досрочный демонтаж. Полученные результаты целесообразно использовать в процессе проектирования и внедрения ТКС. Дальнейшим развитием данных результатов будет учет при оптимизации периодичности КР структур резервирования ТКС.

ЛИТЕРАТУРА

1. Gertsbakh, I. Reliability theory with applications to preventive maintenance / I. Gertsbakh. – N.Y. : Springer Verlag. – 2000. – 219 p.

2. Nakagava, T. Maintenance theory of reliability / T. Nakagava – N.Y. : Springer Verlag. – 2005. – 258 p.

3. Уланский В.В., Конахович Г.Ф., Мачалин И.А. Организация системы технического обслуживания и ремонта радиоэлектронного комплекса Ту-204: Учебное пособие / В.В.Уланский, Г.Ф., Конахович, И.А. Мачалин // – К.: КИИГА, 1992. – 103с.

4. Уланский, В. В. Математическая модель процесса эксплуатации легкозаменяемых блоков систем авионики / В. В. Уланский, И. А. Мачалин // Авіаційно-космічна техніка і технологія. – 2006.–№ 6(32). – С. 74–80.

5. Уланский В. В. Достоверность многоразового контроля работоспособности невосстанавливаемых радиоэлектронных систем/ В. В. Уланский // Ресурсосберегающие технологии обслуживания и ремонта авиационного и радиоэлектронного оборудования воздушных судов гражданской авиации. Сб. науч. тр. – К.: КИИГА. – 1992. – С.14 – 25.

6. Уланский, В. В. Уточненная модель обслуживания одноблочной системы авионики /

7. В.В. Уланский, И. А. Мачалин // Электронное моделирование.– 2008.–Т. 30, № 2. – С. 55–67.

8. MIL-HDBK - 338B. Electronic reliability design handbook// Air Force Research Laboratory Information, Fort Belvoir, Virginia, 1991. – 1046 p.

Надійшла: 13.07.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.

УДК 004.056.53+530.145

Николаенко С.В., Василиу Е.В.

ОЦЕНКА КОРРЕКТИРУЮЩЕЙ СПОСОБНОСТИ ПОМЕХОУСТОЙЧИВОГО КОДА ФАЙРА ДЛЯ РЕАЛИЗАЦИИ ПИНГ-ПОНГ ПРОТОКОЛА С ПАРАМИ ПЕРЕПУТАННЫХ КУБИТОВ В КВАНТОВОМ КАНАЛЕ С ПОМЕХАМИ

В статье разработана имитационная модель пинг-понг протокола с парами перепутанных кубитов в квантовом канале с помехами с целью оценки корректирующей способности помехоустойчивого кода Файра и выяснения границ применимости этого кода для данного протокола квантовой криптографии. Детально проанализированы виды ошибок, которые будут возникать при реализации пинг-понг протокола с парами перепутанных кубитов в квантовом канале с помехами. Показано, что код Файра (60,44) полностью справляется с исправлением ошибок, если вероятность деполяризации кубита в канале не превышает приблизительно 7%, что соответствует современной экспериментальной ситуации при передаче отдельных фотонов на расстояние порядка 100 км. При более высоком уровне помех в канале частичное исправление ошибок кодом Файра позволит увеличить скорость передачи информации в квантовом пинг-понг протоколе.

Ключевые слова: квантовая криптография, пинг-понг протокол, ошибки в квантовом канале связи, помехоустойчивый код Файра, имитационное моделирование.

Введение. В современном информационном обществе существует большое и постоянно нарастающее количество информационных ресурсов, требующих надежных методов защиты от несанкционированного доступа. Важнейшей задачей является защита конфиденциальной информации, передаваемой по открытым каналам связи. Одним из современных методов защиты передаваемой информации является квантовая криптография, основанная на передаче информации квантовыми состояниями отдельных частиц (фотонов). Одно из направлений квантовой криптографии – протоколы квантовой прямой безопасной связи (КПБС), в которых традиционное шифрование и секретный ключ вообще не используются, а роль ключа в некотором смысле играет информационный ресурс квантовой механики – совместно используемые авторизованными пользователями группы перепутанных квантовых частиц.

К настоящему времени предложено несколько десятков различных по назначению протоколов КПБС [1–9]. Одним из таких протоколов, не требующим наличия квантовой памяти большого объема, является пинг-понг протокол с парами перепутанных кубитов, который позволяет передать один бит классической информации за один цикл протокола [2]. Увеличение стойкости протокола возможно путем использования классических криптографических методов (например, обратимое хеширование) [9]. Информационная емкость протокола может быть увеличена за счет использования квантового сверхплотного кодирования, а также использования многомерных квантовых систем [6–9].

