На правах рукописи

Архангельская Анна Васильевна

ПОСТРОЕНИЕ ВЫСОКОСКОРОСТНЫХ КВАНТОВЫХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 05.13.19 Методы и системы защиты информации, информационная безопасность

Автореферат диссертации
на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2008

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования Московском инженерно-физическом институте (государственном университете), на кафедре «Криптология и дискретная математика».

Научный руководитель:

кандидат технических наук, доцент Петрова Тамара Васильевна

Официальные оппоненты:

доктор технических наук, профессор Хомоненко Анатолий Дмитриевич

доктор технических наук Шапошников Игорь Гаврилович

Ведущая организация: ФГУП «НИИ «Квант», г. Москва

Защита состоится «___» апреля 2008 г. в ___ часов на заседании диссертационного совета Д212.229.27 при ГОУ ВПО «Санкт-Петербургский государственный политехнический университет» (по адресу 195251, Санкт-Петербург, ул. Политехническая, д.29/1 ауд. 175 главного здания).

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан «___» марта 2008 г.

Ученый секретарь совета Платонов В.В.

Общая характеристика работы

Актуальность работы. В связи с интенсивным развитием информационных технологий все большую актуальность приобретают проблемы информационной безопасности, от качества решения которых во многом зависит успешное функционирование организаций и предприятий. В настоящее время многие средства защиты информации строятся с применением генераторов случайных чисел (ГСЧ), а вопросами их построения и исследования занимаются такие отечественные и зарубежные ученые, как А. Зубков, А. Щербаков, Д. Кнут, Б. Шнайер, Д. Келси, А. Шамир, М. Наор, О. Рейнголд, Н. Фергюсон.

В системах шифрованной связи случайным образом генерируются не только ключи абонентов, но и разовые ключи сообщений. В протоколах аутентификации, использующих хэш-функции, в протоколах взаимной аутентификации на базе сертификатов требуется использование достаточно большого объема случайных данных, а в протоколах аутентификации типа «запрос-ответ» случайные числа применяются для противодействия атакам повторной передачи. В алгоритмах электронной цифровой подписи (ЭЦП), помимо секретного ключа подписывающего требуется генерация случайного значения, используемого в качестве разового секретного ключа. Однако многие реализации средств защиты информации не имеют надежных источников действительно случайных значений, что зачастую приводит к их взлому.

В силу постоянного роста объемов обрабатываемой и передаваемой информации, подлежащей защите, и увеличения числа пользователей различных систем, в которых требуется решать задачи информационной безопасности, в том числе разграничение доступа к информации, возрастают требования к скорости генерации случайных чисел. Из-за недостатка ключевого материала в ключевых расписаниях энтропия раундовых ключей по сравнению с главным ключом уменьшается, что приводит к снижению стойкости реализации используемых криптографических алгоритмов. Решить эту проблему можно путем увеличения скорости работы ГСЧ. Еще одной причиной для повышения быстродействия ГСЧ является развитие высокоскоростных каналов передачи данных, в особенности оптоволоконных линий связи.

Скорости большинства серийно выпускаемых ГСЧ ограничены используемыми физическими явлениями, как правило, шумовыми процессами, и обычно не превышают 100 Кбит/с. Одна из причин низкого быстродействия заключается в том, что в известных схемах генерации случайных чисел используются события с бинарными характеристиками. Многие ГСЧ основаны на аналоговых событиях, например, шумах в электронных устройствах, преобразованных методом квантования в двоичные значения по определенному порогу, либо на квантовых дискретных событиях: пролете фотона через поляризатор или его поглощение и т.п. Большего быстродействия можно достичь при использовании небинарных последовательностей, характеризующих квантовые процессы.

В этих условиях актуальной является задача разработки и анализа высокоскоростного ГСЧ, основанного на источнике случайных событий (ИСС), состоящем из источника квантового процесса и измерителя его интенсивности, характеризующейся небинарными величинами, и методов анализа свойств указанного ИСС. Построение такого ГСЧ позволит повысить стойкость реализации известных механизмов защиты информации, например, алгоритмов аутентификации и ЭЦП.

Целью диссертационной работы является повышение стойкости механизмов защиты информации за счет разработки и использования метода построения высокоскоростного ГСЧ, основанного на квантовом процессе. Для увеличения скорости выработки случайных чисел предлагается использовать новый класс ИСС, выходные последовательности которых являются небинарными. Такие ИСС могут быть основаны на квантовых процессах, возникающих, например, при излучении фотонов источником света слабой интенсивности и их регистрации.

В соответствии с поставленной целью в диссертационной работе решаются следующие задачи:

- анализ существующих методов построения ГСЧ;
- обоснование использования небинарных последовательностей для построения высокоскоростных ГСЧ;
- выбор физического процесса, характеризующегося недвоичной величиной, который может быть использован для генерации случайных чисел, и разработка основанного на нем ИСС;
- разработка модели ГСЧ, основанных на квантовых событиях, использующих в качестве ИСС световой поток слабой интенсивности, измеряемой фотоэлектронным умножителем (ФЭУ);
- исследование существующих методов статистического тестирования ГСЧ и разработка методики тестирования небинарных последовательностей;
- разработка ГСЧ, соответствующего предложенной модели, анализ его характеристик и выработка рекомендаций по его практическому применению.

