МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математичекого моделирования и анализа данных

Отчёт
о прохождении производственной практики
для специальности
1-31 81 12«Прикладной компьютерный анализ данных»

магистранта 2 года обучения
Деркача Максима Юрьевича

Руководитель практики от кафедры

чл.-корр. НАН Беларуси,
доктор физ.-мат. наук, профессор
Харин Юрий Семенович

Руководитель практики от организации

Пьянов Владислав Сергеевич

Минск, 2019

Оглавление

1 Введение

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим считается криптографический [1].

Нейронная криптография - это раздел криптографии, посвященный анализу применения стохастических алгоритмов, особенно алгоритмов искусственных нейронных сетей, для использования в шифровании и криптоанализе.[2] Существуют решения, построенные на основе искусственных нейронных сетей, позволяющие обеспечить доступность данных [3].

Архитектура искусственных нейронных сетей позволяет эффективно проводить работы по распознаванию образов и классификации множества объектов по любым признакам. Кроме того, благодаря хорошо продуманному алгоритму обученные нейронные сети могут достигать чрезвычайно высоких уровней точности.

Основной целью практики являлось построение нейронных сетей, для апроксимации элементарных преобразований из алгоритма шифрования ГОСТ 28147-89, проведение компьютерных экспериментов и проведение анализа полученных результатов.

2 Описание математических моделей

Опишем однотактовое преобразование шифрования ГОСТ 28147-89.

$Y = g(X, K) = g(X_1||X_2, K) \equiv (S[X_1 \boxplus K] \ll 11) \oplus X_2||X_1$, где
$X \in V_{64}$ - вектор входных данных,
$Y \in V_{64}$ - выходные данные,
$K \in V_{32}$ - ключ,
S - стандартный S-блок из ГОСТ-28147.

Определим следущие математичские модели (элементы преобразования), для которых в дальнейшем будут ппостроены нейронные сети и проведены компьютерные эксперименты.

1. $Y_{g_0} = g_0(x) = g_1(x_1||x_2) \equiv x_1 \oplus x_2$, где

   $x \in V_8$ - вектор входных данных,

   $x_1, x_2 \in V4$ - левая и правая часть входного вектора,

   $Y_{g_0} \in V_4$ - выходные данные модели g_0;

2. $Y_{g_1} = g_1(x) = g_1(x_1||x_2, k) \equiv S[x_1] \oplus x_2$, где

   $x \in V_8$ - вектор входных данных,

   $x_1, x_2 \in V4$ - левая и правая часть входного вектора,

   $Y_{g_1} \in V_4$ - выходные данные модели g_1,

   S - стандартный S-блок из ГОСТ-28147;

3. $Y_{g_2} = g_2(x) = g_2(x_1||x_2, k) \equiv S[x_1 \boxplus k] \oplus x_2$, где

   $x \in V_8$ - вектор входных данных,

   $x_1, x_2 \in V4$ - левая и правая часть входного вектора,

   $k \in V_4$ - некоторый неизвестный постоянный в эксперименте ключ (4-ех битный ключ),

   $Y_{g_2} \in V_4$ - выходные данные модели g_2,

   S - стандартный S-блок из ГОСТ-28147.

Опишем определеные ранее модели как частные случаи однотактового преобразования шифрования ГОСТ 28147-89:

1. Модель g_0 является однотактовым преобразованием шифрования ГОСТ 28147-89, при слудеующих условиях:

   - S-блок - прямая таблица подстановки (подстановка при которой исходное значение переходит в такое же знанчение).
   - $K = 0^{32}$.
   - Отсутствует сдвиг влево на 11 бит.
   - Рассмотриваются только первые 4-бита X_1, X_2, Y.

2. Модель g_1 является однотактовым преобразованием шифрования ГОСТ 28147-89, при слудеующих условиях:

   - S-блок - стандартный S-блок из ГОСТ-28147.
   - $K = 0^{32}$.
   - Отсутствует сдвиг влево на 11 бит.
   - Рассмотриваются только первые 4-бита X_1, X_2, Y.