Поскольку в реальных квантовых каналах связи всегда есть помехи, то для практической реализации пинг-понг протоколов нужны помехоустойчивые коды, исправляющие ошибки. К настоящему времени разработаны несколько семейств квантовых помехоустойчивых кодов, которые исправляют непосредственно испорченные в канале квантовые состояния [10]. Однако, практическое применение таких кодов требует использования квантовых логических элементов (элементов квантового компьютера), что с технологической точки зрения пока что достаточно сложно и нерационально.

Поскольку пинг-понг протокол предназначен для безопасной передачи классической информации квантовыми каналами связи, то имеется возможность кодировать классическими помехоустойчивыми кодами непосредственно классическую информацию до ее передачи квантовыми частицами. В протоколах с группами n перепутанных кубитов информация передается пакетами по n бит [9], поэтому и ошибки будут возникать пачками соответствующей длины. К настоящему времени разработано большое количество классических помехоустойчивых кодов [11–14], которые исправляют пачки ошибок и могут быть применены для защиты от естественных помех информации, передаваемой с помощью квантовых пинг-понг протоколов. Одним из таких кодов является код Файра, используемый для помехоустойчивого кодирования в классических каналах с высокой интенсивностью помех, когда возникают ошибки кратностью две и более. Однако, если оценки корректирующей способности классических кодов Рида–Соломона при передаче информации некоторыми пинг-понг протоколами частично выполнялись ранее [15], то для более простого кода Файра таких оценок ранее вообще не проводилось.

Целью настоящей работы является оценка корректирующей способности кода Файра при реализации пинг-понг протокола с парами перепутанных кубитов и квантовым сверхплотным кодированием [6] в квантовом канале с помехами. Для достижения поставленной цели в работе детально проанализированы виды ошибок, которые будут возникать при реализации данного пинг-понг протокола в квантовом канале с помехами; построен помехоустойчивый код Файра (60,44) в поле Галуа GF(2); разработан алгоритм и программное обеспечение для имитационного моделирования пинг-понг протокола с парами перепутанных кубитов; проанализированы полученные статистические данные.

1. Режим передачи сообщения в пинг-понг протоколе с парами перепутанных кубитов. Рассмотрим кратко режим передачи сообщения пинг-понг протокола с парами полностью перепутанных кубитов и квантовым сверхплотным кодированием [6].

Существуют четыре состояния Белла, которые являются полностью перепутанными состояниями пары кубитов и образуют ортонормированный базис в гильбертовом пространстве двух кубитов:

$$\left|\varphi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right); \qquad \left|\varphi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2\right);$$

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right); \qquad \left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2\right), \qquad (1)$$

где индексы 1 и 2 указывают на номер кубита.

Передающая сторона (Алиса) предварительно разбивает свою строку битов на пары битов. Далее выполняются следующие шаги.

Боб (получатель сообщения) приготавливает пару кубитов в состоянии $|\psi^+\rangle$. В качестве двух базисных состояний кубитов $|0\rangle$ и $|1\rangle$ в данном протоколе используют поляризационные состояния фотонов. Так, например, $|0\rangle$ соответствует вертикальной, а $|1\rangle$ – горизонтальной поляризации фотона. Боб хранит один из фотонов состояния $|\psi^+\rangle$ ("домашний фотон") в квантовой памяти и посылает Алисе (отправитель сообщения) второй фотон ("передаваемый фотон") через квантовый канал. Алиса случайным образом переключается между режимом передачи сообщения и режимом контроля подслушивания. Режим контроля подслушивания в пинг-понг протоколах служит для обнаружения атаки пассивного перехвата и не требует помехоустойчивого кодирования, поэтому здесь мы этот режим не рассматриваем.

В режиме передачи сообщения (рис. 1) Алиса выполняет унитарную операцию U_{ij} над передаваемым фотоном для кодирования информации и посылает этот фотон назад Бобу. Кодирующие операции Алисы имеют вид:

$$U_{00} = I;\ U_{01} = \sigma_z;\ U_{10} = \sigma_x;\ U_{11} = i\sigma_y, \qquad (2)$$

где $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ и $\sigma_y = i\sigma_x\sigma_z = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ – операторы Паули.

Операции (2) преобразуют состояние $|\psi^+\rangle$ в состояния $|\psi^+\rangle$, $|\psi^-\rangle$, $|\varphi^+\rangle$ и $|\varphi^-\rangle$, и соответствуют, например, следующим комбинациям двух классических битов: "00", "01", "10" и "11" (о таком соответствии Алиса и Боб договариваются заранее). Когда Боб получает передаваемый фотон обратно, он выполняет измерение над обоими фотонами в базисе Белла, чтобы декодировать посланную Алисой двухбитовую строку (см. рис. 1). Таким образом, передавая по квантовому каналу один кубит, можно передать два классических бита информации.

