки часто́ты записываются заново. При усреднении и накоплении учитываются данные от прежних циклов проверки. При использовании усреднения записывается среднее арифметическое из принятого и ранее сохраненного. При накоплении в файл панорамы записывается большее из значений. Чаще всего используют усреднение. После завершения работы комплекса полученные данные сохраняются. При дальнейших проверках обнаруженные в эфире сигналы сравниваются по частоте и уровню с сохраненными в панораме. Если значения не отличаются или отличаются незначительно (15...20 %), этот сигнал комплекс пропускает. В результате комплекс регистрирует относительно небольшое количество новых сигналов (от 20 до 60), которые в последующем можно проверить на слух либо можно применить один из существующих методов проверки, упомянутый выше. При работе комплекса в таком режиме не происходит демаскирования факта проведения радиомониторинга, значительно сокращается время проверки. Недостатком является то, что оператор вручную определяет принадлежность сигнала устройству НСД к информации или постороннему радиопередатчику [10].

Обобщенная блок-схема разрабатываемого программно-аппаратного комплекса радиомониторинга показана на рис. 2. Так как на современных персональных компьютерах интерфейс RS-232 (COM-порт) отсутствует, будет использоваться переходник USB-to-COM. Под управляющим контроллером подразумевается устройство на основе микроконтроллера, которое будет производить дополнительную обработку сигналов для реализации различных алгоритмов идентификации обнаруженных электромагнитных сигналов. Примером реализации дополнительного алгоритма идентификации сигналов является использование акустического теста с формированием в проверяемом помещении акустических сигналов с известными параметрами. В качестве дополнительных сигналов могут использоваться демодулированный сигнал

частоты, на которую настроен анализатор спектра, сигнал полосы промежуточной частоты после первого смесителя в схеме анализатора спектра и т. п. (предполагалось уточнить в процессе разработки комплекса).

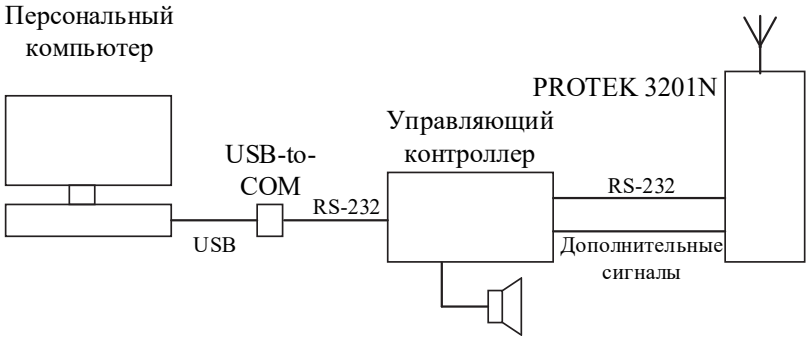


Рис. 2. Обобщенная блок-схема программно-аппаратного комплекса радиомониторига на основе анализатора спектра PROTEK 3201N

Fig. 2. Generalized block diagram of the software and hardware complex of radio monitoring based on the spectrum analyzer PROTEK 3201N

Также в процессе разработки комплекса предполагалось уточнить конкретную модель микроконтроллера, которая будет использоваться для создания управляющего контроллера.

2. ЗАЯВЛЯЕМАЯ ПРОИЗВОДИТЕЛЕМ ТЕХНОЛОГИЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ АНАЛИЗАТОРОМ СПЕКТРА PROTEK 3201N

Особенностью анализатора спектра PROTEK 3201N является то, что набор органов управления отличается от реализованного на большинстве анализаторов спектра, что нужно учитывать при проведении работ по определению параметров электромагнитных сигналов. На рис. 3 показан внешний вид панели управления анализатора спектра PROTEK 3201N.

Описание процесса дистанционного управления анализатором спектра приведено в отдельном документе, поставляемом производителем совместно с оборудованием [5]. Перечень команд, позволяющих реализовать дистанционное управление прибором, приведен в таблице работы [5].