3. Модель g_1 является однотактовым преобразованием шифрования ГОСТ 28147-89, при слудеующих условиях:

   - S-блок - стандартный S-блок из ГОСТ-28147.
   - K - некоторый неизвестный постоянный в эксперименте ключ.
   - Отсутствует сдвиг влево на 11 бит.
   - Рассмотриваются только первые 4-бита X_1, X_2, Y.

3 Описание используемых нейронных сетей

Для решения поставленных задач использовались следующие нейронные сети:

1. Однослойная нерйоная сеть;
2. Многослойная нерйоная сеть с одним скрытым слоем, с переменным количеством нейронов на скрытом слое;
3. Многослойная нерйоная сеть с двумя скрытым слоями, с переменным количеством нейронов на скрытых слоях.

Точность построенной модели к реальной оценивалась использовалось расстояние Хэмминга: $w(y, \hat{y}) = \sum_{i=1}^{j} y_i \oplus \hat{y}_i$, где $y_i \in V_j$.

Для оценки точности проведенного эксперимента использовалось следующая функция: $\hat{f} = L - \frac{1}{T_e} \sum_{j=1}^{T_e} w(y^{(j)}, \hat{y^{(j)}})$, где L - количество бит в выходных данных оцениваемой модели.

Компьютерные эксперименты проводились на следующих данных:

1. Обучающая выборка $T_o = 18 * 10^3$ пар (x, x_1);
2. Экзаменационная выборка $T_e = 2 * 10^3$ пар (x, x_1).

4 Результаты компьютерных экспериментов

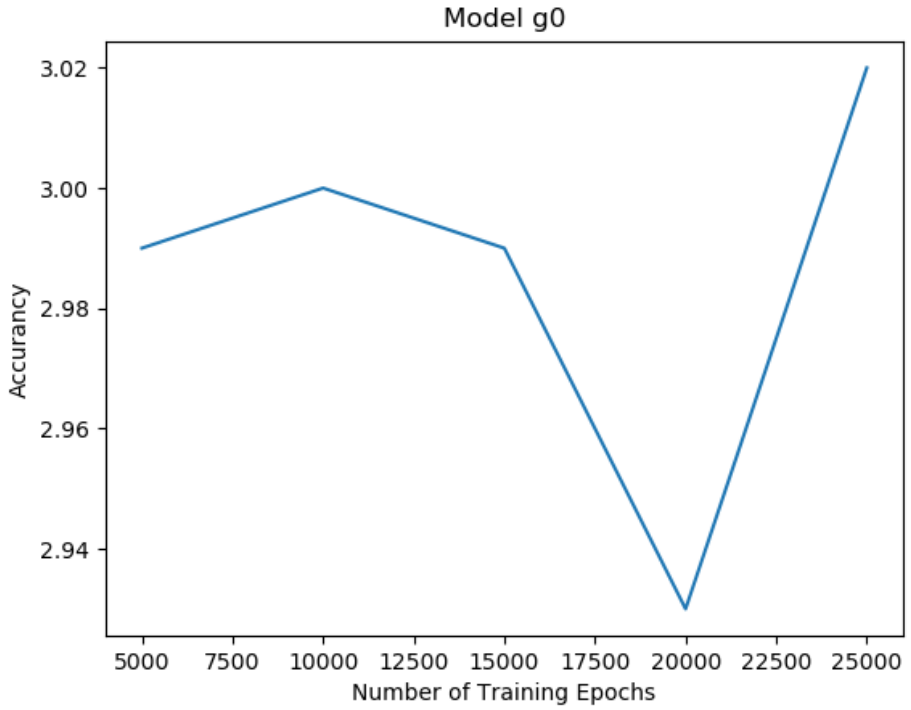

График точности построенной однослойной неройной сети модели g_0 от количества итераций обучения.