2. Виды квантовых ошибок. В классической теории передачи информации, когда информация передается битами, единственный возможный тип ошибок, который может произойти, – это переворот бита. В квантовом случае любое вращение или изменение фазы в гильбертовом пространстве квантового состояния является ошибкой, т.е. существует бесконечное число различных ошибок, которые могут произойти уже с одним, единственным кубитом.

Однако основное и очень важное свойство квантового исправления ошибок заключается в том, что квантовый код, исправляющий некоторое дискретное множество ошибок, способен автоматически исправлять *непрерывное* множество ошибок [16].

Это происходит по причине того, что измерение синдрома ошибки либо проецирует состояние с малой ошибкой на исходное состояние, т.е. состояние без ошибки, либо проецирует ошибочное состояние на одно из состояний из дискретного множества больших ошибок. Таким образом, происходит дискретизация квантовых ошибок, что и позволяет создать квантовые коды для исправления некоторого дискретного множества больших ошибок. Эти коды могут автоматически исправлять любую ошибку в состоянии квантовых систем [10,16].

Множество больших ошибок, которые могут произойти при передаче отдельного кубита по квантовому каналу связи, состоит из следующих трех видов ошибок [10,16]:

1. Ошибка переворота состояния кубита, называемая "классической" ошибкой; при такой ошибке общее состояние кубита $|\psi\rangle = a|0\rangle + b|1\rangle$ преобразуется в $|\psi'\rangle = a|1\rangle + b|0\rangle$.
2. Ошибка переворота фазы, $|\psi\rangle = a|0\rangle + b|1\rangle$ преобразуется в $|\psi'\rangle = a|0\rangle - b|1\rangle$, т.е. относительная фаза между базисными состояниями $|0\rangle$ и $|1\rangle$ изменяется на π.

3. Фазовая ошибка, являющаяся комбинацией переворота кубита и переворота фазы, $|\psi\rangle = a|0\rangle + b|1\rangle$ преобразуется в $|\psi'\rangle = a|1\rangle - b|0\rangle$.

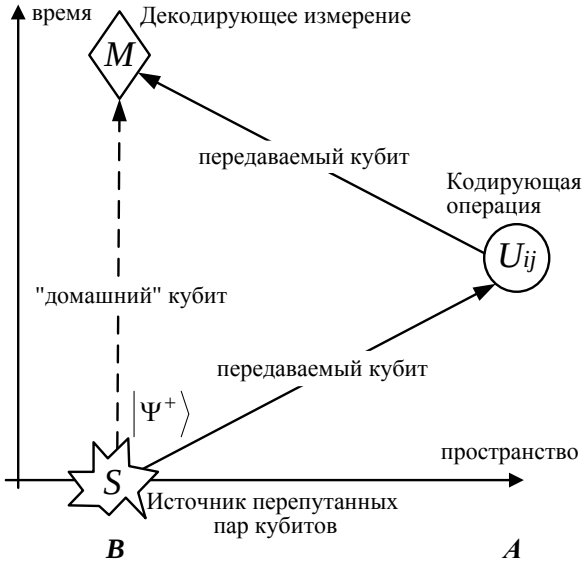


Рис.1. Режим передачи сообщения в пинг-понг протоколе с парами перепутанных кубитов

Эти три вида ошибок могут быть описаны действием на кубит трех операторов Паули. Так, "классическая" ошибка описывается действием на кубит оператора σ_x, ошибка переворота фазы – действием оператора σ_z и фазовая ошибка – оператора σ_y.

Возможны также ошибка затухания амплитуды – это ошибка, связанная с диссипацией энергии, а также ошибка затухание фазы – это чисто квантовомеханический процесс шума, связанный с потерей квантовой информации без потери энергии [10]. Физически он описывает, например, процесс, при котором фотон случайным образом рассеивается при распространении по волноводу. Можно показать [10], что ошибка затухания фазы описывается тем же оператором σ_z, что и ошибка переворота фазы, и, таким образом, может быть исправлена тем же квантовым помехоустойчивым кодом, что и ошибка переворота фазы.

Деполяризующий канал является одной из важных моделей квантового шума и может быть представлен действием оператора [10]

$$\varepsilon(\rho) = (1-p)\rho + \frac{p}{3}\left(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z\right), \qquad (3)$$

где ρ – оператор плотности квантовой системы.