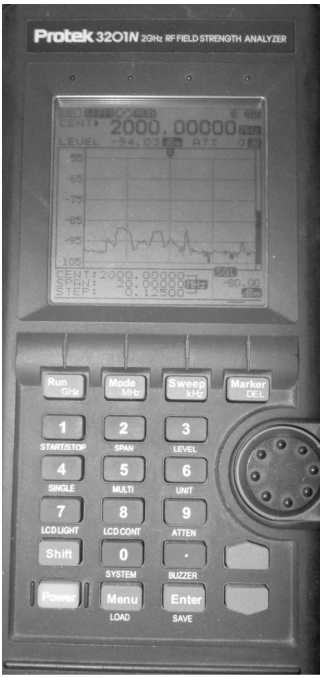


Рис. 3. Внешний вид панели управления анализатора спектра PROTEK 3201N

Fig. 3. Appearance of the control panel of the PROTEK 3201N spectrum analyzer

Перечень команд дистанционного управления анализатором спектра PROTEK 3201N

Команда	ASCII код
«Run/GHz»	X
«Mode/MHz»	T
«Sweep/kHz»	Z
«Marker/DEL»	S
«1»	R
«2»	U
«3»	V
«4»	O
«5»	P
«6»	Q
«7»	K
«8»	L
«9»	M
«0»	H
«Shift»	G
«.»	I
«Menu»	B
«Enter»	D
«Up»	J
«Down»	E
«OK Response»	OK@
«Fail Respounse»	FA@

Для связи анализатора спектра с персональным компьютером используются интерфейс RS-232. Формат обмена данными происходит в соответствии с таблицей кодировки ASCII [6]. Как видно из информации, показанной на рис. 3, в процессе дистанционного управления персональный компьютер должен посылать данные, имитирующие нажатие определенных комбинаций кнопок на панели анализатора спектра. Несмотря на то что в настоящее время в большинстве персональных компьютеров данный интерфейс отсутствует, процесс передачи данных легко реализовать за счет использования переходников USB-to-COM [11]. Вместе с оборудованием производитель поставляет программное обеспечение, которое позво-

ляет реализовать процесс управления анализатором спектра с персонального компьютера. Внешний вид интерфейса данного программного обеспечения показан на рис. 4.

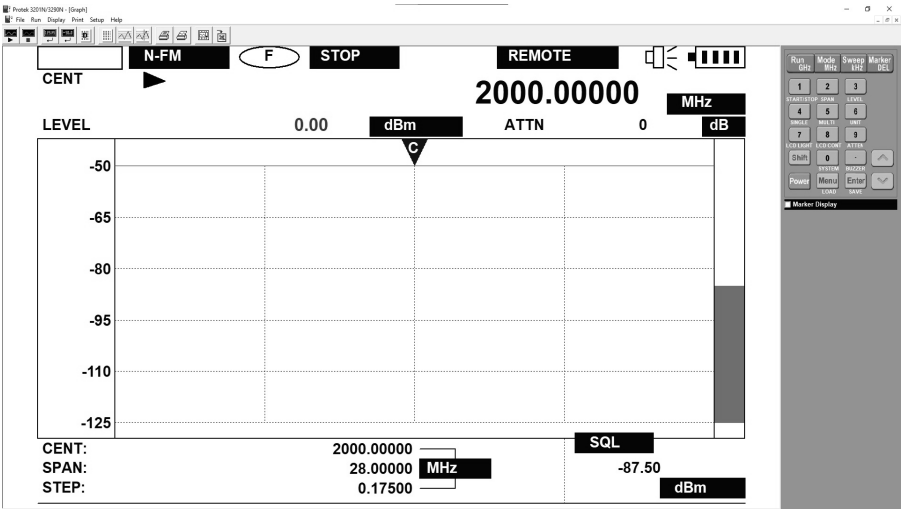


Рис. 4. Вид интерфейса базового программного обеспечения для дистанционного управления анализатором спектра PROTEK 3201N с персонального компьютера

Fig. 4. Interface view of the basic software for remote control of the PROTEK 3201N spectrum analyzer from a personal computer

При попытках реализовать дистанционное управление анализатором спектра было выявлено, что не все заявленные команды работают корректно. Для определения возможностей полноценного дистанционного управления анализатором спектра PROTEK 3201N были проведены дополнительные исследования, суть которых и их результаты будут описаны далее.

