

**В. С. Домрачев, Н. В. Никонов** (Москва, ТК 26, Лаб. ТВП). **О свойствах обобщенных выходных  $\nu$ -грамм полиэдральных классов функций  $k$ -значной логики.**

УДК 532.528.2, 532.694.1      DOI [https://doi.org/10.52513/08698325\\_2020\\_27\\_2\\_138](https://doi.org/10.52513/08698325_2020_27_2_138)

*Резюме:* Изучены свойства некоторых выходных  $\nu$ -грамм с позиции запретов и полузапретов, поступающих с фильтрующего генератора с функцией усложнения  $k$ -значной логики полиэдрального класса, построенного на основе булевой функции от трех существенных переменных.

*Ключевые слова:* запрет, полузапрет, фильтрующий генератор.

#### СПИСОК ЛИТЕРАТУРЫ

1. Словарь криптографических терминов. / Под ред. Б. А. Погорелова, В. Н. Сачкова. М.: МЦНМО, 2006, 92 с. // *Pogorelov B. A., Sachkov V. N.* (Eds.) Dictionary of Cryptographic Terms. Moscow: MCNMO, 2006, 92 p. (In Russian.)
2. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств. — *Обозрение прикл. и промышл. матем.*, 1994, т. 1, в. 1, с. 33–55. // *Sumarokov S. N.* Binary function prohibitions and reversibility for a classes of coding devices. — *OP&PM Surv. Appl. Industr. Math.*, 1994, v. 1, is. 1, p. 33–55. (In Russian.)
3. *Golić J. D.* On the security of nonlinear filter generators. In: Fast Software Encryption. Third International Workshop. FSE 1996. (Cambridge, UK, February 21–23, 1996.) Proceedings / Ed. by D. Gollman. Heidelberg etc.: Springer, 1996, p. 173–188. (Ser. Lect. Notes Comput. Sci. V. 1039.)
4. *Никонов Н. В.* Метод растяжения в построении классов равновероятных  $k$ -значных функций с запретом. — *Обозрение прикл. и промышл. матем.*, 2006, т. 13, в. 6, с. 961–974. // *Nikonov N. V.* Method of extension in construction of classes of equiprobable  $k$ -valued logic functions with interdiction. — *OP&PM Surv. Appl. Industr. Math.*, 2006, v. 13, is. 6, p. 961–974. (In Russian.)
5. *Никонов В. Г.* Пороговые представления булевых функций. — *Обозрение прикл. и промышл. матем.*, 1994, т. 1, в. 3, с. 402–457. // *Nikonov N. V.* Threshold representations of Boolean functions. — *OP&PM Surv. Appl. Industr. Math.*, 1994, v. 1, is. 3, p. 402–457. (In Russian.)
6. *Никонов Н. В.* О классификации всех булевых функций от 3-х переменных с обобщенными запретами. — *Лесной вестник*, 2004, № 5 (36), с. 177–188. // *Nikonov N. V.* Classification of all Boolean functions in three variables with generalized taboo. — *Forestry Bull.*, 2004, № 5 (36), с. 177–188. (In Russian.)
7. *Никонов Н. В.* Полиэдральные классы функций  $k$ -значной логики с обобщенными запретами и полузапретами. — *Матем. вопросы криптографии*, 2012, т. 3, в. 1, с. 53–69. // *Nikonov N. V.* Polyhedral classes of  $k$ -valued logic functions with generalized filter taboo and semi-taboo. — *Math. Asp. Cryptogr.*, 2012, v. 3, is. 1, p. 53–69. (In Russian.)

UDC 532.528.2, 532.694.1      DOI [https://doi.org/10.52513/08698325\\_2020\\_27\\_2\\_138](https://doi.org/10.52513/08698325_2020_27_2_138)

**Domrachev V. S., Nikonov N. V.** (Moscow, Technical Committee 26, TVP Laboratories). **On properties of generalized output sequences of polyhedral  $k$ -valued logic functions.**

*Abstract:* Properties of some output  $\nu$ -blocks in sequences generated by the filter generator with a  $k$ -valued logic output function in three essential variables are studied, taboo and semi-taboo  $\nu$ -blocks being in the focus of investigation.

*Keywords:* filter generator, interdiction, half-interdiction, semi-taboo, taboo.