Для чистого состояния отдельного кубита действие деполяризующего канала заключается в следующем: с вероятностью $1-p$ состояние кубита остается неизменным (т.е. ошибки не происходит) и с вероятностью p этот кубит деполяризуется, т.е. происходит либо переворот состояния кубита, либо переворот его фазы, либо фазовая ошибка. Следовательно, деполяризующий канал является моделью, учитывающей основные виды больших дискретных квантовых ошибок, и широко используется в квантовой теории информации как модель источника квантового шума.

3. Ошибки, возникающие при реализации пинг-понг протокола в квантовом канале с шумом. Будем считать, что состояние домашнего фотона хранится у Боба в надежной квантовой памяти и не подвержено ошибкам. Таким образом, возможно только изменение состояния передаваемого фотона. Будем также считать, что Боб оставляет у себя первый фотон и передает второй по квантовому каналу. В качестве модели квантового шума рассмотрим деполяризующий канал. Деполяризация фотона с вероятностью p может происходить как на пути Боб $\rightarrow$ Алиса, так и на пути Алиса $\rightarrow$ Боб. Рассмотрим сначала случай, когда ошибка происходит на пути Боб $\rightarrow$ Алиса. Так как начальное, приготовленное

Бобом состояние пары фотонов – $|\psi^+\rangle$, то необходимо рассмотреть действие деполяризующего канала на второй фотон пары, которая находится в этом состоянии. Таким образом, нужно применить оператор $\varepsilon(\rho)$ (3) ко второму кубиту матрицы плотности

$$\rho = |\psi^+\rangle\langle\psi^+| = \frac{1}{2}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right)\left(\langle 1|_2\langle 0|_1 + \langle 0|_2\langle 1|_1\right). \quad (4)$$

Вычисления показывают, что действие оператора переворота кубита $\sigma_x\rho\sigma_x$ на второй кубит в состоянии (2) преобразует оператор плотности ρ в оператор плотности $\rho' = \frac{1}{2}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right)\left(\langle 0|_2\langle 0|_1 + \langle 1|_2\langle 1|_1\right) = |\varphi^+\rangle\langle\varphi^+|$. Таким образом, оператор $\sigma_x\rho\sigma_x$ преобразует состояние $|\psi^+\rangle$ в состояние $|\varphi^+\rangle$. Аналогично, операторы $\sigma_y\rho\sigma_y$ и $\sigma_z\rho\sigma_z$ преобразуют состояние $|\psi^+\rangle$ в состояния $|\varphi^-\rangle$ и $|\psi^-\rangle$ соответственно. Таким образом, в результате деполяризации фотона при его передаче от Боба к Алисе, состояние $|\psi^+\rangle$ случайным образом превращается в одно из трех остальных белловских состояний.

Аналогичным образом можно показать, что действие оператора $\varepsilon(\rho)$ (3) на второй кубит состояний $|\varphi^+\rangle$, $|\varphi^-\rangle$ и $|\psi^-\rangle$ с вероятностью $1-p$ оставляет состояние неизменным и с вероятностью p преобразует каждое из этих состояний в одно из трех других состояний базиса Белла. Так, например, если ошибка не происходит на пути Боб $\rightarrow$ Алиса, то перепутанная пара сохраняется в состоянии $|\psi^+\rangle$. Тогда, предположим, Алиса хочет передать пару битов "01" и выполняет кодирующую операцию $U_{01} = \sigma_z$, преобразуя состояние $|\psi^+\rangle$ в $|\psi^-\rangle$. Однако на пути Алиса $\rightarrow$ Боб происходит переворот передаваемого кубита σ_x и состояние пары кубитов становится $|\varphi^-\rangle$. Выполнив измерение в базисе Белла и получив $|\varphi^-\rangle$, Боб решает, что Алиса передала "11".

Даже если предположить, что деполяризация происходит с одним и тем же передаваемым фотоном и на пути Боб $\rightarrow$ Алиса, и на пути Алиса $\rightarrow$ Боб, вероятность чего пропорциональна p^2 и очень мала при малых p, то результатом измерения Боба всё равно будет одно из состояний $|\psi^+\rangle$, $|\psi^-\rangle$, $|\varphi^+\rangle$, или $|\varphi^-\rangle$. Следовательно, можно сделать вывод, что при реализации пинг-понг протокола с перепутанными парами кубитов в деполяризующем канале возможные ошибки приводят к тому, что вместо правильного состояния Боб получает одно из трех других состояний базиса Белла. Это означает, что ошибки в передаваемых битовых строках будут возникать *пачками длиной два бита*. Отсюда и следует необходимость применения помехоустойчивых кодов, исправляющих пачки ошибок.

