Всероссийская научно-техническая конференция, посвященная 100-летию со дня рождения одного из основоположников советской вычислительной техники Б.И. Рамеева, на тему: «Информационно-управляющие и телекоммуникационные системы специального назначения». Секция «Биометрическая поддержка криптовалют, блокчейн реестров, облачных сервисов», проводится в конференц-зале Технопарка высоких технологий «Рамеев», доклад 16 мая 2018 года с $11^{30}$ до $11^{45}$ (ул. Центральная, д. 1), г. Пенза.

Безяев А.В.

# Нейросетевая молекула: механизм направленной квантовой коррекции большого числа ошибок длинного кода высокоразмерных биометрических образов

Аннотация.

*Актуальность и цели.* Целью работы является создание высокоэффективных механизмов корректировки большого числа ошибок в длинных выходных кодах нейросетевых преобразователей.

*Материалы и методы.* Классические коды с обнаружением и исправлением ошибок не могут корректировать более 10% ошибок. Предложено нейросетевой преобразователь биометрии рассматривать как нейросетевую молекулу и поддерживать для нее режим нейродинамики за счет добавления на ее входы белого шума. В режиме нейродинамики предложено контролировать показатели стабильности каждого из 256 кубит выходного кода. Предложено ускорить подбор верного кодового состояния за счет корректировки наиболее нестабильных разрядов кода.

*Результаты.* Наблюдается многократное сокращение времени корректировки ошибочных разрядов длинных кодов за счет замены полного просмотра всех возможных состояний фрагментов кода, на направленный перебор состояний, начиная с наиболее слабых разрядов кода.

*Выводы.* Моделирование уравнений Шредингера на обычном компьютере имеет экспоненциальную вычислительную сложность по отношению к числу степеней свободы. По этой причине создание квантовых корректоров ошибок даже для кодов длинной в 30 бит через моделирование уравнений Шредингера технически невозможно. Для реализации квантовых вычислений в рамках квантовой механики придется ждать появления новой элементной базы, охлаждаемой жидким гелием. Однако, если мы переходим в квантовую нейродинамику, то положение меняется. Моделирование искусственных нейронов имеет линейную вычислительную сложность и легко может быть воспроизведено на обычных вычислительных машинах.

Ключевые слова: искусственные нейронные сети, корректировка ошибок длинных кодов, поддержка квантовой суперпозиции, стабильность состояний разрядов корректируемых кодов.

## Необходимость корректировки ошибок в кодах, получаемых из биометрических данных

Информатизация современного общества приводят к необходимости расширения применения криптографии. Обычные люди не могут запоминать длинные пароли доступа и криптографические ключи. Для решения этой проблемы в США и Евросоюзе развиваются технологии «нечетких экстракторов» [1, 2, 3], построенных на корректировке ошибок классическими кодами с обнаружением и исправлением ошибок. При этом выходной код «нечетких экстракторов» является коротким из-за того, что классические коды с приемлемой избыточностью в 50% способны корректировать не более 5% ошибок [4, 5]. Ошибки исходных кодов «нечетких экстракторов» могут составлять от 20% до 30% от длины кода, что заставляет использовать самокорректирующиеся коды с 20-ти кратной избыточностью. То есть длина выходного кода «нечеткого экстрактора» оказывается в 20

раз меньше, чем число биометрических параметров, из которых «нечеткий экстрактор» восстанавливает код ключа.

В России развивается технология нейросетевого преобразования биометрии в длинный код доступа или длинный код личного криптографического ключа [5, 6]. Нейросетевые преобразователи биометрия-код, выполненные в соответствии с пакетом стандартов ГОСТ Р 52633.xx [7, 8], обучаются на выборках порядка 20 примеров образа «Свой». При этом вероятность ошибок первого рода (отказ в доступе «Своему») составляет от 0.05 до 0.1. Для снижения вероятности ошибок первого рода необходимо либо увеличивать число примеров в обучающей выборке, либо осуществлять коррекцию ошибок. Для нейросетевых преобразователей биометрия-код нет проблемы коротких выходных кодов так как за один разряд кода отвечает один нейрон, а число нейронов выбирает разработчик биометрического средства защиты информации. Тем не менее, выходные коды нейросетевых преобразователей нуждаются в корректировке.