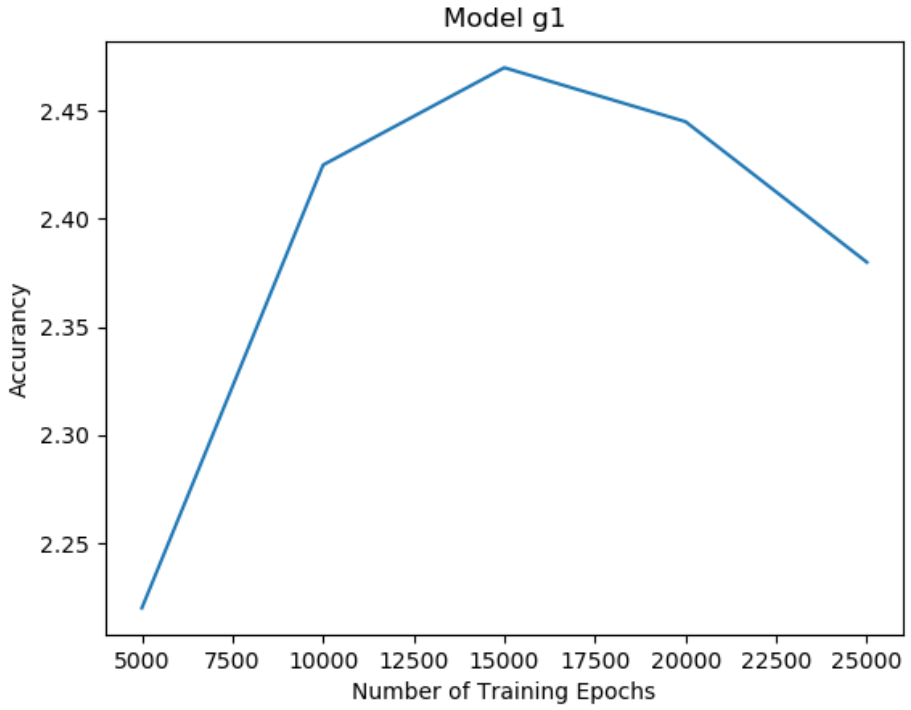

График точности построенной однослойной неройной сети модели g_1 от количества итераций обучения.