Отметим, что модель деполяризующего канала (3) учитывает только большие дискретные ошибки. Однако учет малых ошибок качественно не меняет картины: результаты измерений Боба будут теперь зависеть не от вероятностей больших ошибок, а от вероятностей малых изменений фазы передаваемого фотона.

4. Код Файра над полем Галуа GF(2). Рассмотрим *алгоритм кодера Файра*:

1. Умножение кодовой комбинации (битовой строки) $g(x)$ на одночлен x^m, имеющий ту же степень, что и образующий многочлен $p(x)$ [12].
2. Деление произведения $g(x)\,x^m$ на образующий многочлен $p(x)$:

$$g(x)\,x^m / p(x) = q(x) + r(x) / p(x), \quad (5)$$

где $q(x)$ – частное от деления; $r(x)$ – остаток.

Умножая выражение (5) на $p(x)$ и перенося $r(x)$ в другую часть равенства, согласно правилам алгебры двоичного поля, т.е. без перемены знака на обратный, получаем

$$f(x) = g(x)p(x) = g(x)\, x^m + r(x). \quad (6)$$

Алгоритм декодера Файра. Согласно (6), декодирование закодированного сообщения $f(x)$ можно выполнить умножением заданной кодовой комбинации $g(x)$ на одночлен x^m, имеющий ту же степень, что и образующий многочлен $p(x)$, с добавлением к этому произведению остатка $r(x)$, полученного после деления произведения $g(x)\cdot x^m$ на образующий многочлен $p(x)$.

Код Файра может исправлять пачку ошибок длинной l_s и обнаруживать пачку ошибок длинной l_r , так как в коде Файра понятие кодового расстояния d не используются.

Следовательно, образующий многочлен кода Файра $p(x)_\phi$ определяется из выражения $p(x)_\phi = p(x)(x^c-1)$.

Число проверочных символов определяется из выражения

$$m=c+L, \quad (7)$$

где L – степень неприводимого многочлена [14], c – параметр: $c \geq l_s + l_r - 1$.

При передаче информации посредством квантового канала вероятность возникновения ошибок достаточно велика, поэтому был выбран кода Файра (60,44), позволяющий исправлять пачки ошибок длиной два бита, возникающие при изменениях состояний перепутанных пар кубитов, используемых в рассматриваемом в данной статье пинг-понг протоколе.

5. Имитационное моделирование пинг-понг протокола с парами перепутанных кубитов в квантовом канале с помехами. Для усиления стойкости пинг-понг протоколов можно применять метод обратимого хеширования, предложенный в [9]. Вкратце, этот метод состоит в следующем.

Перед передачей Алиса разбивает свое двоичное сообщение на l блоков некоторой фиксированной длины r, обозначим эти блоки через a_i $(i = 1,\ldots l)$, затем генерирует для каждого блока отдельно случайную обратимую двоичную матрицу K_i размера $r \times r$ и умножает полученные матрицы на соответствующие блоки сообщения: $b_i = K_i a_i$. Полученные в результате блоки b_i передаются по квантовому каналу с использованием пинг-понг протокола. Даже если подслушивающему агенту (Еве) удастся перехватить один (или несколько) из этих блоков, оставшись не обнаруженной, то, не зная использованных матриц K_i, Ева не может восстановить исходные блоки a_i.

Для обеспечения достаточного уровня безопасности длина блока r и соответственно размер матриц K_i должны выбираться так, чтобы вероятность необнаружения Евы после передачи *одного* блока была пренебрежимо малой величиной. Матрицы K_i передаются Бобу по обычному открытому каналу после завершения квантовой передачи, но только в том случае, если Алиса и Боб убедились в отсутствии подслушивания. Затем Боб обращает полученные матрицы и, умножив их на соответствующие блоки b_i, восстанавливает исходное сообщение: $a_i = K_i^{-1} b_i$.

В соответствии с вышеизложенным методом усиления стойкости пинг-понг протоколов для имитационного моделирования протокола с парами перепутанных кубитов разработан алгоритм последовательности действий, который состоит в следующем.

Шаг 1. Сообщение разбивается на l блоков a_i заданной длины r. Длина блока определяется из условия того, что вероятность необнаружения атаки после передачи одного блока не превышает заданную величину 10^{-k} [9]:

$$r \geq I = \frac{-kI_0}{\lg((1-q)/(1-q\cdot(1-d)))}, \quad (8)$$

где I – количество информации, которое получает Ева при передаче одного блока;
I_0 – количество информации, которое получает Ева за один раунд протокола;
q – вероятность перехода в режим контроля подслушивания;
d – уровень ошибок, вносимый атакой Евы.