**Корректирующие коды, безопасно хранящие информацию о синдромах ошибок в коротких фрагментах хэш-функций**

В биометрических кодах может содержаться до до10-:15 ошибок, если строить коды, способные обнаруживать до 16 ошибок, то весь код следует разбить на 16 фрагментов по 16 бит. Структурная схема хэш-корректора приведена на рисунке 1.

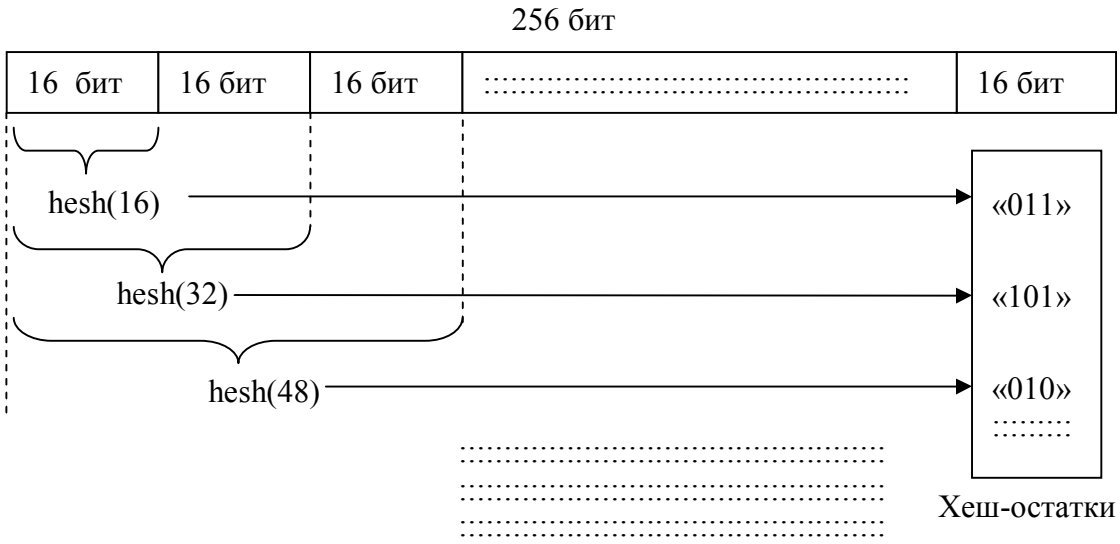


Рис. 1. Безопасная схема рекурсивного формирования эталонных хеш-остатков

Корректирующий код построен на том, что защищаемая последовательность в 256 бит делится на 16 фрагмента по 16 бит. Для верного состояния защищаемого кода вычисляются хеш-функции для 16, 32, 48,…., 256 бит. Три бита каждой хеш-функции запоминают в таблицу хеш-остатков, например, это могут быть последние 3 бита каждой из хеш-функций.

Такой код способен корректировать до трех ошибок в каждом из выделенных 16 фрагментах. Корректировка выполняется путем перебора состояний всех возможных положений трех ошибок. Всего приходится проверять: $C_{16}^{3} = \frac{16!}{3!(16-3)!} = 560$ состояний для каждого из 16-битных фрагментов кода. По такой схеме, крайне редко, но все-таки возможно скорректировать 3x16=48 ошибок. Вероятность коррекции столь большого числа ошибок мала и составляет менее 0.00001. Однако, если число ошибок не более 16 и все они попали в разные фрагменты кода, то все они однозначно исправляются.

Так как на каждые 16 бит кода хранится 3 бита информации, в первом приближении можно считать, что эти три бита скомпрометированы. То есть стойкость к атакам подбора кода ключа длинной в 256 бит не может быть выше 208 бит.

**Поддержка квантовой суперпозиции для наблюдения показателей стабильности разрядов кода нейронной сети**

При выполнении требований пакета национальных стандартов ГОСТ Р 52633.xx энтропия кодов преобразователя приводит к тому, что энтропия кодов примеров образа «Свой» мала:

$$H("c_1, c_2, ...., c_{256}") \approx 0.05 \text{ бит} \qquad (1).$$

Это связано с тем, что данные примеров образа «Свой» находятся внутри многомерного эллипса «Свой». При обучении преобразователя по ГОСТ Р 53633.5 [8] каждый нейрон будет давать разделяющую гиперплоскость, причем все гиперплоскости нейронов пересекаются в центре области все «Чужие». Сечение многомерного пространства по паре любых биометрических параметров дает плоскость, отображенную на рисунке 2. На рисунке видно, что примеры 1, 2, …., 7 образа «Свой» находятся внутри эллипса, полученного при обучении.