Основными методами исследований, используемыми в работе, являются методы комбинаторики, теории вероятностей, математической статистики, теории информации и криптологии.

Научная новизна работы заключается в следующем:

- разработан подход к построению высокоскоростных ГСЧ на основе небинарных последовательностей;
- предложен новый тип ИСС, основанных на квантовом процессе и измерителе его интенсивности;
- предложен класс ГСЧ, основанный на разработанном ИСС, выходные величины которого являются недвоичными;

• разработана методика статистического тестирования ИСС и ГСЧ, применимая к недвоичным последовательностям, основанная на проверке гипотезы независимости случайных величин, соответствующих элементам последовательностей, и методе отбеливания фон Неймана.

По тематике работы подана заявка на изобретение № 2007123264 от 21.06.2007.

Практическую ценность представляют:

• методика тестирования выходных последовательностей ИСС и ГСЧ, позволяющая исследовать недвоичные последовательности, и ее программная реализация;

• действующий макет ГСЧ, основанный на небинарном ИСС, позволяющий осуществлять генерацию статистически независимых последовательностей с высокой скоростью;

• рекомендации по практическому применению разработанного класса ГСЧ и выбору их параметров.

Результаты работы представляют практическую ценность для обеспечения различных аспектов безопасности информации, в первую очередь, конфиденциальности и целостности, позволяют усовершенствовать системы распределения ключей, протоколы аутентификации и схемы ЭЦП.

Внедрение результатов исследований. Основные результаты исследований используются в ЗАО «Голлард» при проектировании защищенных систем обработки информации. Результаты диссертационной работы внедрены в учебный процесс на факультете «Информационная безопасность» Московского инженерно-физического института (государственного университета).

Публикации и апробация работы. По теме диссертации опубликовано 17 печатных работ, в том числе 6 научных статей, из них 5 в изданиях, включенных в Перечень ведущих рецензируемых научных журналов, и 11 тезисов докладов. Результаты работы докладывались на Российской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (С.-Петербург, 2004 – 2007 гг.), на Всероссийской научно-практической конференции «Проблемы информационной безопасности государства, общества и личности» (Томск, 2005 г.), Международной научно-практической конференции «Информационная безопасность» (Таганрог, 2005 г.), Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы» (Москва, 2005 – 2007 гг.), Международной конференции «Комплексная защита информации» (Суздаль, 2006 г.), Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT'06 (Шушенское, 2006 г.) и SIBECRYPT'07 (Горно-Алтайск, 2007 г.). Работа поддержана грантом Министерства образования и науки РФ

в рамках ведомственной научной программы «Развитие научного потенциала высшей школы» (2005 г.).

Основные положения, выносимые на защиту:

- подход к построению высокоскоростных ГСЧ, основанный на применении небинарных последовательностей;
- структура ИСС, содержащего источник элементарных частиц слабой интенсивности и приемник частиц, позволяющий получать мгновенную аналоговую характеристику квантовых явлений, пропорциональную количеству зарегистрированных частиц;
- модель высокоскоростного ГСЧ, основанного на разработанном ИСС, выходы которого являются недвоичными величинами;
- методика статистического тестирования недвоичных последовательностей, позволяющая исследовать свойства ИСС, основанных на процессах, характеризующихся многозначными величинами, например, интенсивностью физического процесса;
- рекомендации по выбору параметров ИСС и ГСЧ, основанных на квантовых событиях.

Структура работы. Работа состоит из введения, пяти глав, заключения, списка литературы, включающего 238 наименований, и одиннадцати приложений.

Содержание работы

Во введении обосновывается актуальность темы диссертации, выделяются и формулируются цели и задачи исследования, описывается структурно-логическая схема диссертационной работы.

В первой главе приводится обзор современных ГСЧ, исследуются и уточняются методы и пути решения поставленной научной задачи.

В работе проанализирован ряд известных ГСЧ, среди которых генераторы, описанные в стандарте ANSI X9.17 и в американском стандарте на цифровую подпись DSS, и ГСЧ, основанные на квантовых процессах. На основании сравнения рассмотренных ГСЧ по таким показателям, как быстродействие, физический процесс, лежащий в основе ИСС, и энтропия случайной величины, соответствующей выходному значению генератора, сделан вывод о перспективности построения ГСЧ, основанных на квантовых событиях. Однако в существующих подходах применяются однофотонные явления, характеризующиеся двоичной величиной, что не позволяет достичь удовлетворяющей современным требованиям скорости выработки случайных чисел. В силу свойств физических процессов, использующихся в ИСС, существенного увеличения скорости генерации случайных чисел можно добиться

только при помощи небинарных последовательностей или при увеличении частоты отсчетов ИСС, чему и посвящена настоящая работа.

Для изучения свойств ГСЧ предлагается использовать следующую схему, общую для всех генераторов: к выходам ИСС $a_1,\ldots, a_n$ применяется некоторое преобразование, в результате чего получается последовательность случайных чисел $b_1,\ldots, b_m$ (рисунок 1), причем длина результирующей последовательности не обязательно должна равняться длине исходной последовательности.