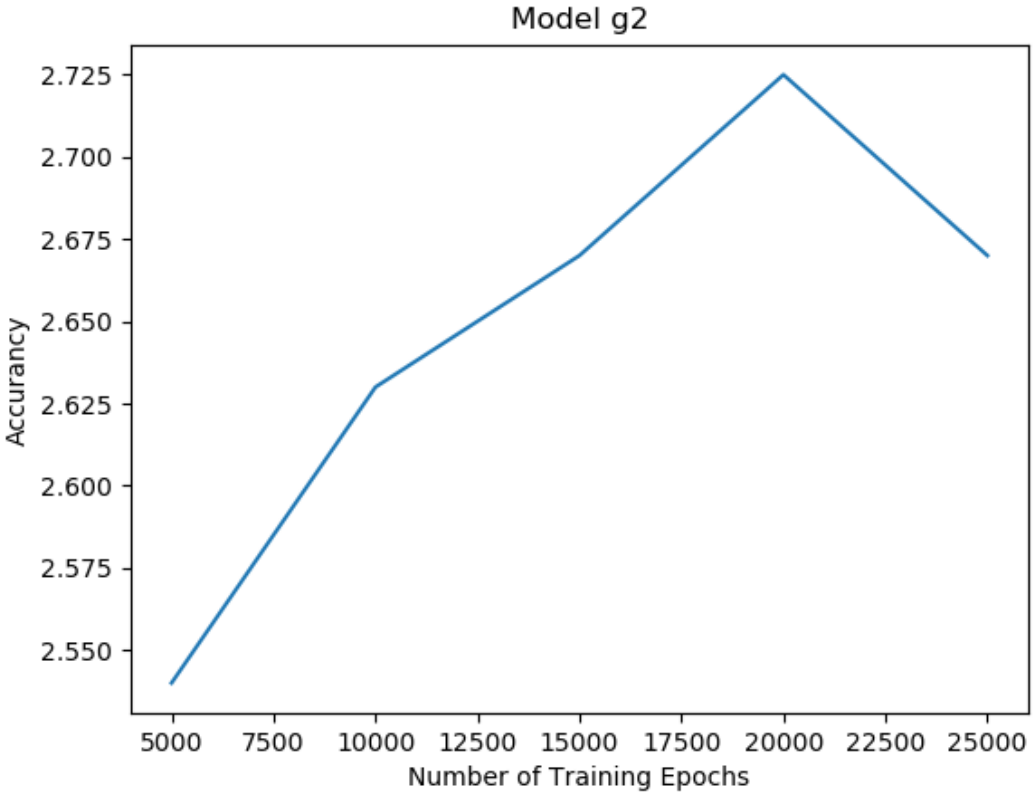

График точности построенной однослойной неройной сети модели g_2 от количества итераций обучения.

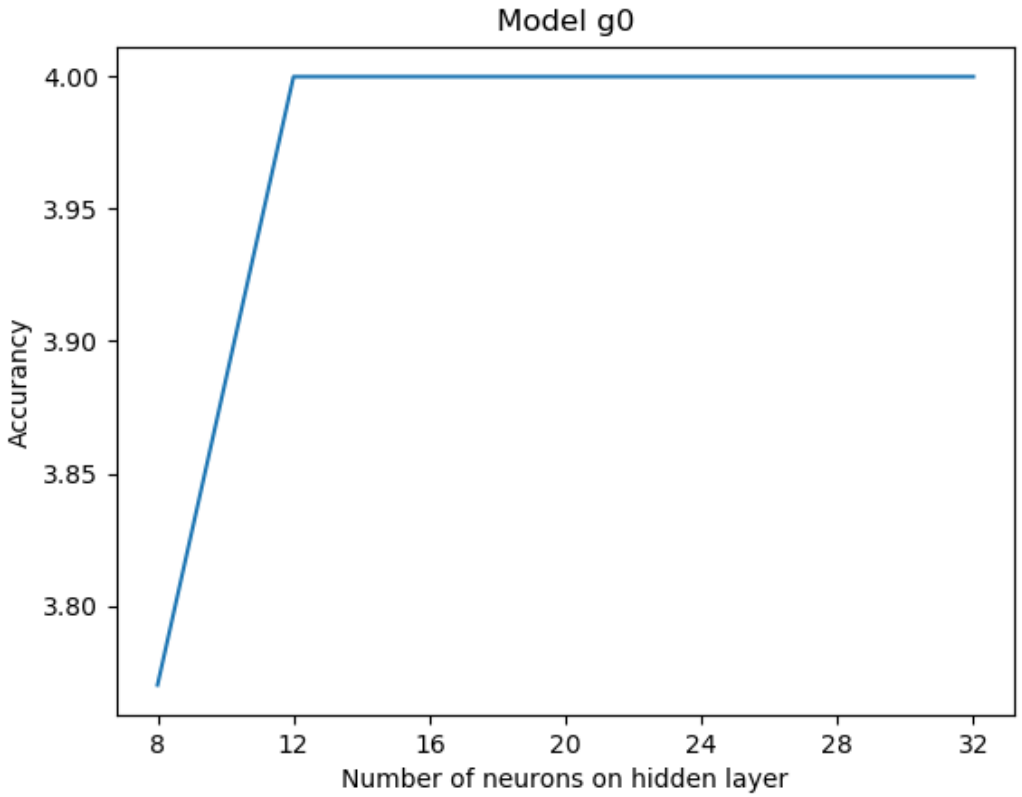

График точности построенной неройной сети модели g_0 от кол-ва нейронов на скрытом слое.