2. ВЫЯВЛЕННЫЕ ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ АНАЛИЗАТОРОМ СПЕКТРА PROTEK 3201N

2.1. ОРГАНИЗАЦИЯ ПРОЦЕССА ПЕРЕДАЧИ ДАННЫХ

Для анализа отправленных команд и ответов устройства использовалась программа «Device monitoring studio».

Описание процесса отслеживания отправленных команд:

1) подключение устройства к компьютеру через переходник USB-to-COM;

2) запуск поставляемого с устройством ПО «PROTEK 3201N GUI Program»;

3) запуск программы для анализа «Device monitoring studio»;

4) конфигурация программы для анализа и запуск сканирования.

Для конфигурации программы нужно выбрать COM-порт, к которому подключено устройство, а также режим отображения данных;

5) тестирование ПО, поставляемого с устройством, отправка различных команд и анализ ответов устройства.

При использовании ПО «PROTEK 3201N GUI Program» необходимо учесть следующие особенности устройства:

1) полоса частот должна быть 1…200 МГц;

2) максимальная частота 2000 МГц;

3) невозможно выставить значение шага сканирования, он подстраивается устройством автоматически.

На этапе сканирования было выявлено, что ПО отправляет команды, не указанные в документации, например: команда начальной инициализации прибора (GUI@), команда остановки сканирования (AX), команда отправки данных с устройства (A) и другие. В свою очередь, указанные в документации команды работают корректно.

2.2. ОСОБЕННОСТИ ОТОБРАЖЕНИЯ РЕЗУЛЬТАТОВ ИЗМЕРЕНИЙ

В ответ на команду «передать данные» соответствующей комбинации символов AX устройство отправляет 181 числовое значение: первые 17 значений – конфигурационные. Начиная с 18-го значения устройство отправляет информацию об уровнях сигнала на определенной частоте, при этом всегда передает фиксированное количество значений (161), тогда как часто́ты, соответствующие значениям уровня, не передаются вместе со значениями, их необходимо высчитать самостоятельно, опираясь на значения частот, переданных устройству. Вид отображаемых данных по результатам сканирования

показан на рис. 5. Информация об уровнях сигнала измеряется в дБм. При этом по умолчанию предполагается, что значения уровня имеют отрицательный знак и перед последними двумя цифрами должна стоять запятая. То есть передаваемое значение «9770» обозначает, что уровень сигнала на данной частоте –97,70 дБм. Определение конкретного значения частоты производится по следующему алгоритму:

- определяется шаг изменения частоты по принципу: конечное значение диапазона сканирования минус начальное значение диапазона сканирования разделить на 160;
- для определения конкретного значения частоты значение шага частоты умножается на порядковый номер уровня и полученное значение прибавляется к начальному значению частоты диапазона сканирования.

```
2,1,0,1,1,1,  42000000,   4000000,  4,120, 50, -55, 10,0,    0,    0,    0,
9305, 9255, 9145, 9080, 9030, 9220, 9180, 9155, 9160, 9270, 9250, 9524,
9220, 9215, 9220, 9300, 9357, 9752, 9770, 9523, 9770, 9688, 9764, 9576,
9747, 9764, 9700, 9747, 9782, 9764, 9576, 9357, 9611, 9190, 9255, 9130,
9185, 9270, 9305, 9195, 9180, 9215, 9170, 9200, 9385, 9305, 9205, 9310,
9125, 8956, 9135, 9065, 9030, 8993, 9220, 9150, 8956, 8825, 8781, 8775,
8831, 9055, 9045, 9110, 9240, 9235, 9095, 9080, 9305, 9215, 9185, 9335,
9215, 9110, 9025, 8875, 8737, 8570, 8333, 8015, 7590, 7050, 6500, 5750,
5485, 5485, 5486, 5484, 5480, 5476, 5478, 5483, 5485, 5486, 5485, 5487,
5493, 5525, 5700, 5750, 5900, 6733, 7640, 8375, 8868, 9030, 9145, 9090,
9030, 9145, 8881, 8906, 8725, 8925, 8912, 8925, 9050, 9110, 9050, 9080,
9005, 9030, 9185, 9175, 9090, 9120, 9215, 9105, 9135, 9275, 9320, 9140,
9270, 9300, 9185, 9140, 9355, 9205, 9160, 9190, 9325, 9385, 9245, 9350,
9340, 9185, 9165, 9235, 9365, 9090, 9066, 9115, 9190, 9130, 9435, 9270,
9066, 9100, 9180, 9240, 9330,0,1101,0,
```

