

ДОСТОВЕРНЫЙ КОНТРОЛЬ ЗАЩИЩЕННОСТИ КВАНТОВАННОГО И ВОССТАНОВЛЕННОГО РЕЧЕВОГО СИГНАЛА

М.М.БАРАНОВСКИЙ

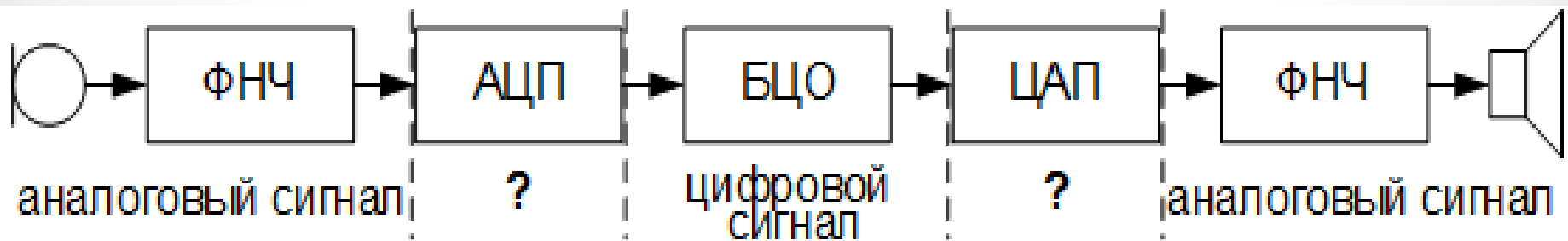
(Оперативно-аналитический центр при Президенте Республики Беларусь)

В.К.ЖЕЛЕЗНЯК

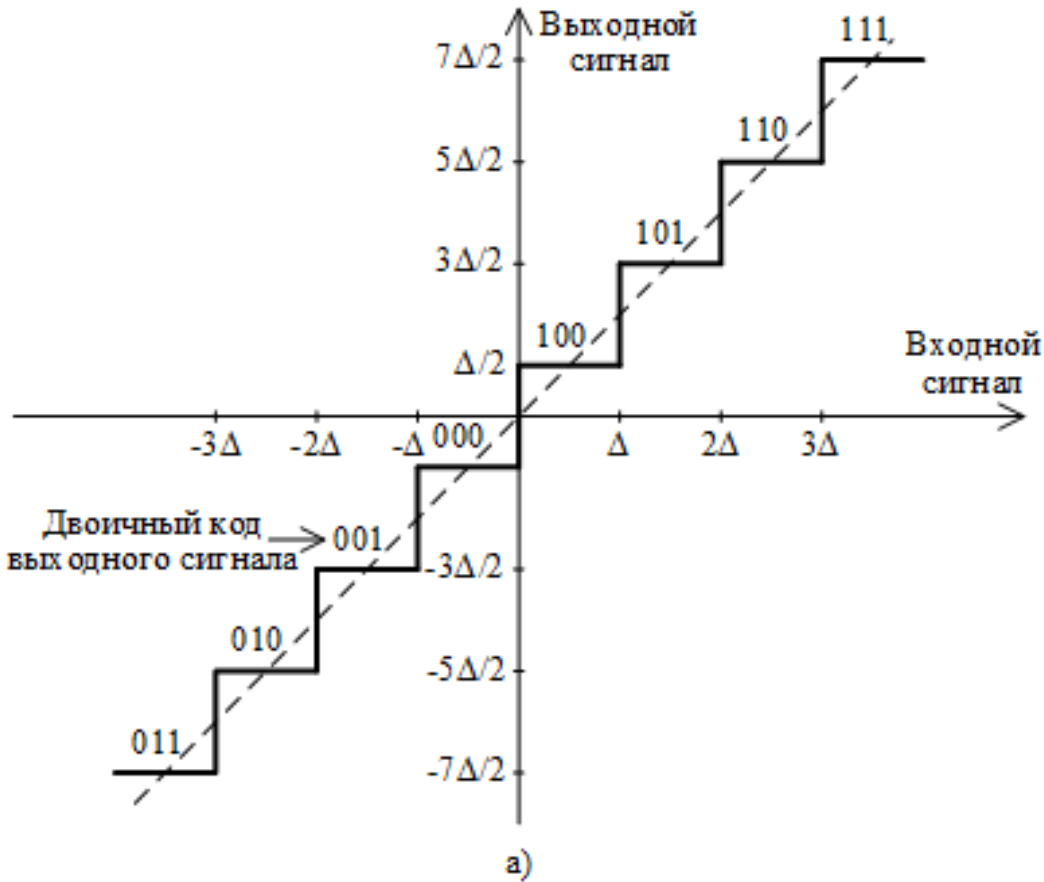
(Учреждение образования «Полоцкий государственный университет»)