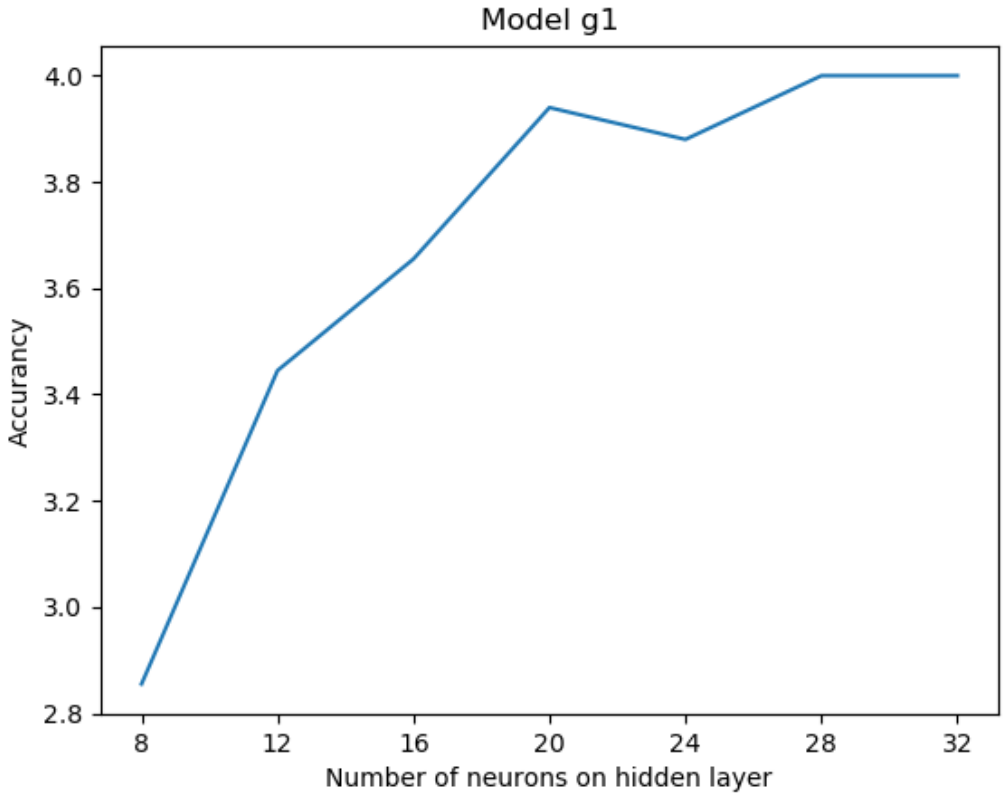

График точности построенной неройной сети модели g_1 от кол-ва нейронов на скрытом слое.