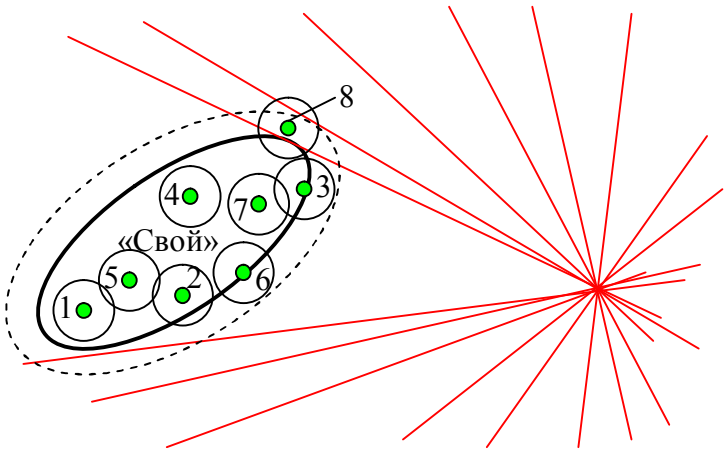


Рис. 2. Обнаружение нестабильных разрядов кода путем добавления тестового белого шума во входные данные

Пример-8 находится вне эллипса «Свой» за одной из линий, являющихся проекциями разделяющих гиперплоскостей нейронов. Это означает, что в одном из 256 разрядов кода появится ошибка при предъявлении примера-8 образа «Свой».

Расстояние между примерами и прямыми линиями рисунка 2 отражает стабильность разрядов кода. Для того, что бы оценить стабильность разрядов кода, предъявленного нейронной сети примера необходимо добавить к данным примера белый шум, как это показано на рисунке 3. На рисунке 2 добавление белого шума приводит к появлению окружностей, накрывающих точку каждого из примеров. Из рисунка 2 видно, что окружность шума, накрывшая пример-8, пересекает две прямые, что приводит к нестабильности не менее двух бит выходного кода нейронной сети. Другие окружности примеров 1, 2, …, 7 не пересекают разделяющих прямых, то есть эти примеры будут давать стабильные разряды кода.

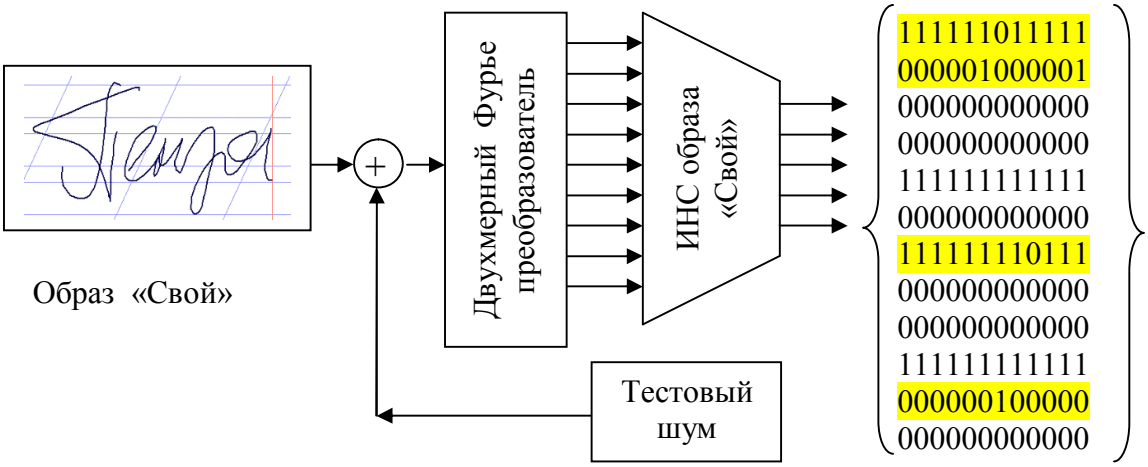


Рис. 3. Схема поддержки квантовой суперпозиции на выходах нейронной сети преобразователей биометрия-код

Для того, что бы определить уровень нестабильности каждого из разрядов кода необходимо получать множество выходных кодов, как это показано на рисунке 3. Поданный на вход нейросети аддитивный белый шум дает множество выходных кодов, при этом полностью стабильные разряды не меняют своего состояния. В нестабильных разрядах состояния меняются.