ВВЕДЕНИЕ

Используемые в настоящее время подходы к оценке защищенности каналов утечки речевых сигналов при их преобразовании в цифровую форму сводятся к отдельной оценке аналогово речевого сигнала и речевого сигнала, представленного в цифровой форме при его передаче по линиям связи. В качестве измерительного сигнала используют, как правило, гармонический сигнал который не учитывает особенностей дискретно-квантованного представления речевых сигналов.



ОСОБЕННОСТИ ДИСКРЕТНО-КВАНТОВАННОГО ПРЕОБРАЗОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ



$$\Delta = \frac{U_{\max}}{2^N} \quad (1)$$

где N – число бит цифровой передачи;
 U_{\max} – общий динамический диапазон входного сигнала.

$$e(t) = y(t) - x(t) \quad (2)$$

$$-\frac{\Delta}{2} \leq e(t) \leq \frac{\Delta}{2}$$

Среднее значение мощности
ошибки квантования

$$P_{\Delta} = \frac{\Delta^2}{12} = \frac{1}{12} \left(\frac{U_{\max}}{2^N} \right)^2 \quad (3)$$

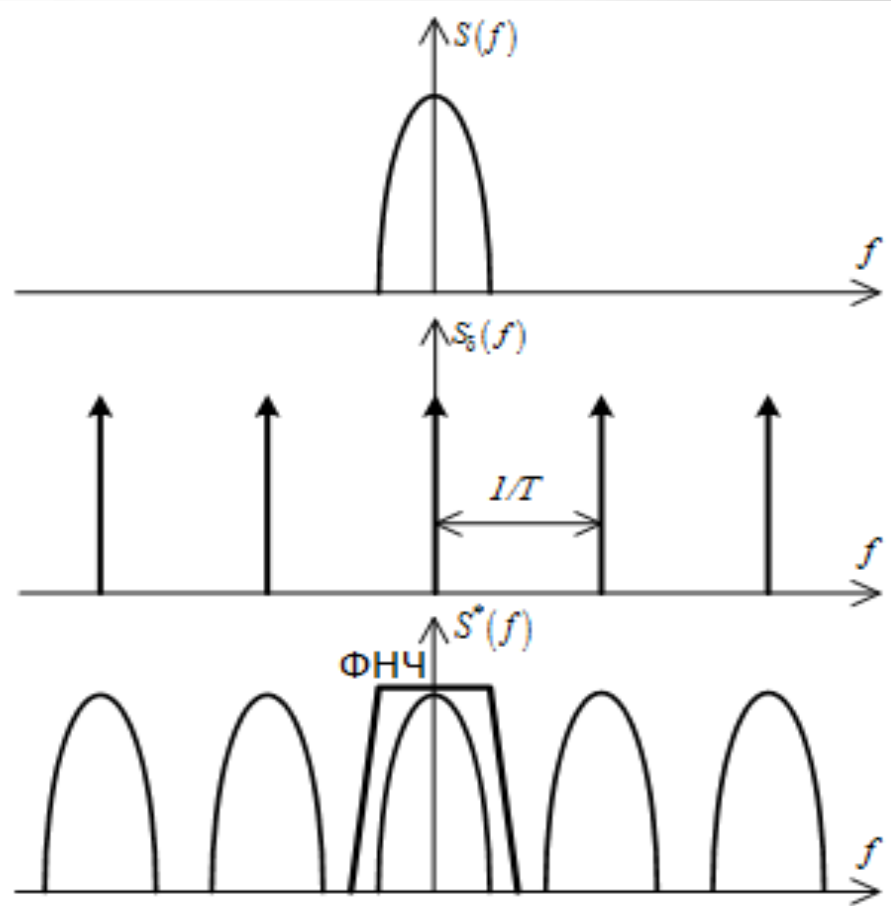
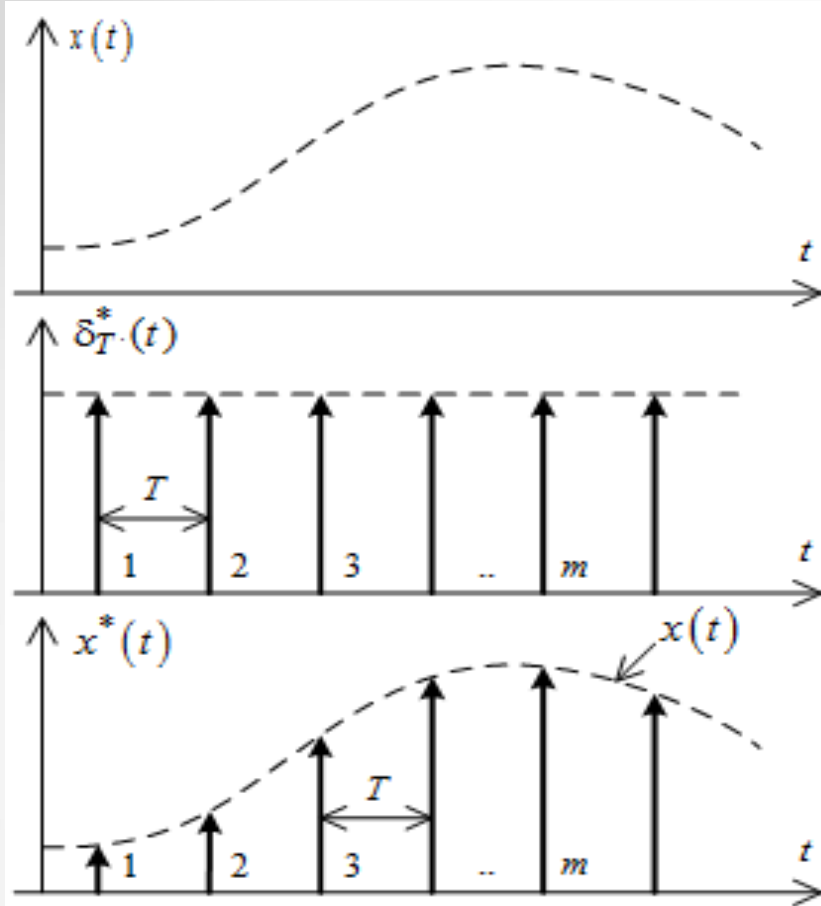
Эффективное значение
ошибки квантования

$$\varepsilon_{\Delta} = \frac{\Delta}{2\sqrt{3}} = \frac{1}{\sqrt{3}} \left(\frac{U_{\max}}{2^{N+1}} \right) \quad (4)$$

Отношение сигнал/шум

$$SNR = 6,02N + 10 \lg \left(\frac{F_{\text{д}}}{2\Delta f_B} \right) + C_s \quad (5)$$

где C_s – постоянная, учитывающая форму входного сигнала;
 U_{\max} – общий динамический диапазон входного сигнала;
 N – число бит цифровой передачи;
 Δf_B – верхнее значение рабочей полосы частот;
 $F_{\text{д}}$ – частота дискретизации.