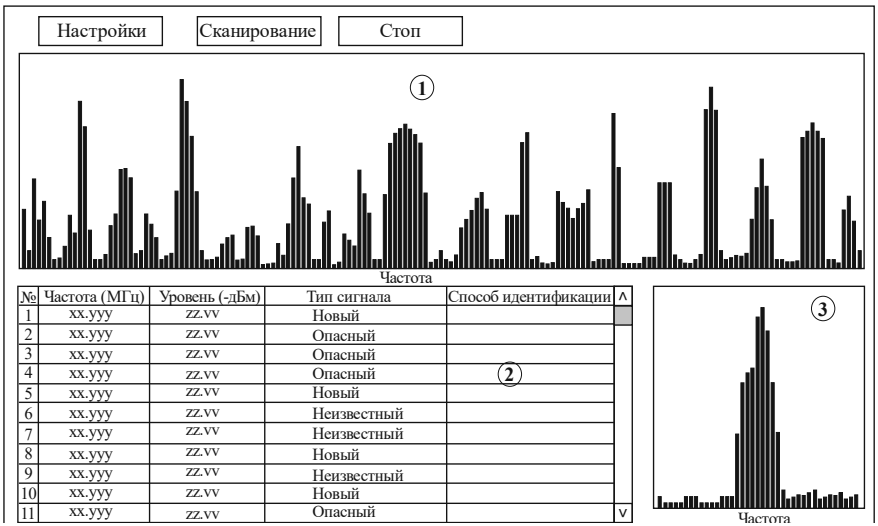
Рис. 5. Вид отображаемых данных по результатам сканирования

Fig. 5. View of the displayed data based on the scan results

Для проверки полученной информации была написана отладочная программа на языке программирования Python с использованием библиотеки PySerial [13]. Исходя из полученных экспериментальных данных можно сделать предварительный вывод, что использование анализатора спектра PROTEK 3201N позволяет создать комплекс радиомониторинга, относящегося к типу с анализом интегрального уровня в полосе ПЧ без доработки анализатора спектра и создания дополнительного управляющего контроллера.

2.3. ПРЕДПОЛАГАЕМЫЙ ФУНКЦИОНАЛ И АЛГОРИТМ РАБОТЫ ПРОГРАММНОГО ОБЕПЕЧЕНИЯ

На рис 6. показан предполагаемый вид отображения результатов работы программно-аппаратного комплекса радиомониторинга на основе анализатора спектра PROTEK 3201N. В управляющей программе предполагается наличие трех кнопок управления: «Настройки», «Сканирование», «Стоп».