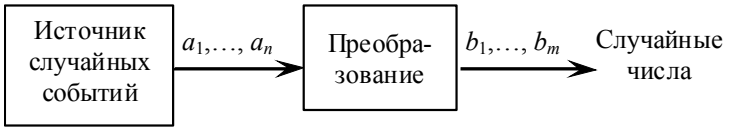

Рисунок 1 – Обобщенная схема ГСЧ

Недетерминированность в работу ГСЧ вносится за счет ИСС, т.е. физического источника сигналов, выходы которого являются случайными сами по себе, к которым, как правило, с целью улучшения статистических характеристик применяется криптографическое преобразование.

В настоящее время существует множество подходов к построению ИСС. Большинство из них используют временные характеристики процессов, происходящих в компьютере, или основаны на физическом явлении, которое само по себе обладает некоторой непредсказуемостью, например, испускание элементарных частиц радиоактивным веществом или неустойчивые колебания. Также существуют методы получения случайных чисел с использованием квантовомеханических процессов в полупроводниковых устройствах или квантовых явлений, таких как пролет фотонов через полупрозрачное зеркало. Однако эти методы не позволяют получить скорость генерации случайных чисел, достаточную для современных приложений.

Основной задачей, возникающей при построении ГСЧ, являющихся компонентами средств защиты информации, и решаемой в настоящей диссертационной работе, является не только выработка выходных последовательностей, удовлетворяющих некоторому набору статистических тестов, но и обеспечение высокой скорости генерации случайных чисел. Для увеличения энтропии каждого отсчета ИСС в целях повышения скорости генерации случайных чисел целесообразно выбрать физический процесс, имеющий небинарную характеристику интенсивности. Однако в этом случае требуется разработка методики статистического тестирования, применимой к недвоичным последовательностям, т.к. существующие статистические тесты, специально предназначенные для анализа ГСЧ, оперируют только с бинарными последовательностями.

Вторая глава посвящена исследованию методов построения ГСЧ, обоснованию требований, предъявляемых к ним, разработке структуры ИСС и обоснованию выбора физического процесса, положенного в его основу.

Существующие ГСЧ, как правило, построены с использованием одной из двух схем. Первая схема основана на предположении о получении достаточного количества случайных данных на выходе ИСС так, чтобы каждому

из выходных битов соответствовал один бит «истинно» случайных данных. Во второй схеме к выходам ИСС для улучшения свойств его выходных последовательностей применяются некоторые криптографические преобразования, например, блочные или поточные шифры, т.е. схема основана на предположении о возможности накопления достаточного количества случайных данных для перевода ГСЧ в состояние, которое невозможно предсказать иным, кроме угадывания, способом. Таким образом, если однажды состояние ГСЧ было заведомо неизвестно криптоаналитику, то при условии предсказуемости всех остальных накопленных случайных данных или вмешательства криптоаналитика в их генерацию, ГСЧ остается по-прежнему безопасным. Предлагаемый в работе класс ГСЧ строится с использованием второй схемы.

При разработке ГСЧ должны быть определены требования к основным компонентам генератора и к ГСЧ в целом. В диссертационной работе обоснованы требования к накопителю случайных событий, блоку обновления, блоку генерации и блоку управления обновлением состояния ГСЧ. Основными требованиями, которым должен удовлетворять разрабатываемый ГСЧ, являются следующие:

- статистическая независимость случайных величин, реализациями которых являются элементы последовательностей, вырабатываемых ИСС и ГСЧ;
- прохождение определенного набора статистических тестов выходными последовательностями ИСС и ГСЧ и высокая энтропия случайных величин, соответствующих их элементам;
- высокая скорость генерации случайных чисел, превышающая быстродействие известных ГСЧ.

В работе обоснована целесообразность использования в блоке генерации схемы, позволяющей управлять изменениями состояния, так называемого затвора генератора, обеспечивающего стойкость ГСЧ к компрометации состояния. Рассмотрен способ, при помощи которого криптоаналитик может предсказывать следующее состояние, сгенерированное блоком затвора генератора, основанный на наличии повторов значений случайных величин, описываемых парадоксом дней рождений. Вероятность хотя бы одного повтора среди m выбранных чисел из n возможных оценивается следующим образом:

$$P(n,m) \approx 1 - e^{-\frac{m(m-1)}{2n}} + r(n,m), \text{ где } |r(n,m)| < \frac{m^3}{6(n-m+1)^2}.$$

С использованием указанных формул получена верхняя оценка частоты срабатывания затвора генератора, равная $2^{n/3}$, где n – размер блока шифра, применяющегося для улучшения статистических свойств выходных последовательностей ГСЧ.

Впервые предложена схема ИСС (рисунок 2), в которой используются групповые квантовые события, а на выходе получаются независимые недвоичные реализации случайной величины - интенсивности квантового процесса. ИСС состоит из источника элементарных частиц слабой интенсивности, детектора частиц – высокочувствительного кремниевого ФЭУ, позволяюще-

го получать мгновенное аналоговое значение, пропорциональное количеству зарегистрированных частиц, и аналого-цифрового преобразователя (АЦП).