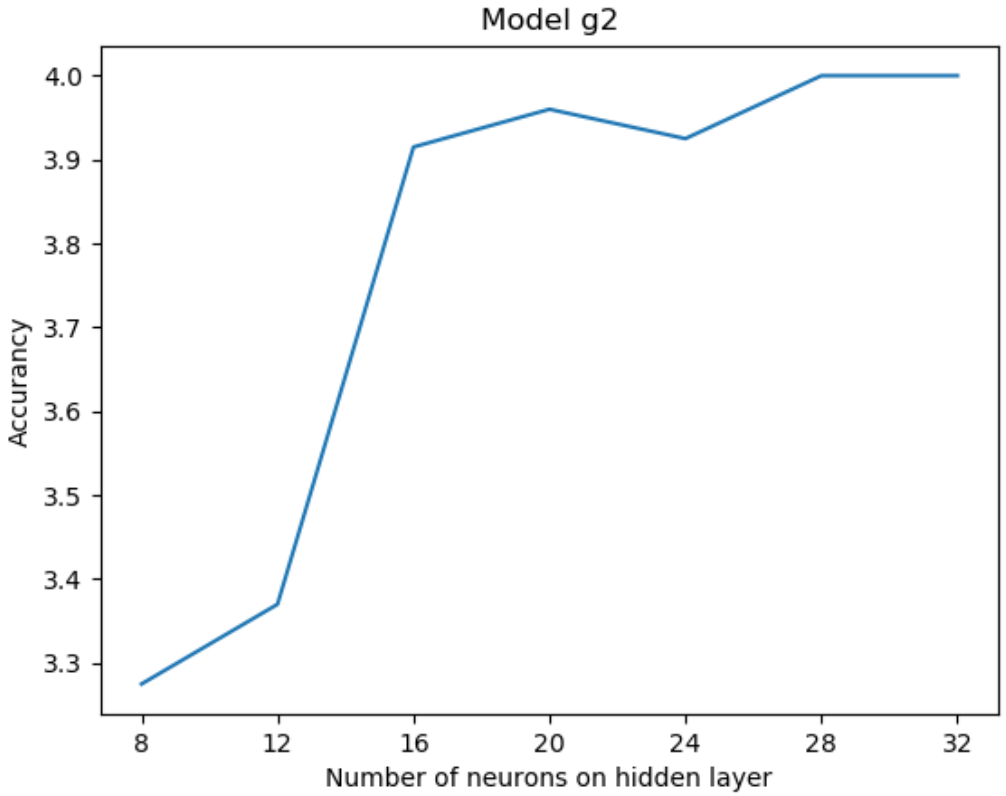

График точности построенной неройной сети модели g_2 от кол-ва нейронов на скрытом слое.

График точности построенной неройной сети модели g_0 от кол-ва нейронов на скрытых слоях.

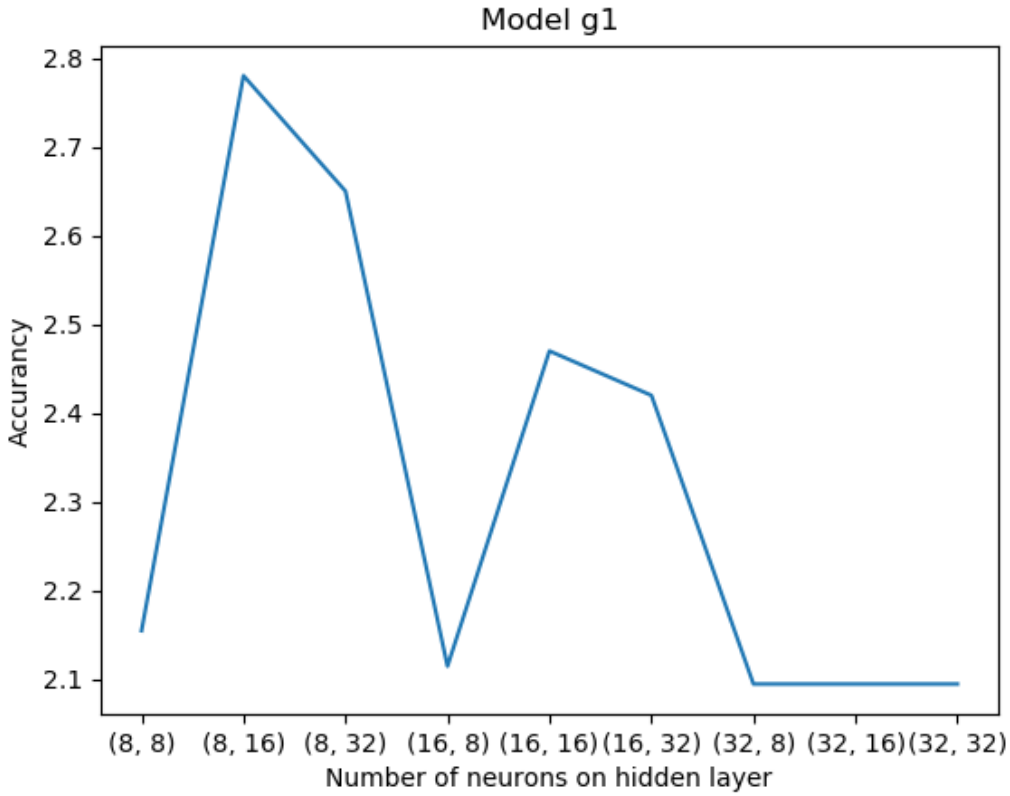

График точности построенной неройной сети модели g_1 от кол-ва нейронов на скрытых слоях.

