Исправления в соответствие с рецензией

1. Добавлен следующий текст:

"При запрете на элиминацию импликации задача выяснения возможности свободного назначения для эквивалентных переменных сильно связной компоненты становится, вообще говоря, существенно труднее проблемы выполнимости булевой функции. В частности, трудность этой проблемы может быть оценена классом **DP**, определяемым как множество языков $L = L_1 \cap L_2$, где $L_1 \in \mathbf{NP}$, $L_2 \in \mathbf{co-NP}$ (см. [58], пункт 17.1)."

2. Добавлен следующий текст:

"Определение класса **TFNP** опирается на класс **FNP**. Обычно определение класса **FNP** вводится через определение класса **NP** на основе проверочного отношения. Согласно [Cook2006], проверочное отношение — это бинарное отношение $R \subseteq \Sigma^* \times \Pi^*$ для некоторых алфавитов Σ и Π. Произвольному проверочному отношению R можно поставить в соответствие язык $L_R = \{x\#y \mid R(x,y)\}$ над алфавитом $\Sigma \cup \Pi \cup \{\#\}$, где $\# \notin \Sigma$. Говорят, что отношение R вычислимо за полиномиальное время, если $L_R \in \mathbf{P}$ [Cook2006]. Язык L над алфавитом Σ принадлежит классу **NP** тогда и только тогда, когда существует натуральное число k и вычислимое за полиномиальное время проверочное отношение R такие, что для всех $x \in \Sigma^*$ слово x принадлежит языку L тогда и только тогда, когда существует y, удовлетворяющее условиям $|y| \leq |x|^k$ и $R(x,y)$ [Cook2006]. Для произвольного языка $L \in \mathbf{NP}$ мы можем определить проблему FL, требующую на вход $x \in \Sigma^*$ ответить "Нет", если $x \notin L$, и найти $y \in \Pi^*$, если $x \in L$. Соответственно, класс **FNP** можно определить как множество $\{FL \mid L \in \mathbf{NP}\}$ (см. [58], глава 10). Формально класс **TFNP** определяется как подкласс класса **FNP**, состоящий из всех проблем имеющих решение для любых исходных данных (см. [58], глава 10)."

Добавлена библиографическая ссылка:

[Cook2006] *Cook S.* The P versus NP Problem //*The Millennium Prize Problems* /Eds. J. Carlson, A. Jaffe, and A. Wiles. Providence: American Mathematical Society, 2006. P. 87–104.

3. Добавлен следующий текст и соответствующие библиографические ссылки:

"Заметим, что повышение сложности множества M в общем случае создает определенные трудности как злоумышленнику, так и защитнику. Однако злоумышленнику необходимо решать задачу принадлежности множеству M, что соответствует проблеме распознавания множества M: в общем случае множество распознаваемых языков равно классу рекурсивных языков **R**. Защитнику необходимо уметь решать лишь задачу генерации множества M, что соответствует проблеме перечисления множества M: в общем случае множество перечислимых языков равно классу рекур-

сивно перечислимых языков **RE**. Хорошо известно, что $\mathbf{R} \subset \mathbf{RE}$. Поэтому в общем случае защитник имеет существенное преимущество, располагая возможностью выбрать язык из множества $\mathbf{RE} \backslash \mathbf{R}$. Естественно соотношение $\mathbf{R} \subset \mathbf{RE}$ гарантирует защитнику лишь теоретическое преимущество, поскольку с практической точки зрения представляют интерес лишь полиномиальные вычисления. На сегодняшний день известно несколько полиномиальных аналогов класса рекурсивно перечислимых языков (см., например, [**?**, **?**, **?**, **?**]). В частности, в работе [**?**] введено понятие полиномиальной перечислимости по итерации. Как показано в работе [**?**], класс языков, которые полиномиально перечислимы по итерации, является весьма обширным (см. [**?**], теорема 4.2) и, в частности, включает все **EXPTIME**-полные языки (см. [**?**], следствие 4.7), где **EXPTIME** — класс языков, которые распознаваемы за экспоненциальное время. Поэтому защитник за полиномиальное время может генерировать, например, множество M, являющееся некоторой комбинацией **EXPTIME**-полных языков. При этом злоумышленнику придется осуществлять гарантированно экспоненциальное по времени вычисление только для решения задачи принадлежности множеству M. Таким образом, учитывая то, что $\mathbf{P} \neq \mathbf{EXPTIME}$, при использовании такого подхода к шифрованию невозможность взлома за полиномиальное время можно гарантировать даже в случае $\mathbf{P} = \mathbf{NP}$."