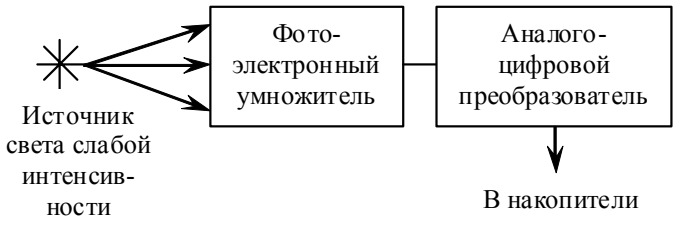

Рисунок 2 – Схема ИСС

С использованием предложенного ИСС разработан новый класс ГСЧ (рисунок 3), в основу которого положен подход, связанный с накоплением случайных данных. Отличие данного ГСЧ от известных методов генерации случайных чисел заключается в использовании в качестве выхода ИСС некоррелированной последовательности небинарных величин.

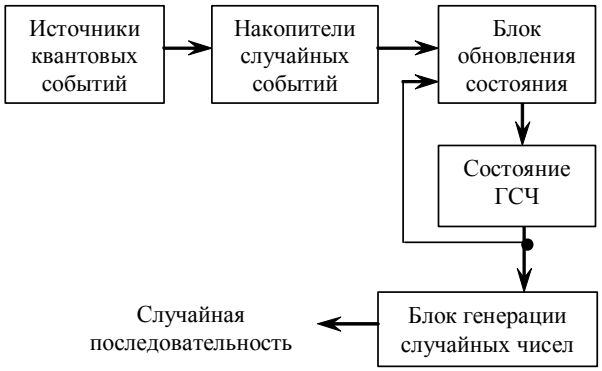

Рисунок 3 – Структура ГСЧ, основанного на источнике квантовых событий

Для повышения быстродействия ГСЧ целесообразно увеличить частоту получения случайных событий, что в пороговых схемах, широко используемых при построении ГСЧ, представляется сложным. С ростом частоты измерения характеристик аналоговых событий соседние отсчеты оказываются зависимыми и энтропия ИСС увеличивается слабо. В указанных целях в разработанном ГСЧ использован источник квантовых событий и измерительное устройство, позволяющие получить многозначные величины, характеризующие происходящие события. Для приведения полученной недвоичной выходной последовательности ИСС к двоичному виду и сглаживания статистических характеристик источника используется криптографическое преобразование, например, хэш-функция или свертка, основанная на алгоритме шифрования.

ИСС предложенного класса ГСЧ имеют следующие преимущества по сравнению с используемыми в существующих реализациях ГСЧ:

- не требуется знать характер и параметры распределения случайной величины – выхода ИСС, важна только независимость его отсчетов, что существенно упрощает анализ ИСС;
- в отличие от традиционных ИСС, которые порождают поток равновероятных двоичных цифр, выходом ИСС является количественная оценка интенсивности квантового явления, что увеличивает энтропию отсчета ИСС и, следовательно, скорость генерации случайных чисел.

Поскольку выходная величина ИСС принимает сотни различных значений, каждый отсчет имеет энтропию значительно больше единицы, что существенно превышает значения для традиционных пороговых источников. Именно это свойство позволяет говорить о существенном повышении скорости генерации случайных чисел. В силу использования квантовых событий числовые значения характеристики явления распределены практически неза-

висимо, что следует из физических особенностей квантового процесса и подтверждается экспериментальным исследованием статистических характеристик вырабатываемых последовательностей.

Схема квантового процесса, положенного в основу ИСС, приведена на рисунке 4, где $I_{ест.}$ – интенсивность естественного света, а φ – угол между плоскостями поляризаторов.

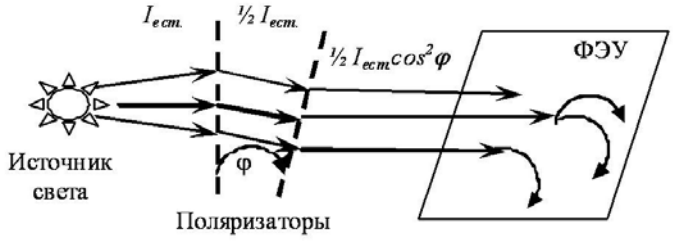

Рисунок 4 - Схема применяемого в ИСС квантового процесса

Световой поток должен быть таким, чтобы ФЭУ не попадал в область насыщения, поэтому испускаемый свет должен быть пропущен через систему поляризаторов. Если поставить на пути естественного два поляризатора, то из первого поляризатора выйдет плоскополяризованный свет, интенсивность которого равна $I_0 = ½\ I_{ест.}$. Тогда в соответствии с законом Малюса из второго поляризатора выйдет свет интенсивности $I_0 \cos^2\varphi$. Таким образом, интенсивность света, прошедшего через два поляризатора равна $½\ I_{ест.} \cos^2\varphi$. Переходя от интегральной оценки – интенсивности, к поведению отдельного произвольно поляризованного фотона, получаем, что вероятность его прохождения через описанную систему из двух поляризаторов равна $½ \cos^2\varphi$. Из результатов, полученных в квантовой физике, известно, что процесс порождения вторичных фотоэлектронов, происходящий при попадании фотона на ФЭУ, является случайным. Эти факты позволяют говорить о вероятностном характере квантового процесса, положенного в основу ИСС.