№	Частота (МГц)	Уровень (-дБм)	Тип сигнала	Способ идентификации
1	xx.yyy	zz.vv	Новый	
2	xx.yyy	zz.vv	Опасный	
3	xx.yyy	zz.vv	Опасный	
4	xx.yyy	zz.vv	Опасный	
5	xx.yyy	zz.vv	Новый	
6	xx.yyy	zz.vv	Неизвестный	
7	xx.yyy	zz.vv	Неизвестный	
8	xx.yyy	zz.vv	Новый	
9	xx.yyy	zz.vv	Неизвестный	
10	xx.yyy	zz.vv	Новый	
11	xx.yyy	zz.vv	Опасный	

Рис. 6. Предполагаемый вид отображения результатов сканирования программного аппаратного комплекса на основе анализатора спектра PROTEK 3201N

Fig. 6. The intended type of display of scanning results of the software hardware complex based on the spectrum analyzer PROTEK 3201N

В области «1» отображается результат сканирования с индикацией уровня сигнала на определенной частоте. В области «2» показаны параметры обнаруженных сигналов с указанием в текстовой форме частоты, уровня и типа сигнала. В области «3» предполагается отображать более подробный вид спектра конкретного сигнала из обозначенного в областях «1» и «2». Активация кнопки «Настройки» вызывает появление дополнительного окна, где указываются значения начала и конца диапазона частот сканирования; уровень сигнала, выше которого сигнал считается отличным от фоновых значений; способ идентификации обнаруженных сигналов. Активация кнопки «Сканирование» приводит к началу работы по проверке сигналов в диапазоне частот,

указанных при активации кнопки «Настройка». Активация кнопки «Стоп» приводит к остановке процесса проверки диапазона частот. По результатам проверки возможен более детальный анализ обнаруженных сигналов. В частности, при двойном щелчке манипулятора «мышь» на сигналах в областях «1» и «2» анализатор спектра настраивается на данную частоту (что позволяет прослушать демодулированный сигнал) и в области «3» отображается более подробный вид спектра данного сигнала. Параметры сканирования участка диапазона частот для получения информации о более подробном виде спектра проверяемого сигнала предполагается получить в результате выполнения работ по созданию комплекса радиомониторинга.

Программную основу для комплекса предполагается реализовать на языке Python, интерфейс – на языке библиотеки Tkinter и PyQt5, отправку-получение команд – на языке PySerial. [12, 14, 15]

ЗАКЛЮЧЕНИЕ

В результате проведенных исследований были получены комбинации сигналов, позволяющие реализовать процесс дистанционного управления анализатором спектра PROTEK 3201N в полной мере. Существующие команды управления позволяют создать полноценный программно-аппаратный комплекс радиомониторинга на основе анализатора спектра PROTEK 3201N.

СПИСОК ЛИТЕРАТУРЫ

1. Прайс-лист компании «Радиосервис» – URL: https://radioservice.ru/price/ (дата обращения: 26.08.2022).

2. *Быков С.В.* Исследование возможностей и особенностей применения программно-аппаратного комплекса радиомониторинга RS-turbo: методическое пособие к лабораторному практикуму. – Новосибирск: Изд-во НГТУ, 2007. – 25 с.

3. *Каргашин В.Л.* Проблемы обнаружения и идентификации радиосигналов средств негласного контроля информации // Специальная техника. – 2000. – № 3; 4; 5.

4. *Хорев А.А.* Комплексы радиоконтроля для выявления электронных устройств перехвата информации // Специальная техника. – 2003. – № 1.

5. GUI Software Guide Protek 3200. – URL: https://guidessimo.com/document/1232768/gsi-protek-3200-series-operation-user-s-manual-82.html (accessed: 31.08.2022).

6. *Хаммел Р.Л.* Последовательная передача данных: руководство для программиста: пер. с англ. – М.: Мир, 1996. – 752 с.

7. *Соболев А.Н., Кириллов В.М.* Физические основы технических средств обеспечения безопасности. – М.: Гелиос АРВ, 2004. – 224 с.

8. Радиоприемные устройства / под. ред. А.П. Жуковского. – М.: Высшая школа, 1989. – 342 с.

9. Приобретение базовых навыков определения параметров высокочастотных электрических и электромагнитных сигналов / С.В. Быков, И.А. Ершов, И.Л. Рева, Е.А. Теличко. – Новосибирск: Изд-во НГТУ, 2020. – 91 с.