Для каждого разряда может быть вычислен показатель стабильности:

$$w_i = 2\left|P("0_i") - 0.5\right| = 2\left|P("1_i") - 0.5\right| \qquad (2),$$

где $i$ – номер контролируемого разряда, $P("0_i")$ - вероятность появления состояния «0» в i-том разряде кода, $P("1_i")$ - вероятность появления состояния «1» в i-том разряде кода.

Показатель стабильности может меняться в интервале от 0 до 1, при $w_i = 0$ состояние i-го разряда абсолютно нестабильно (имеем полноценный кубит). При $w_i = 1$ состояние i-го разряда абсолютно стабильно (квантовая суперпозиция полностью отсутствует). На рисунке 3 стабильные разряды даны без заливки, а нестабильные разряды помечены заливкой.

**Нейросетевая молекула, поддержка ее состояний в нейродинамики**

В 80-х годах наш соотечественник Юрий Манин занимался струнами и предложил концепцию организации вычислений [12, 13], осуществляемых на квантово-механических вычислительных элементах нового поколения. За последующие 30 лет развития эта новая концепция активно углублялась, была создана полноценная квантовая математика под квантовую механику уравнения Шредингера. Были найдены эффективные квантовые алгоритмы полиномиальной вычислительной сложности. Например, Питер Шор в 1994 году создал квантовый алгоритм под решение задачи поиска простых чисел по их произведению (обратная задача для RSA алгоритма шифрования). Возник значительный интерес мировой научно-технической и криптографической общественности к практическим реализациям квантовых вычислений. Однако, исследования квантовых алгоритмов показали, что решение уравнений Шредингера на обычном компьютере становится технически невозможным уже при 30 степенях свободы, так как эти алгоритмы имеют экспоненциальную вычислительную сложность. В рамках квантовой механики сформулирован постулат о невозможности симуляции достаточно большого числа кубит на обычном компьютере.

Ситуация меняется когда речь идет о моделировании искусственных нейронных сетей, корреляционных молекул, хи-квадрат молекул [14, 15, 16]. В этом случае задача моделирования имеет линейную вычислительную сложность.

Применительно к задаче коррекции кодов мы имеем дело с режимом поддержки нейродинамики. Нейронную сеть можно рассматривать как нейросетевую молекулу, откликающуюся спектром выходных дискретных (цифровых) состояний на зашумление входных данных образа «Свой».

На рисунке 4 приведена структура нейросетевой молекулы преобразующей континуумы входных состояний в спектр последовательности цифровых кодов.