Для квантового процесса, на котором основан ИСС, построена вероятностная схема и определена вероятность p_c того, что при испускании источником света n фотонов ФЭУ размерности k зарегистрирует c из них:

$$p_c = \frac{1}{2^n}\binom{k}{k-c}\sum_{r=c}^{n}\frac{\binom{n}{r}\binom{r-1}{c-1}}{\binom{k+r-1}{r}}\cos^{2r}\varphi(2-\cos^2\varphi)^{n-r}\ .$$

В третьей главе рассматриваются задачи разработки методики исследования ГСЧ и построения статистических тестов, применимых к недвоичным последовательностям.

Проведенный в работе анализ существующих статистических тестов, предназначенных для исследования ГСЧ, показал, что все они применимы только к двоичным последовательностям. Поэтому использование небинарного ИСС требует разработки методики тестирования недвоичных последовательностей. Предложенная в работе методика направлена на проверку наиболее важного показателя качества ГСЧ – непредсказуемости получаемых

значений, позволяет исследовать как ГСЧ, так и положенные в их основу ИСС, вырабатывающие недвоичные величины, и решает задачу обобщения методов статистического тестирования последовательностей на случай более сложных распределений, отличных от равномерного. ГСЧ, успешно протестированные при помощи предложенной методики, удовлетворяют основному требованию, предъявляемому к современным ГСЧ – случайные величины, реализациями которых являются элементы последовательностей, вырабатываемых ИСС и ГСЧ, статистически независимы.

Оценка энтропии случайных величин, полученных при помощи ИСС, позволяет прогнозировать статистические свойства вырабатываемых случайных чисел и оценивать быстродействие ГСЧ. Применительно к независимым испытаниям случайной величины ξ с известным распределением вероятностей энтропия $H(\xi)$ определяется формулой

$$\xi = \begin{pmatrix} a_1 \ldots a_n \\ p_1 \ldots p_n \end{pmatrix}, \; H(\xi) = -\sum_{i=1}^{n} p_i \log_2 p_i .$$

Для применения данного выражения, необходимо проверить гипотезу о независимости вырабатываемых ИСС значений.

В предложенной методике статистического тестирования недвоичных последовательностей предлагается вначале проверить необходимое условие независимости их элементов. Для этого рассматриваются две случайные величины ξ и η, которые соответствуют нечетным и четным элементам выходной последовательности соответственно, и для них рассчитывается значение коэффициента корреляции:

$$\rho(\xi, \eta) = \frac{E(\xi, \eta) - E\xi \cdot E\eta}{D\xi \cdot D\eta},$$

где $E\xi$, $E\eta$ – математические ожидания случайных величин ξ и η соответственно; $E(\xi, \eta)$ – математическое ожидание пары ξ и η; $D\xi$, $D\eta$ – дисперсии ξ и η соответственно. Таким образом проверяется, связаны ли исследуемые случайные величины связаны линейной зависимостью или нет.

Для дальнейшей проверки независимости предлагается воспользоваться критерием согласия χ^2:

$$\chi^2 = \sum_{i=1}^{n} \frac{(f_i - e_i)^2}{e_i},$$

где n – количество различных значений, принимаемых случайной величиной, f_i – частота появления значения с номером i, e_i – ожидаемая частота.

Поскольку совместное выборочное распределение f_i является полиномиальным порядка n с индексом $k = \sum_{i=1}^{n} f_i$ и с вероятностями $p_1, p_2, \ldots, p_n$, где p_i – вероятность того, что наблюдаемая случайная величина будет равна i, $i = \overline{1, n}$, ожидаемая частота рассчитывается по формуле:

$$e_i = kp_i.$$

В исследуемой задаче при распределениях вероятностей случайных величин ξ и η

$$\xi = \begin{pmatrix} a_1 \ldots a_s \\ p_1^1 \ldots p_s^1 \end{pmatrix},\ \eta = \begin{pmatrix} b_1 \ldots b_t \\ p_1^2 \ldots p_t^2 \end{pmatrix}$$

статистика χ^2 имеет следующий вид:

$$\chi^2 = \sum_{k=1}^{s} \sum_{l=1}^{t} \frac{\left(\frac{p_k^1 p_l^2}{N} - p_{k,l} \right)^2}{\frac{p_k^1 p_l^2}{N}},$$

где N – количество элементов в выборках и $p_{k,l}$ – вероятность совместного события.

Полученные значения статистики необходимо сравнить с квантилями распределения χ^2 и сделать вывод о независимости отсчетов, если значения не превышают соответствующие квантили.