10. *Каторин Ю.Ф., Разумовский А.В., Спивак А.И.* Защита информации техническими средствами. – СПб.: НИУ ИТМО, 2012. – 416 с.

11. *Магда Ю.С.* Программирование последовательных интерфейсов. – СПб.: БХВ-Петербург, 2009. – 304 с.

12. *Быков В.И.* Система ввода-вывода ЭВМ и ВС и ее интерфейсы. – Владимир: Изд-во ВлГУ, 2015. – 230 с.

13. *Буйначев С.К., Боклаг Н.Ю.* Основы программирования на языке Python. – Екатеринбург: Изд-во Урал. ун-та, 2014. – 92 с.

14. *Сергеев С.Ф., Падерно П.И., Назаренко Н.А.* Введение в проектирование интеллектуальных интерфейсов. – СПб.: НИУ ИТМО, 2011. – 108 с.

15. *Прохоренок Н.А*., *Дронов В.А.* Python 3 и PyQt 5. Разработка приложений. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2018. – 832 с.

Быков Сергей Владимирович, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – измерение параметров электромагнитных сигналов в реальном масштабе времени, цифровая обработка сигналов. E-mail: bykov_72@ngs.ru

Исаков Игорь Владимирович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – цифровая схемотехника, микроконтроллеры, машинное обучение. E-mail: einbesserwisser@yandex.ru

Швенк Богдан Сергеевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – компьютерные сети и UNIX-подобные ОС. E-mail: schwenkbogdan@mail.ru

DOI: 10.17212/2782-2230-2022-3-9-25

Remote control of the PROTEK 3201N spectrum analyzer to solve radiomonitoring tasks*

S.V. Bykov[1], I.V. Isakov[2], B.S. Shwenk[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the Department of Information Security. E-mail: bykov_72@ngs.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: einbesserwisser@yandex.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: shcwenkbogdan@mail.ru*

Electrical measuring instruments related to spectrum analyzers allow you to quickly obtain information about the distribution of energy of electrical and electromagnetic signals in a certain frequency band. The range of signal frequencies that can be measured by spectrum analyzers depends on the specific instrument model. Extending the signal frequency range measured by the spectrum analyzer increases its cost. But depending on the signal processing algorithm, spectrum analyzers with the same frequency range can also vary significantly in cost. The PROTEK3201N spectrum analyzer considered in this article costs around 50,000 rubles, while the similar GW Instek GSP-7730 spectrum analyzer costs about 150,000 rubles. Given the range of prices, the PROTEK3201N spectrum analyzer can be considered as the best option for implementing a system for measuring the parameters of high-frequency electrical and electromagnetic signals. One of the areas of application of this equipment is radio monitoring within the controlled area. Radio monitoring is understood as a set of measures to determine the frequency and level of electromagnetic signals, and their identification. The essence of identification is to determine whether the detected electromagnetic signals belong to a regular radio transmitter or a device that performs unauthorized removal of information from a controlled area. One of the possible identification methods is a detailed analysis of the electromagnetic signal spectrum shape. This can be achieved by changing the scanning step of the frequency range by the radio receiver. It is spectrum analyzers that have the most developed functionality for changing the scanning step without changing the frequency range in which radio monitoring is performed.

Keywords: Spectrum analyzer, RS-232 interface, ASCII encoding, radio microphone, radio monitoring, controlled area, software and hardware system, command set

REFERENCES

1. Prais-list kompanii «Radioservis» [Price list of the "Radioservice" company]. Available at: https://radioservice.ru/price/ (accessed 26.08.2022).

* *Received 09 July 2022.*

2. Bykov S.V. *Issledovanie vozmozhnostei i osobennostei primeneniya programmno-apparatnogo kompleksa radiomonitoringa RS-turbo* [Study of the possibilities and features of using the hardware-software complex of radio monitoring "RS-turbo"]. Novosibirsk, NSTU Publ., 2007. 25 p.