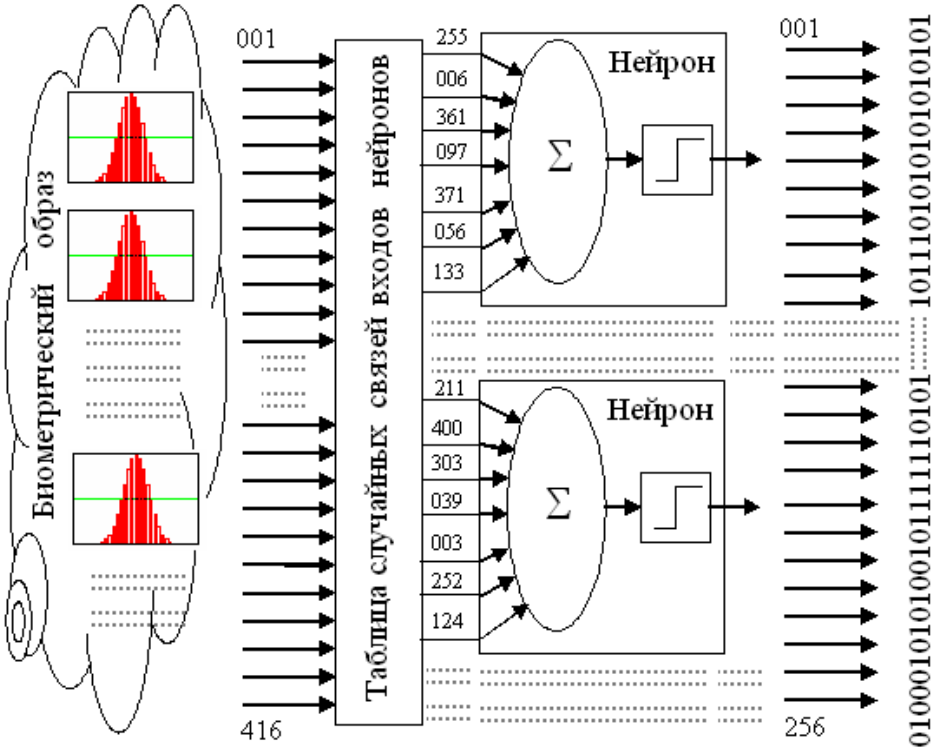


Рис. 4. Нейросетевой преобразователь, находящейся в режиме поддержки нейродинамики

Нами был рассмотрен только один режим поддержки квантовой суперпозиции через зашумление входов нейросетевой молекулы (рисунок 3), однако это не единственный способ. При решении обратной задачи нейросетевой биометрии [14] приходится скрещивать между собой образы «Чужой» и тем самым поддерживать режим нейродинамики преобразователя биометрия-код. Когда речь идет о хи-квадрат молекулах [16, 17] поддержки квантовых эффектов в нейродинамике, приходится поддерживать нейродинамику случайно выбирая данные серий малых выборок из одной большой выборки.

Главное состоит в том, что моделирование нейронов (сумматоров и квантователей) является задачей линейной вычислительной сложности. Если уравнения Шредингера с большим числом степеней свободы нельзя воспроизводить на обычной вычислительной машине, то уравнения нейросетевой молекулы или хи-квадрат молекулы легко воспроизводятся на обычных компьютерах при большом числе степеней свободы. В нашем случае нейросетевой преобразователь биометрия-код с 416 входами и 256 выходами на обычной вычислительной машине удается воспроизводить до 10 000 раз в секунду. За одну секунду мы получаем 10 000 кодов-откликов на входной вектор «Свой», окрашенный белым шумом.

**Преимущества, получаемые за счет поддержки квантовой суперпозиции**

Схема самокорректирующихся кодов с хэш-остатками (рисунок 1) способна корректировать некоторое число ошибок меньшее, чем число запомненных разрядов остатков. При этом, наблюдая расхождение эталонных хэш-остатков и реально вычисленных хэш-остатков, мы не можем указать положения ошибок, при наличии ошибки в первом фрагменте кода.

Однако если мы воспроизведем квантовую суперпозицию и оценим показатели стабильности разрядов кода, то нам удастся определить число и положение «слабых» бит кода. Зная эту информацию, мы можем значительно ускорить поиск и расширить область проверяемых состояний кода.

Например, если мы обнаружили в первых 16 разрядах 5 «слабых» бит, а в следующих трех фрагментах с 17-го бита до 64 бита нет «слабых» разрядов мы можем однозначно восстановить код перебирая $C_{16}^{5} = 4368$ состояний, контролируя при этом 4x3=12 эталонных бит Хэш-остатков.

Ранее использовавшиеся коды, без контроля стабильности разрядов в нейродинамике [9], были не способны корректировать ошибки, группирующиеся в начале схемы корректировки (рисунок 1). В нашем же случае даже группировка 8 ошибок в первых 16 битах и 8 ошибок в следующих 16 битах однозначно корректируется при отсутствии ошибок в последующих фрагментах кода.

Выигрыш по времени при корректировке 16 бит при известном положении «слабых» разрядов в сравнении с проверкой по три возможных положения ошибок в каждом из 16 фрагментов кода может составить до 20 000 раз. То есть самокорректирующиеся коды с поддержкой квантовой суперпозиции способны корректировать до 16 ошибок в коде в реальном масштабе времени ввода и обработки биометрических данных.