Для проверки независимости случайных величин ξ и η, соответствующих четным и нечетным элементам выходной последовательности ИСС, также предлагается оценить их условную энтропию:

$$H(\xi|\eta) = -\sum_{i=1}^{t} p_i^2 \sum_{j=1}^{s} p(a_j|b_i) \log_2 p(a_j|b_i),$$

где $p(a_j|b_i)$ – условная вероятность того, что случайная величина ξ приняла значение a_j при условии, что случайная величина η приняла значение b_i. Вывод о независимости величин ξ и η может быть сделать в случае, если $H(\xi|\eta) = H(\xi)$.

Для дополнительной проверки гипотезы о независимости элементов недвоичных последовательностей предлагается использовать следующий метод, обобщающий существующие статистические тесты на случай распределения, отличного от равномерного.

1. Найти пороговое значение, при котором эмпирическая функция распределения принимает значение, максимально близкое к 0.5.

2. Числам, превышающим указанное пороговое значение, поставить в соответствие единицу, а остальным – ноль.

3. Применить метод отбеливания фон Неймана для получения равномерного распределения.

4. Сформированные массивы и их подпоследовательности подвергнуть статистическим тестам, используемым для оценки двоичных ГСЧ, например, NIST STS, DIEHARD. Вывод о качестве последовательности следует делать в соответствии с методикой применяемых тестов.

Данный метод применим только в том случае, когда элементы исследуемой последовательности являются независимыми. При использовании метода фон Неймана объем исходного материала сокращается в 4 раза, но он позволяет исследовать собственные свойства последовательности, не подвергнутой каким-либо преобразованиям, которые, как правило, применяются

к выходным значениям ИСС, и могут существенно исказить полученные результаты.

Предложенная методика статистического тестирования недвоичных последовательностей реализована в виде программного комплекса, позволяющего автоматизировать обработку и исследование больших объемов данных, что особенно важно при высокой скорости работы ИСС и ГСЧ.

В четвертой главе рассматриваются вопросы, связанные с получением и анализом таких характеристик разработанного ГСЧ, как независимость случайных величин, соответствующих различным отсчетам ИСС, их коэффициентов корреляции и энтропии отсчета.

Проведены эксперименты с импульсным лазером и постоянно включенным светодиодом, в каждом эксперименте получено и проанализировано порядка 10^6 отсчетов. Распределение случайных величин, соответствующих отсчетам ИСС, для различных источников света приведено на рисунке 5.

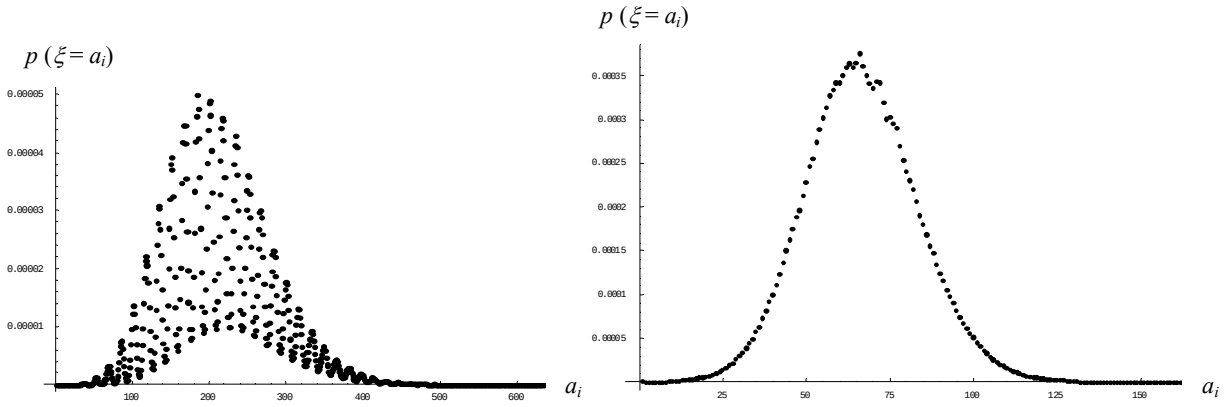

Рисунок 5 – Эмпирические распределения вероятностей случайных величин, соответствующих числу зарегистрированных ФЭУ фотонов, для лазера и светодиода

Поскольку качество ГСЧ, используемых в средствах защиты информации, определяется статистическими характеристиками вырабатываемых последовательностей, в процессе исследования ИСС проверена гипотеза о непредсказуемости выходных значений, результирующие последовательности подвергнуты тестам на независимость и оценена их энтропия.

Значения статистики χ^2, использованной для проверки гипотезы о независимости соседних пар отсчетов ИСС, приведены в таблице 1.

Таблица 1 – Значения статистики χ^2

	Лазер			**Светодиод**
	Среднее на отсчет количество испускаемых фотонов			
	3	10	30	
χ^2	3.7	1.0	1.1	2.5
Количество степеней свободы	30	29	28	30

При сравнении полученных значений статистики с квантилями распределения χ^2 получаем, что гипотезы о независимости исследуемых случайных величин принимаются при уровне значимости $\alpha = 0.001$.

Поскольку гипотеза о независимости отсчетов не отвергается, определена энтропия выходных значений ИСС, значений которой приведены в таблице 2.