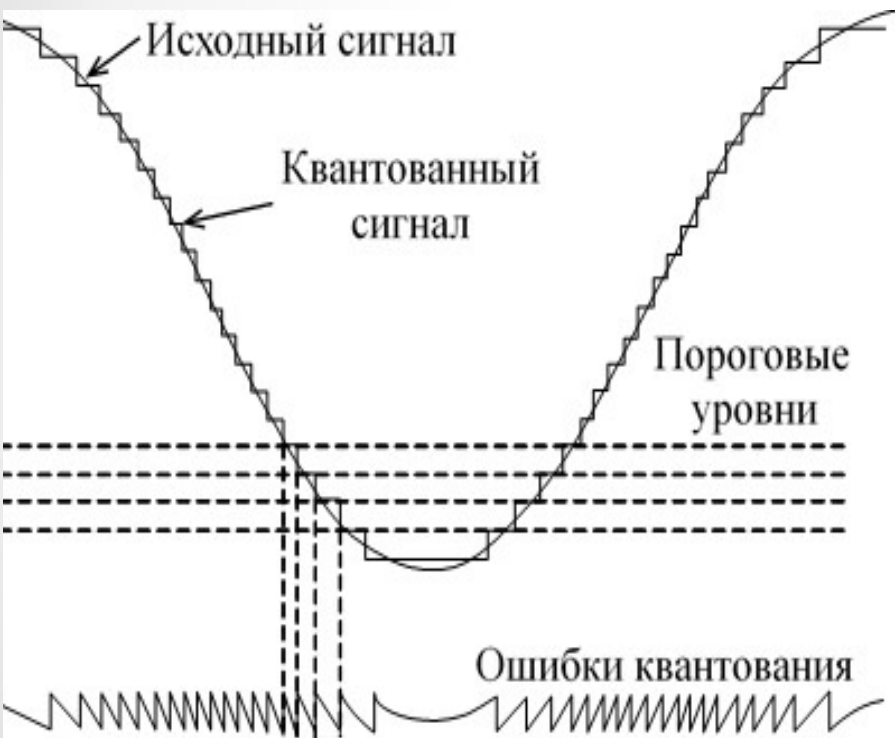


$$x^*(t) = x(t) \cdot \delta_T^*(t) = \sum_{m=-\infty}^{\infty} x(mT) \cdot \delta(t - mT) \quad (6)$$

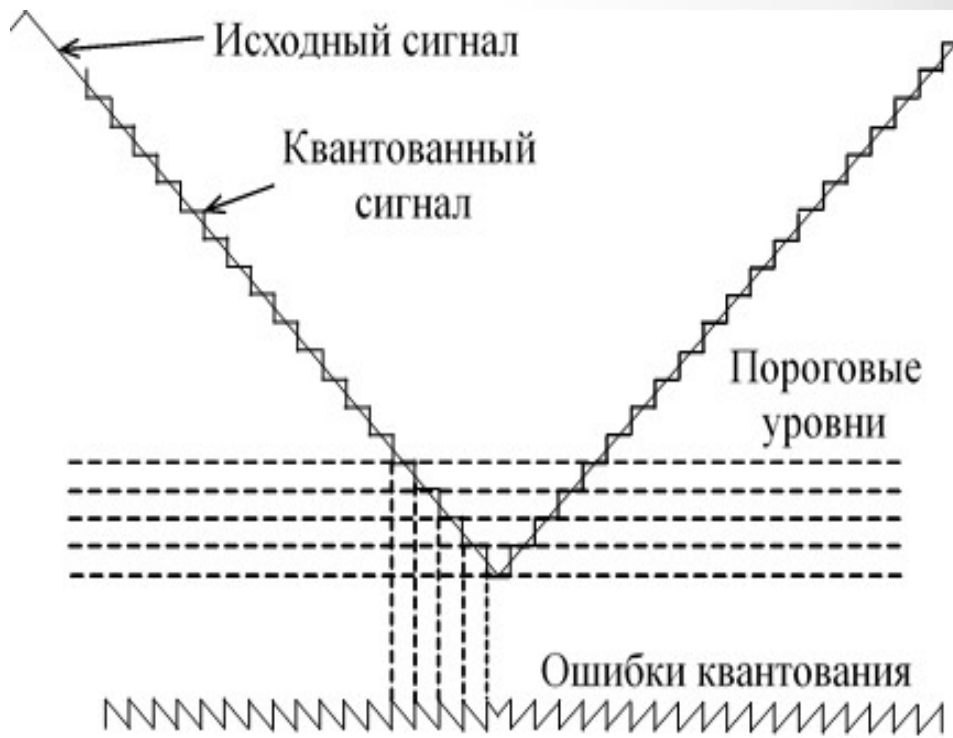
$$x(t) = \sum_{m=-\infty}^{\infty} x(mT) \frac{\sin \omega_c (t - mT)}{\omega_c (t - mT)} \quad (7)$$