**Литература:**


1. Juels A., Wattenberg M. A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security, Singapore — November 01 – 04, 1999, p. 28–36.

2. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes. //Advances in Artificial Intelligence - IBERAMIA-SBIA 2006 (LNCS 4140), p. 178-187, 2006

3. Feng Hao, Ross Anderson, and John Daugman. Crypto with Biometrics Effectively, IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 9, SEPTEMBER 2006.

4. Иванов А.И. Нечеткие экстракторы: проблема использования в биометрии и криптографии. // Первая миля. № 1, 2015 г. с. 40-47.

5. Язов Ю.К. и др. Нейросетевая защита персональных биометрических данных. //Ю.К.Язов (редактор и автор), соавторы В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров // М.: Радиотехника, 2012 г. 157 с. IBSN 978-5-88070-044-8.

6. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа. Монография, Казахстан, г. Алматы, ТОО «Издательство LEM», 2014 г. -144 с., находится в открытом доступе (http://portal.kaznu.kz/files/publicate/2014-06-27-11940.pdf)

7. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

8. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

9. Безяев А.В. Безкомпроматная индикация качества ввода фрагментов тайного составного биометрического образа «Нейрокомпьютеры: разработка, применение» №6, 2009 с. 59- 62

10. Безяев А.В., Иванов А.И., Фунтикова Ю.В. Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций. «Вестник Уральского федерального округа. Безопасность в информационной сфере» 2014 г. № 3*(13)* с. 4-14.

11. Волчихин В.И., Иванов А.И., Безяев А.В., Елфимов А.В., Юнин А.П. Оценка эффекта ускорения вычислений, обусловленного поддержкой квантовой суперпозиции при корректировке выходных состояний нейросетевого преобразователя биометрии в код //«Известия высших учебных заведений. Поволжский регион. Технические науки. № 1, 2017 с. 43-55.

12. Нильсон М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир. 2006 г. 821 с.

13. Душкин Р.В. Квантовые вычисления и функциональное программирование. ДМК Пресс, 2015-234 с. IBSN: 978-597060-257-1.

14. Волчихин В.И., Иванов А.И. Нейросетевая молекула: решение обратной задачи биометрии через программную поддержку квантовой суперпозиции на выходах сети искусственных нейронов //Вестник Мордовского университета. Т27. №4, 2017, с 518-523.

15. Волчихин В.И., Иванов А.И., Сериков А.В., Серикова Ю.И. Квантовая суперпозиция дискретного спектра состояний математической молекулы корреляции для малых выборок биометрических данных // Вестник Мордовского университета. Т27. №2, 2017, с 230-243.

16. Волчихин В.И., Иванов А.И., Пащенко Д.В., Ахметов Б.Б., Вятчанин С.Е. Перспективы создания циклической континуально-квантовой хи-квадрат машины для проверки статистических гипотез на малых выборках биометрических данных и данных иной природы. // Известия высших учебных заведений. Поволжский регион. Технические науки. – Пенза: ПГУ, №1, 2017 с. 5-15

17. Волчихин В.И., Иванов А.И. Хаотическая нейродинамика хи-квадрат молекул, квантовая обработка малых выборок биометрических данных на обычном компьютере. // Всероссийская научно-техническая конференция, посвященная 100-летию со дня рождения одного из основоположников советской вычислительной техники Б.И. Рамеева, на тему: «Информационно-управляющие и телекоммуникационные системы специального назначения». Секция «Биометрическая поддержка криптовалют, блокчейн реестров, облачных сервисов», проводится в конференц-зале Технопарка высоких технологий «Рамеев», доклад 16 мая 2018 года с $11^{15}$ до $11^{30}$ (ул. Центральная, д. 1), г. Пенза.

**Безяев Александр Викторович** – к.т.н., ведущий специалист Пензенского филиала ФГУП НТЦ «Атлас», E mail: Bezyaev_Alex@mail.ru

**Bezjaev Alexander Victorovich** – Candidate of engineering, lead specialist of STC “Atlas” Penza branch, “Information security questions” journal’s editorial office-authors interaction coordinator , E-mail: Bezyaev_alex@mail.ru.