Таблица 2 – Оценка значения энтропии

	Лазер			**Светодиод**
	Среднее на отсчет количество испускаемых фотонов			
	3	10	30	
$H(\xi)$**, бит**	6.8	7.9	8.5	6.1

Полученные значения энтропии отсчета предложенного ИСС согласуются с теоретическими оценками энтропии случайной величины, равной количеству зарегистрированных ФЭУ фотонов, для вероятностной схемы, построенной во второй главе работы.

Проведенная экспериментальная проверка предложенных принципов построения высокоскоростных ГСЧ подтверждает обоснованную в работе независимость элементов выходных последовательностей разработанного ИСС, что позволяет использовать его при построении высокоскоростных ГСЧ, применяющихся в средствах защиты информации.

В пятой главе описываются результаты практического применения предложенного в работе ГСЧ для решения прикладных задач, приводятся параметры компонентов ГСЧ, обеспечивающие большие значения энтропии выходной последовательности и вследствие этого более высокую скорость генерации случайных чисел.

Поскольку случайные величины, соответствующие значениям интенсивности физического процесса, положенного в основу разработанного ИСС, обладают энтропией, превышающей энтропию отсчета существующих ИСС при требуемой скорости генерации случайных чисел, возможно снизить частоту отсчетов приемника частиц, и тем самым обеспечить независимость отсчетов, нарушающуюся на больших частотах. Этот подход позволяет решить поставленную в работе задачу с приемлемыми экономическими характеристиками, т.к. снижение скважности наблюдения, приводит к уменьшению частоты дискретизации АЦП и частоты работы измерителя интенсивности процесса, что снижает их стоимость.

Проведенные эксперименты показывают, что при частоте отсчетов 10 МГц случайные величины, соответствующие элементам выходной последовательности ИСС, являются независимыми и их энтропия принимает значения от 6 до 8 бит. Поскольку быстродействие предложенного класса ГСЧ пропорционально частоте отсчетов приемника элементарных частиц и энтропии случайной величины, соответствующей указанным отсчетам, полученные данные позволяют вычислить скорость генерации случайных чисел, которую можно достичь, применяя разработанный ИСС. При использовании группового квантового события малой интенсивности, характеризующегося целочисленной недвоичной величиной, скорость генерации случайных чисел принимает значения в диапазоне от $6 \cdot 10^8$ до $8 \cdot 10^8$ бит/с, что на два порядка превышает показатели современных ГСЧ.

Для обеспечения указанных характеристик ГСЧ и ИСС необходимо использовать источник света такой, что количество фотонов, достигающих ФЭУ, приблизительно в два раза превышает его размерность, и ФЭУ, позволяющий измерять интенсивность светового потока каждые 10 нс.

Полученные в работе результаты позволяют построить и применять на практике ключевые расписания, которые, в отличие от существующих, не уменьшают энтропию раундовых ключей по сравнению с главным ключом, что, способствует повышению стойкости реализации алгоритмов защиты информации.

В результате диссертационных исследований:

1. Предложен и обоснован подход к построению высокоскоростных ГСЧ на основе физических процессов, характеризующихся небинарной величиной. В качестве указанного процесса предлагается использовать излучение и регистрацию фотонов.

2. Предложена структура ИСС, основанного на выбранном физическом процессе, состоящего из источника элементарных частиц слабой интенсивности, приемника частиц, имеющего квантовую природу и позволяющего получать мгновенную аналоговую характеристику квантовых явлений, и АЦП.

3. Разработана модель ГСЧ на основе предлагаемого ИСС, рассматривающая процесс как с позиций квантовой физики, так и при помощи описание его вероятностной схемы.

4. Разработана методика статистического тестирования недвоичных последовательностей, позволяющая исследовать свойства предложенного ИСС, основанная на проверке гипотезы независимости случайных величин, соответствующих отсчетам измерителя интенсивности квантовых событий, и методе отбеливания фон Неймана.

5. Реализован опытный образец ГСЧ, оценены его основные характеристики, в частности скорость, которая на два порядка превышает показатели современных генераторов.

6. Составлены и обоснованы рекомендации по выбору параметров ИСС и ГСЧ, основанных на квантовых событиях, включающие в себя требования к используемому источнику элементарных частиц, ФЭУ и АЦП.

Основные результаты диссертации изложены в 17 печатных работах:

1. Архангельская, А.В. Некоторые аспекты разработки генераторов случайных чисел / А.В. Архангельская // Безопасность информационных технологий. – 2004. – № 3. – С. 45 – 48. – Библиогр.: с. 48. (перечень ВАК).

2. **Архангельская, А.В.** Об одном подходе к построению генератора случайных чисел / А.В. Архангельская // Методы и технические средства обеспечения безопасности информации. Материалы XIII Общероссийской научно-технической конференции: сб. науч. тр. / Санкт-Петербургский государственный политехнический университет. – СПб., 2004. – С. 51. – Библиогр.: с. 51.

3. Архангельская, А.В. О статистическом тестировании источников случайности, применяемых для построения генераторов случайных чисел / А.В. Архангель-

ская // Безопасность информационных технологий. – 2005. – № 2. – С. 21 – 27. – Библиогр.: с. 27. (перечень ВАК).