ВЫБОР ИЗМЕРИТЕЛЬНОГО СИГНАЛА

КОСИНУСОИДАЛЬНЫЙ



треугольный



Разложение периодической функции треугольной формы (измерительного сигнала) и импульсов пилообразной формы (шума квантования) в ряд Фурье

$$f(t) = \frac{8A}{\pi^2} \sum_{k=1}^{\infty} (-1)^{\frac{k-1}{2}} \frac{\sin k\omega t}{k^2}, \quad (8)$$

где A – амплитуда сигнала;

k – номер гармоники ($k=1,3,5,\dots$);

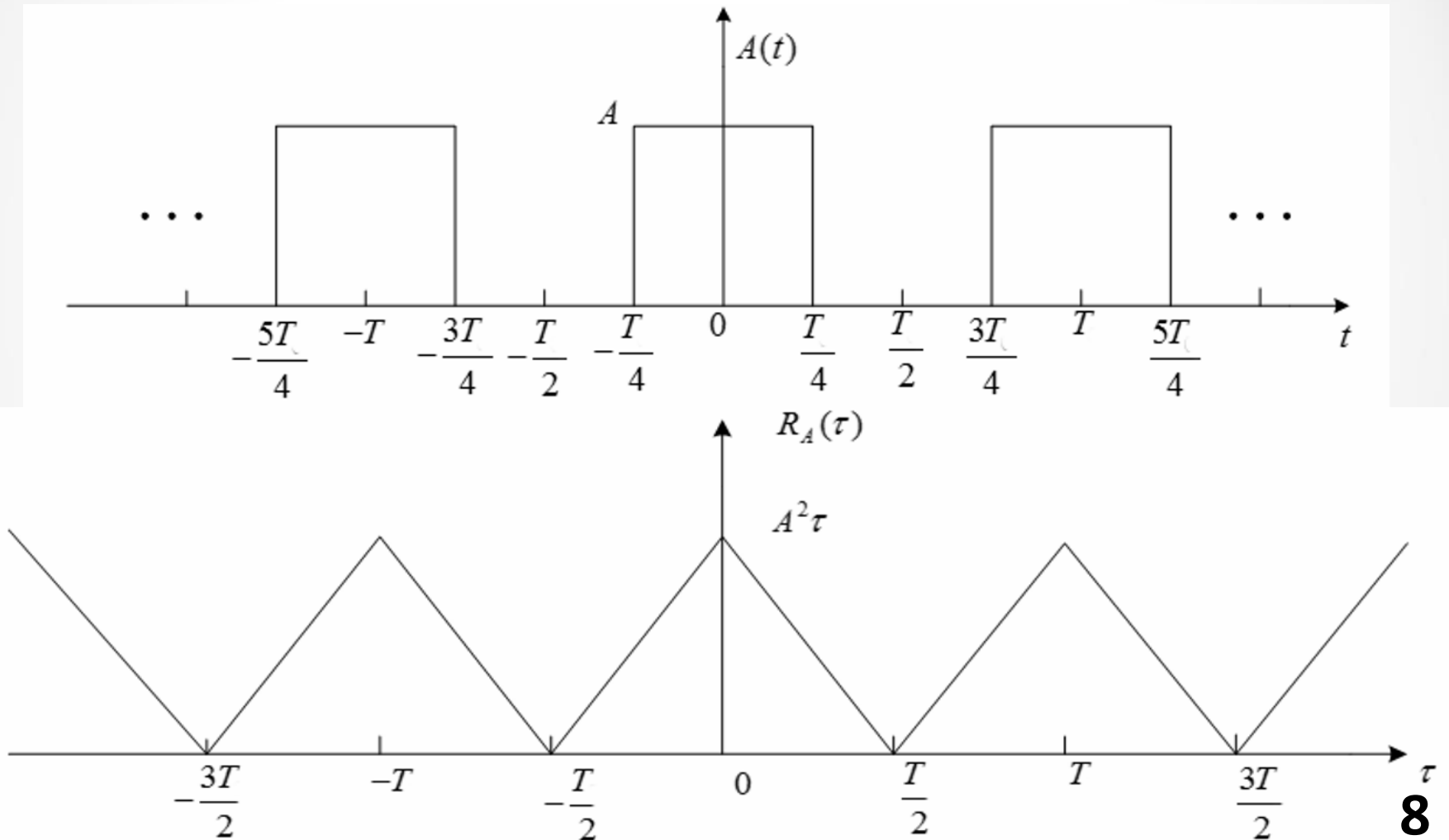
$\omega = \frac{2\pi}{T_{\Pi}}$ – угловая частота сигнала;