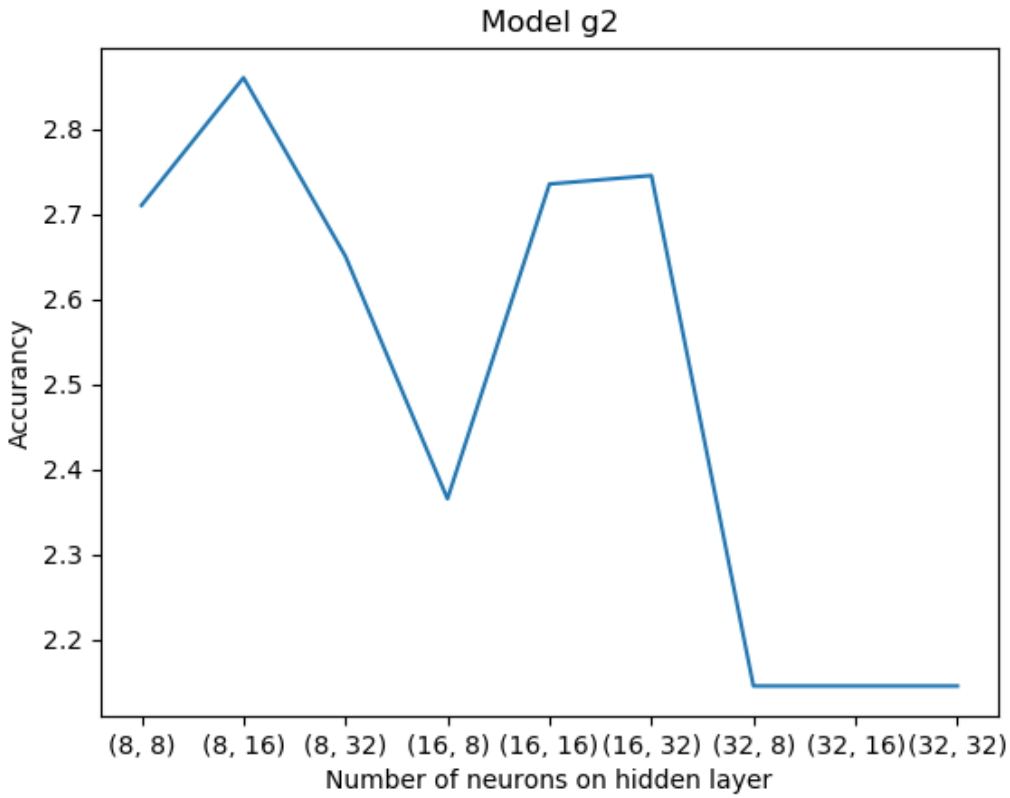

График точности построенной неройной сети модели g_2 от кол-ва нейронов на скрытых слоях.

5 Анализ результатов

Исходя из полученных результатов можно сделать выводы, что нейронная сеть с одним скрытым слоем наиболее точно аппроксимирует построенные модели.

И для аппроксимации однотактового преобразования шифрования ГОСТ 28147-89, можно воспользоваться моделью g_2 и нейронной сетью, построенной для это модели.