Шаг 2. Генерация случайной, обратимой в поле GF(2) двоичной матрицы K_i размером $r \times r$ и умножение матрицы на соответствующий блок $b_i = K_i a_i$.

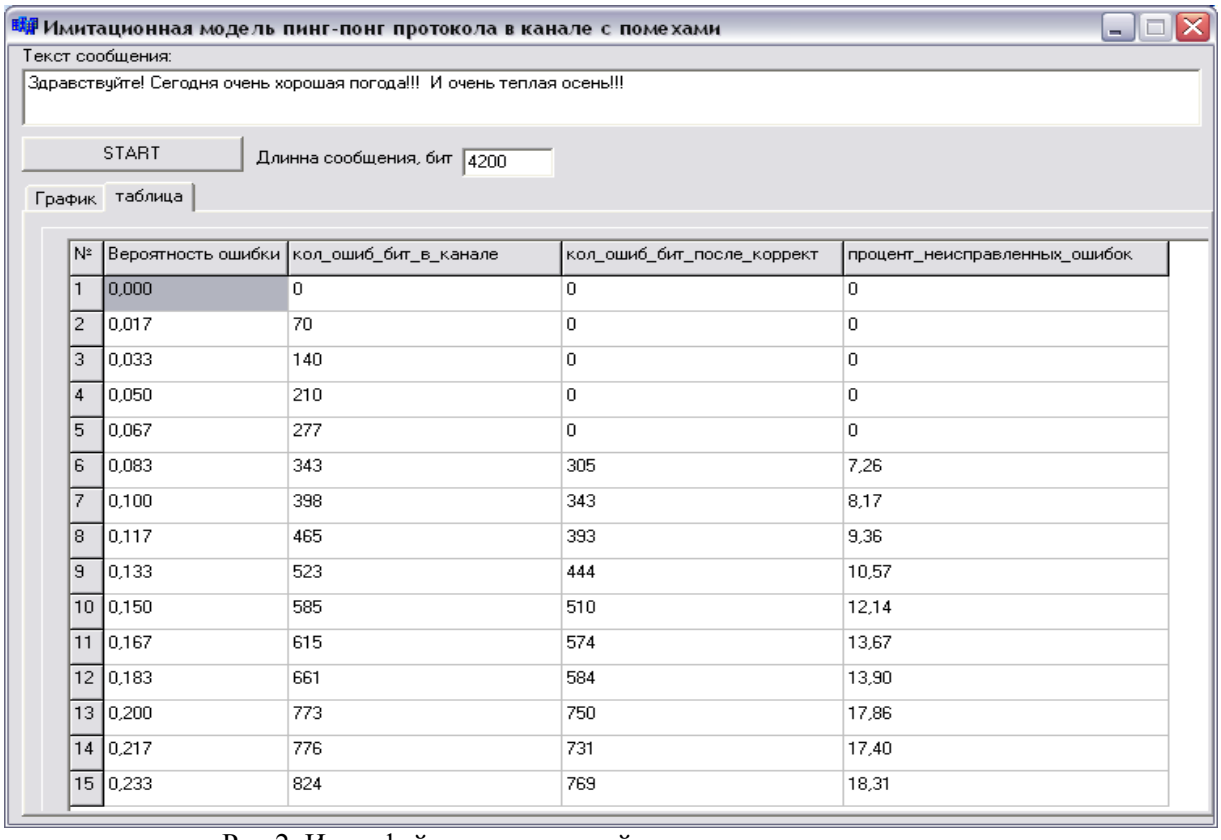
Шаг 3. Кодирование полученного блока b_i с помощью кодера кода Файра (60,44).

Шаг 4. Выполнение режима передачи сообщения пинг-понг протокола с парами перепутанных кубитов, т.е. моделирование передачи блока b_i при возникновении с заданной вероятностью пачек ошибок длиной 2 бита в канале. Режим контроля подслушивания пинг-понг протокола не моделировался.

Шаг 5. Декодирование блока b_i с помощью декодера кода Файра (60,44).

Шаг 6. Восстановление исходного блока данных a_i умножением полученного блока b_i на соответствующую обратную матрицу: $a_i = M_i^{-1} b_i$.

6. Результаты моделирования. Для моделирования работы режима передачи сообщения пинг-понг протокола с парами перепутанных кубитов в среде программирования C++ Builder разработано программное обеспечение, интерфейс которого показан на рис. 2, 3. В результате моделирования получены статистические данные о корректирующей способности кода Файра. Пример этих данных для строки длиной 4200 бит также показан на рис. 2, 3.