T_{Π} – период сигнала.

$$f(t) = \frac{A}{2} - \frac{A}{\pi} \sum_{k=1}^{\infty} \frac{1}{k} \sin k\omega t, \quad (9)$$

где $k = 1, 2, 3, \dots$

Преобразование автокорреляционной функцией периодической импульсной последовательности прямоугольной формы в периодическую импульсную последовательность треугольной формы



Параметры измерительного сигнала

i	F_i , Гц	T_i , мкс
1	250	4000
2	500	2000
3	650	1538
4	800	1250
5	950	1053
6	1125	889
7	1300	769
8	1500	667
9	1700	588
10	1875	533
11	2050	488
12	2250	444
13	2425	412
14	2725	367
15	3100	323
16	3500	286
17	3850	260
18	4550	220
19	6150	163
20	8600	116

ОЦЕНКА ЗАЩИЩЕННОСТИ ДИСКРЕТНО-КВАНТОВАННОГО РЕЧЕВОГО СИГНАЛА

1. На вход АЦП подают измерительный сигнал.
2. Измеряют параметры преобразованного измерительного сигнала в точке наблюдения и шума в той же точке наблюдения.
3. По полученным значениям сигнала и шума определяют отношение сигнал/шум.
4. Определяют отношение нормированных параметров сигнала и шума в канале утечки речевого сигнала.
5. Сравнивают отношение сигнал/шум, полученные в процессе оценки в точке наблюдения с нормированным отношением сигнал/шум. Если отношение сигнал/шум нормированных параметров больше отношения измеренных параметров, то принимают решение о защищенности, т.е. отсутствии канала утечки речевой информации. В противном случае – о наличии канала утечки речевого сигнала.

ЛИТЕРАТУРА

1. Железняк, В.К. Синтез измерительного композитного сигнала для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании / В.К. Железняк, С.В.Лавров, А.Г.Филиппович, М.М.Барановский // Доклады БГУИР. – 2020. – № 18(6), – С. 81-87.
2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – Москва: Горячая линия – Телеком, 2017. – 586 с.
3. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – Санкт-Петербург: ГУАП, 2006. – 188 с.
4. Шкритек, П. Справочное руководство по звуковой схемотехнике / П.Шкритек. – Москва: Мир, 1991 – 446 с.
5. Цыпкин, Я.З. Основы теории автоматических систем / Я.З. Цыпкин. – Москва: Наука, 1977. – 560 с.
6. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – Москва: Вильямс, 2007. – 1104 с.

ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ



НАЦИОНАЛЬНЫЙ ЦЕНТР
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

(19) ВУ (11) **23689**

(13) **С1**

(46) **2022.04.30**

(51) МПК

H 04R 29/00 (2006.01)

(54) СПОСОБ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПРЕОБРАЗОВАННОГО В ЦИФРОВУЮ ФОРМУ РЕЧЕВОГО СИГНАЛА

(21) Номер заявки: а 20190343

(22) 2019.12.04

(43) 2021.08.30

(71) Заявитель: Учреждение образования
"Полоцкий государственный уни-
верситет" (ВУ)

(72) Авторы: Железняк Владимир Кирил-
лович; Лавров Сергей Викторович;
Филиппович Андрей Геннадьевич;
Барановский Михаил Михайлович
(ВУ)

(73) Патентообладатель: Учреждение об-
разования "Полоцкий государствен-
ный университет" (ВУ)

(56) ВУ 16924 С1, 2013.

ВУ 15588 С1, 2012.

ЖЕЛЕЗНЯК В.К. и др. Критерии
оценки защищенности от утечки рече-
вых сигналов. Вести НАН Беларуси.
Серия физико-технических наук. 2017,
№ 1, с. 122-128.

ЖЕЛЕЗНЯК В.К. и др. Метод оценки
защищенности информации, преобра-
зованной в цифровую форму. Вестник
ПГУ. Серия С. Фундаментальные нау-
ки. 2012, № 12, с. 12-193.

CN 106157961 A, 2016.

СПАСИБО ЗА ВНИМАНИЕ