Метод построение нейронной сети для аппроксимации однотактового преобразования шифрования ГОСТ 28147-89:

1. Входной вектор $X_1 \in V_{64}$ разбиваем на блоки длинной 4 бита (x_1^i).
2. Входной вектор $X_2 \in V_{64}$ сдвигаем вправо на 11 бит и разбиваем на блоки длинной 4 бита (x_2^i).
3. Выходной вектор Y также сдвигаем вправо на 11 бит разбиваем на блоки длинной 4 бита (y^i).
4. Для каждого набора блоков $x_1^i, x_2^i, y^i, i = 1, ..8$, обучаем нейронную сеть.
5. Полученный набор нейронных сетей можно использовать для аппроксимации однотактового преобразования шифрования ГОСТ 28147-89.

Для данного метода были проведены компьютерные эксперименты, используя нейронные сети с одним скрытым слоем.

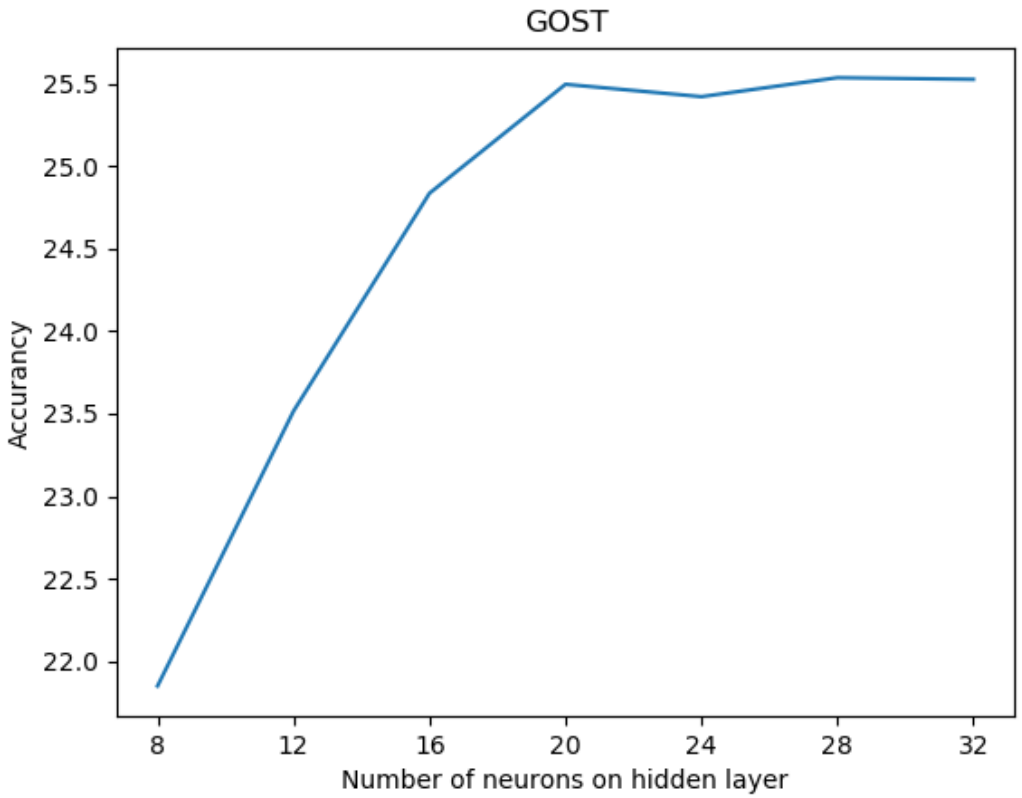

График точности построенной неройной сети от кол-ва нейронов на скрытом слое.

Данный метод показывает высокую точность и не требует больших вычислительных ресурсов, как в случае с построением нейронной сети для однотактового преобразования шифрования ГОСТ 28147-89.

Литература

1. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. — 2003. — Минск.
2. Neural networks in cryptography [Электрон. ресурс]. — 2015. — $http://cryptowiki.net/index.php?title=Neural\_networks\_in\_cryptography$.
3. Pattanayak S., Ludwig S.A. Encryption based on Neural Cryptography. — 2017.
4. Kinzel F., Kanter I. Neural Cryptography. — 2002.