№	Вероятность ошибки	кол_ошиб_бит_в_канале	кол_ошиб_бит_после_коррект	процент_неисправленных_ошибок
1	0,000	0	0	0
2	0,017	70	0	0
3	0,033	140	0	0
4	0,050	210	0	0
5	0,067	277	0	0
6	0,083	343	305	7,26
7	0,100	398	343	8,17
8	0,117	465	393	9,36
9	0,133	523	444	10,57
10	0,150	585	510	12,14
11	0,167	615	574	13,67
12	0,183	661	584	13,90
13	0,200	773	750	17,86
14	0,217	776	731	17,40
15	0,233	824	769	18,31

Рис.2. Интерфейс имитационной модели пинг-понг прокола с парами перепутанных кубитов в квантовом канале с помехами

Выводы. Полученные в результате моделирования статистические данные показывают, что помехоустойчивый код Файра (60,44) полностью справляется с исправлением ошибок, если вероятность деполяризации кубита в канале не превышает приблизительно 7%, что соответствует современной экспериментальной ситуации при передаче отдельных фотонов на расстояние порядка 100 км. Этот код, в принципе, может

быть использован и при более высоком уровне помех в канале, когда возникнет необходимость повторной передачи блоков.

Однако даже частичное исправление ошибок кодом Файра позволит повысить скорость передачи, как и при использовании более сложных кодов Рида – Соломона [15].

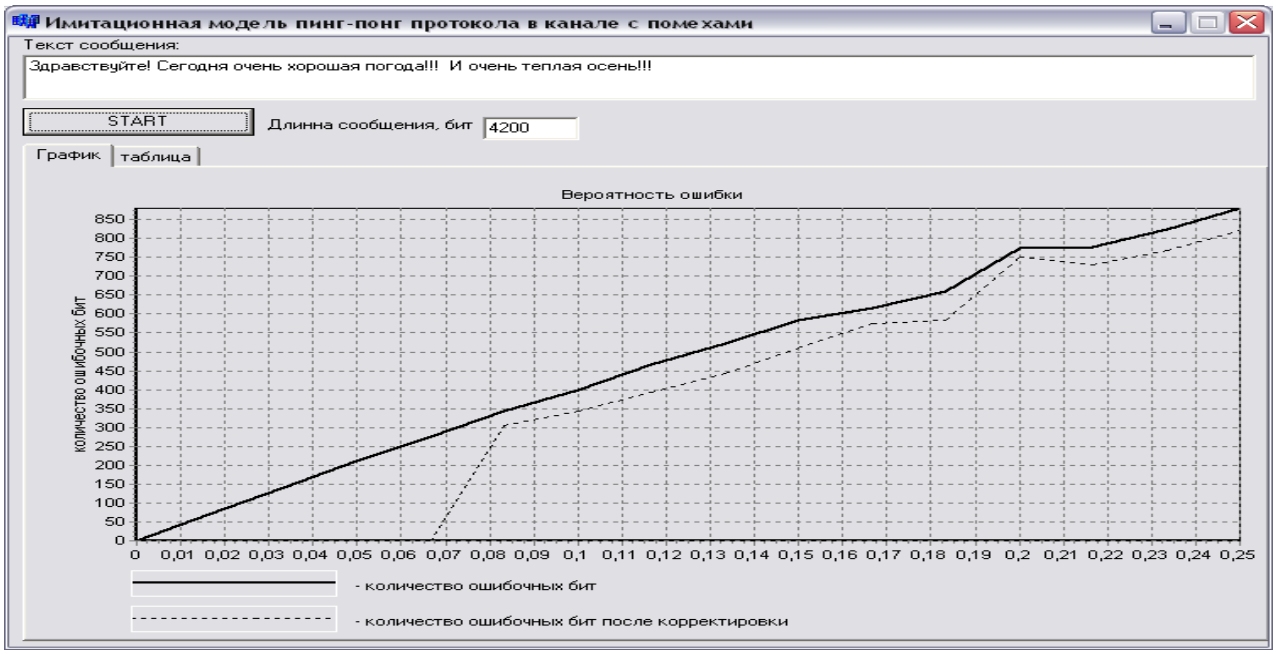


Рис.3. Зависимость количества ошибочных бит от вероятности ошибки в деполяризирующем квантовом канале

Следовательно, можно сделать вывод, что двоичный код Файра (60,44) достаточно эффективен для помехоустойчивого кодирования в пинг-понг протоколе с парами перепутанных кубитов.

ЛИТЕРАТУРА

1. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.

2. Deng F.-G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block / F.-G. Deng, G.L. Long, X.-S. Liu // Physical Review A. – 2003. – V. 68, № 4. – 042317.

3. Wang Ch. Multi – step quantum secure direct communication using multi – particle Greenberger – Horne – Zeilinger state / Ch. Wang, F.G. Deng, G.L. Long // Optics Communications.– 2005. – V. 253, № 1. – P. 15 – 20.