3. Kargashin V.L. Problemy obnaruzheniya i identifikatsii radiosignalov sredstv neglasnogo kontrolya informatsii [Problems of detection and identification of radio signals of means of covert control of information]. *Spetsial'naya tekhnika = Special Equipment*, 2000, no. 3, 4, 5.

4. Khorev A.A. Kompleksy radiokontrolya dlya vyyavleniya elektronnykh ustroistv perekhvata informatsii [Radio monitoring systems for detecting electronic devices for intercepting information]. *Spetsial'naya tekhnika = Special Equipment*, 2003, no. 1.

5. *GUI Software Guide Protek 3200*. Available at: https://guidessimo.com/document/1232768/gsi-protek-3200-series-operation-user-s-manual-82.html (accessed 31.08.2022).

6. Hummel R.L. *Programmer`s technical reference: data and fax communications*. Emeryville, CA, Ziff-Devis Press, 1993 (Russ. ed.: Khammel R.L. *Posledovatel'naya peredacha dannykh: rukovodstvo dlya programmista*. Moscow, Mir Publ., 1996. 752 p.).

7. Sobolev A.N., Kirillov V.M. *Fizicheskie osnovy tekhnicheskikh sredstv obespecheniya bezopasnosti* [The physical basis of security engineering]. Moscow, Gelios ARV Publ., 2004. 224 p.

8. Zhukovskii A.P., ed. *Radiopriemnye ustroistva* [Radio receivers]. Moscow, Vysshaya shkola Publ., 1989. 342 p.

9. Bykov S.V., Ershov I.A., Reva I.L., Telichko E.A. *Priobretenie bazovykh navykov opredeleniya parametrov vysokochastotnykh elek-tricheskikh i elektromagnitnykh signalov* [Acquisition of basic skills in determining the parameters of high-frequency electrical and electromagnetic signals]. Novosibirsk, NSTU Publ., 2020. 91 p.

10. Katorin Yu.F., Razumovskii A.V., Spivak A.I. *Zashchita informatsii tekhnicheskimi sredstvami* [Protection of informatics by technical means]. St. Petersburg, NRU ITMO Publ., 2012. 416 p.

11. Magda Yu.S. *Programmirovanie posledovatel'nykh interfeisov* [Programming serial interfaces]. St. Petersburg, BHV Publ., 2009. 304 p.

12. Bykov V.I. *Sistema vvoda-vyvoda EVM i VS i ee interfeisy* [Input-output system of electronic computers and computer systems and its interfaces]. Vladimir, VlSU Publ., 2015. 230 p.

13. Buinachev S.K., Boklag N.Yu. *Osnovy programmirovaniya na yazyke Python* [Fundamentals of Python programming]. Ekaterinburg, URFU Publ., 2014. 92 p.

14. Sergeev S.F., Paderno P.I., Nazarenko N.A. *Vvedenie v proektirovanie intel-lektual'nykh interfeisov* [Introduction to intelligent interface design]. St. Petersburg, NRU ITMO Publ., 2011. 108 p.

15. Prokhorenok N.A., Dronov V.A. *Python 3 i PyQt 5. Razrabotka prilozhenii* [Python 3 and PyQt 5. Application вevelopment]. St. Petersburg, BHV Publ., 2018. 832 p.

Для цитирования:

Быков С.В., Исаков И.В., Швенк Б.С. Дистанционное управление анализатором спектра PROTEK 3201N для решения задач радиомониторинга // Безопасность цифровых технологий. – 2022. – № 3 (106). – С. 9–25. – DOI: 10.17212/2782-2230-2022-3-9-25.

For citation:

Bykov S.V., Isakov I.V., Shwenk B.S. Distantsionnoe upravlenie analizatorom spektra PROTEK 3201N dlya resheniya zadach radiomonitoringa [Remote control of the PROTEK 3201N spectrum analyzer to solve radiomonitoring tasks. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 3 (106), pp. 9–25. DOI: 10.17212/2782-2230-2022-3-9-25.