4. Архангельская, А.В. Обзор и анализ современных генераторов случайных и псевдослучайных чисел / А.В. Архангельская // Безопасность информационных технологий. – 2005. – № 4. – С. 31 – 39. – Библиогр.: с. 39. (перечень ВАК).

5. **Архангельская, А.В.** О разработке генератора случайных чисел, основанного на квантовых эффектах / А.В. Архангельская // Проблемы информационной безопасности государства, общества и личности: Материалы Седьмой Всероссийской и научно-практической конференции: сб. науч. тр. / Института оптики атмосферы СО РАН. – Томск, 2005. – С. 186 – 188. – Библиогр.: с. 188.

6. **Архангельская, А.В.** О выборе параметров генератора случайных чисел, основанного на схеме с затвором / А.В. Архангельская // Материалы VII Международной научно-практической конференции «Информационная безопасность»: сб. науч. тр. / Таганрогский технологический институт. – Таганрог, 2005. – С. 191 – 194. – Библиогр.: с. 194.

7. **Архангельская, А.В.** Об одном методе тестирования генераторов недвоичных случайных чисел / А.В. Архангельская // Методы и технические средства обеспечения безопасности информации. Материалы XIV Общероссийской научно-технической конференции: сб. науч. тр. / Санкт-Петербургский государственный политехнический университет. – СПб., 2005. – С. 54. – Библиогр.: с. 54.

8. **Архангельская, А.В.** Об одном подходе к определению понятий генераторов случайных и псевдослучайных чисел / А.В. Архангельская // Научная сессия МИФИ-2006. XIII Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы»: сб. науч. тр. / Московский инженерно-физический институт (государственный университет). – М., 2006. – С. 14 – 15. – Библиогр.: с. 15.

9. Архангельская, А.В. Об исследовании статистических характеристик квантового источника случайности / А.В. Архангельская // Вестник ТГУ. Приложение. – 2006. – № 17. – С. 276 – 279. – Библиогр.: с. 279. (перечень ВАК).

10. **Архангельская, А.В.** О компонентах генераторов случайных чисел, используемых в криптографических приложениях, и требованиях к ним / А.В. Архангельская // X Международная конференция «Комплексная защита информации»: сб. науч. тр. / Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации. – Минск: «Амалфея», 2006. – С. 204 – 206. – Библиогр.: с. 206.

11. **Архангельская, А.В.** Анализ методов построения генераторов случайных чисел / А.В. Архангельская // Методы и технические средства обеспечения безопасности информации. Материалы XV Общероссийской научно-технической конференции: сб. науч. тр. / Санкт-Петербургский государственный политехнический университет. – СПб., 2006. – С. 68. – Библиогр.: с. 68.

12. Архангельская, А.В., Запечников С.В. Способ вычисления псевдослучайных функций с распределенным секретным ключом / А.В. Архангельская, С.В. Запечников // Безопасность информационных технологий. – 2006. – № 3. – С. 44 – 49. – Библиогр.: с. 49. (перечень ВАК).

13. **Архангельская, А.В.** Анализ подходов к определению термина «случайность» / А.В. Архангельская // Научная сессия МИФИ-2007. XIV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы»: сб. науч. тр. / Московский инженерно-физический институт (государственный университет). – М., 2007. – С. 22 – 23. – Библиогр.: с. 23.

14. **Архангельская, А.В., Запечников, С.В.** Криптографические генераторы псевдослучайных чисел с распределенным секретным ключом / А.В. Архангельская, С.В. Запечников // Научная сессия МИФИ-2007. XIV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы»: сб. науч. тр. / Мо-

сковский инженерно-физический институт (государственный университет). – М., 2007. – С. 24 – 25. – Библиогр.: с. 25.

15. **Архангельская, А.В., Запечников, С.В.** Протокол дистанционного управления ключами псевдослучайного генератора / А.В. Архангельская, С.В. Запечников // Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2007», посвященной 45-летию ТУСУРа: сб. науч. тр. / Томский государственный университет систем управления и радиоэлектроники. – Томск: Издательство «В-Спектр», 2007. – Ч.2. – С.213 – 216. – Библиогр.: с. 216.

16. **Архангельская, А.В., Архангельский, В.Г.** Архитектура генератора случайных чисел, основанного на квантовых событиях / А.В. Архангельская, В.Г. Архангельский // Методы и технические средства обеспечения безопасности информации: Материалы XVI Общероссийской научно-технической конференции: сб. науч. тр. / Санкт-Петербургский государственный политехнический университет. – СПб., 2007. – С. 60. – Библиогр.: с. 60.

17. **Архангельская, А.В.** О применении схемы с затвором для генерации случайных чисел / А.В. Архангельская // Вестник ТГУ. Приложение. – 2007. – № 23. – С. 100 – 103. – Библиогр.: с. 103.

Подписано в печать 11 марта 2008 г.
Формат 60х90 $\frac{1}{16}$. Объем 1 печ. л. Тираж 100 экз.

Отпечатано в Печатном салоне «ОТТИСК»
101000, г. Москва, ул. Мясницкая, д. 17