4. Li X.-H. Multiparty Quantum Remote Secret Conference / X.-H. Li, C.-Y. Li, F.-G. Deng et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23 – 26.

5. Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X. Ji, Y.-Q. Zhang et al // Physics Letters A. – 2006. – V. 354, № 1-2. – P. 67 – 70.

6. Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32 – 38.

7. Василиу Е.В. Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера / Е.В. Василиу, Л.Н. Василиу // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171 – 176.

8. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // Quantum Information Processing. – 2011. – V. 10, num. 2. – P. 189–202.

9. Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. — 2009, № 1. — С. 83–91.

10. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М.: Мир, 2006. – 824 с.

11. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р. – Пер. с англ. – М.: Мир, 1986. – 576 с.

12. Касами Т., Токура Н., Ивадари Ё. Теория кодирования / Т. Касами, Н. Токура, Ё. Ивадари. – М.: Мир, 1978. – 576 с.

13. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – Москва: Техносфера, 2005. – 320 с.

14. Вернер М. Основы кодирования: учебник для ВУЗов / М. Вернер. – Москва: Техносфера, 2004. – 288 с.

15. Корченко О.Г. Оцінка корегувальної здатності завадостійких трійкових РС-кодів при передачі інформації повністю переплутаними станами кутритів квантовим каналом із шумом / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий, А.М. Горчинська // Науково-технічний журнал «Захист інформації». – 2010. – №4. – С. 44–53.

16. Прескилл Дж. Квантовая информация и квантовые вычисления / Дж. Прескилл. – Т. 1. – Ижевск: "Регулярная и хаотическая динамика", 2008. – 464 с.

Надійшла: 21.07.12 р.

Рецензент: д.т.н., професор Корченко О.Г.

УДК 004.8.565.5

Терейковський І. А.

ОПТИМІЗАЦІЯ СТРУКТУРИ БАГАТОШАРОВОГО ПЕРСПЕТРОНУ В СИСТЕМАХ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

Стаття присвячена розробці методики оптимізації структури багатошарового перспетрону призначеного для використання в комп'ютерних системах захисту інформації з метою моніторингу та управління їх параметрами. Доведена доцільність використання двохшарового перспетрону. Отримано розрахункові вирази для визначення кількості нейронів у схованому шарі.

Ключові слова: захист інформації, двошаровий персептрон, нейронна мережа.

Постановка проблеми у загальному вигляді та її зв'язок із важливими практичними завданями. Одним із найбільш важливих напрямків розвитку систем захисту комп'ютерної інформації є вдосконалення математичного забезпечення підсистем моніторингу та управління. Оскільки використання явних моделей в багатьох випадках вже не приносить позитивних результатів все більшу популярність завойовують моделі які базуються на сучасних математичних теоріях, в тому числі і на теорії штучних нейронних мереж (НМ).

Використання НМ як правило полягає у застосуванні багатошарового перспетрону (БШП), призначеного для вирішення задачі розпізнавання образів. Хоча вказана нейромережева модель однозначно довела свою перспективність, але результати досліджень [3, 5] вказують на необхідність підвищення ефективності її застосування в першу чергу за рахунок оптимізації структури, що і визначає загальну проблематику даної статі.

Аналіз останніх досліджень та постановка проблеми. В загальному випадку БШП, структурна модель якого показана на рис.1, представляє собою НМ, яка складається із декількох послідовно з'єднаних між собою шарів штучних нейронів. Будемо розглядати розглядається класичний БШП у якого кожен нейрон схованого шару приймає всі вихідні сигнали попереднього шару, а його вихідний сигнал надсилається всім нейронам наступного шару.

Основними параметрами, що визначають структуру БШП являються: кількість вхідних нейронів, кількість схованих шарів нейронів, кількість нейронів у кожному схованому шарі та кількість вихідних нейронів. Базуючись на результатах [3, 4] в першому наближені можна вважати, що кількість вхідних та вихідних нейронів відповідає кількості контролюємих параметрів та кількості розпізнаваємих образів відповідно.

Дані величини задаються апріорно і не підлягають оптимізації. Тому оптимізувати структуру БШП можливо лише за рахунок кількості схованих шарів нейронів та кількості схованих нейронів. В [2, 4] наведено відповідні розрахункові вирази. Однак практичний досвід та результати [3] вказують на те, що на сьогодні теоретичні аспекти задачі визначення кількості схованих шарів та нейронів у схованому шарі вирішені далеко не повністю. Навіть в підходах до такого визначення існують деякі протиріччя. Так в [4]