УДК 004.01

РАЗРАБОТКА МЕХАНИЗМА БЕЗОПАСНОЙ КОММУНИКАЦИИ НА БАЗЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ[1]

Статья поступила в редакцию 20.03.2020, в окончательной варианте – 01.06.2020.

Власов Роман Сергеевич, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
студент, e-mail: roma1202@mail.ru
Лукащик Елена Павловна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
кандидат физико-математических наук, доцент, e-mail: lep_9091@mail.ru
Осипян Валерий Осипович, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
доктор физико-математических наук, профессор, e-mail: v.osippyan@gmail.com

Разработка безопасного канала передачи данных – одно из решений проблемы обеспечения безопасности данных клиентов, которая по-прежнему остается первоочередной для современных информационных сервисов. Возможное решение этой проблемы видится в создании механизма, способного адаптироваться к текущему состоянию канала и в целях усиления безопасности автоматически изменять его криптографические характеристики. Для решения сложных задач, которые выходят за рамки простых функциональных спецификаций, в настоящее время все чаще используют методы машинного обучения. В данной работе при создании системы безопасной передачи данных по защищенному каналу применяют нейронные сети. Организация предлагаемой криптосистемы соответствует классическому сценарию в области безопасности. Эта система состоит из трех нейронных сетей: **A**, **B** и **E**. Основная задача сетей **A** и **B** – безопасное общение на основе симметричного шифрования. Сеть **E** желает подслушать их «информационный обмен», проанализировать его и в конечном счете получить возможность знакомиться с содержанием передаваемых сообщений, содержащих конфиденциальную информацию. Главной отличительной чертой предлагаемой системы защиты является то, что она не основана на строгом криптографическом алгоритме, а обучается безопасной коммуникации с течением времени. Состязательное функционирование нейронных сетей приводит к постоянной модификации системы шифрования. Предложенная система демонстрирует способности нового адаптивного метода обеспечения безопасности – нейронного. Искусственный интеллект способен автоматически разработать такое шифрование, которое будет недоступно для взлома. Примеров успешного применения нейросетевой технологии в криптографии к настоящему моменту крайне мало, что связано со спецификой данной области. Однако, учитывая потенциал передовых информационных технологий, можно утверждать, что применение методов машинного обучения в эру квантовых компьютеров, что, по-видимому, ожидает нас в ближайшем будущем, будет необходимым при создании оптимальных систем защиты.

Ключевые слова: безопасная коммуникация, защищенный канал связи, криптография, искусственный интеллект, машинное обучение, нейронные сети, состязательность

DEVELOPMENT OF SECURE COMMUNICATION MECHANISM BASED ON MACHINE LEARNING METHODS

The article was received by the editorial board on 20.03.2020, in the final version – 01.06.2020.

Vlasov Roman S., Kuban State University, Krasnodar, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
student, e-mail: roma1202@mail.ru
Lukashchik Elena P., Kuban State University, Krasnodar, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
Cand. Sci. (Physics and Mathematics), Associate Professor, e-mail: lep_9091@mail.ru
Osipyan Valery O., Kuban State University, Krasnodar, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
Doct. Sci. (Physics and Mathematics), Professor, e-mail: v.osippyan@gmail.com

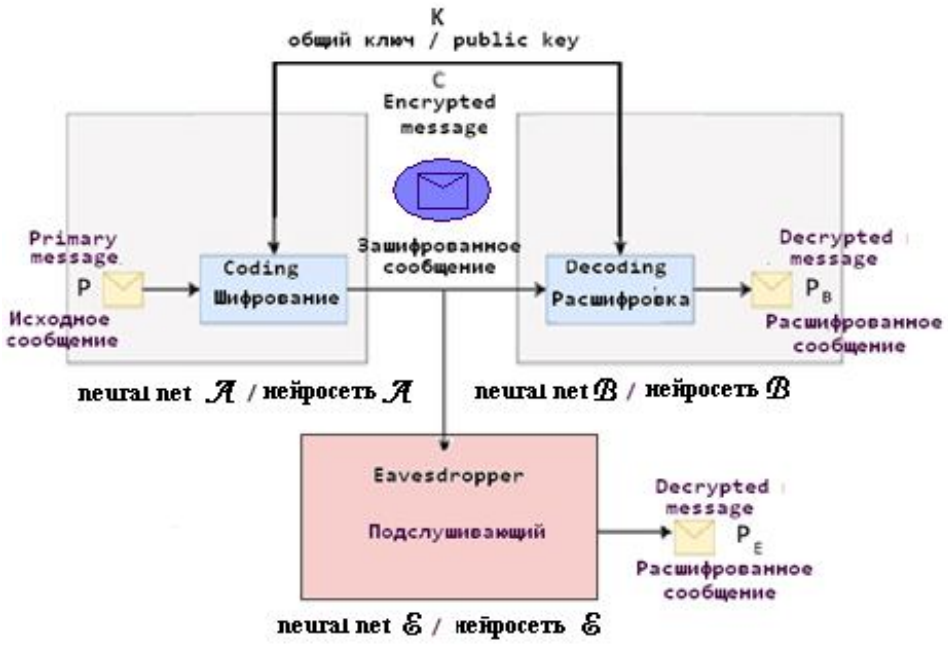
Development of a secure data transmission channel is one of the solutions to the problem of customer data security, which remains a priority for modern information services. One of the solutions seems to be the creation of a

[1] Работа поддержана грантом РФФИ № 19-01-00596 «Теоретико-числовые и алгоритмические аспекты разработки математических моделей систем защиты информации, содержащих диофантовы трудности».

mechanism that can adapt to the current state of the channel and, in order to enhance security, automatically change its cryptographic characteristics. To solve complex problems that go beyond simple functional specifications, machine learning methods are increasingly being used. In this work, during creating a system for the secure transmission of data over a secure channel, neural networks are used. The organization of the proposed cryptosystem corresponds to the classical scenario in the security field. This system consists of three neural networks: **A**, **B** and **E**. Networks **A** and **B** want to communicate securely using symmetric encryption. Network **E** wants to eavesdrop on their messages in order to receive the original message. The main distinguishing feature of the proposed security system is that it is not based on a strict cryptographic algorithm, but learns how to communicate securely over time. The adversarial functioning of neural networks leads to constant modification of the encryption system. The proposed system demonstrates the capabilities of a new security method - neural, when artificial intelligence itself develops such encryption that will be inaccessible for hacking. To date, there are very few examples of the use of neural network technology in cryptography due to its specificity. However, given the potential of the advanced information technologies, it can be argued that the application of machine learning methods in the era of quantum computers, into which we are gradually diving, will be necessary for creating optimal security systems.

Keywords: secure communication, secure communication channel, cryptography, artificial intelligence, machine learning, neural networks, adversary

Graphical annotation (Графическая аннотация)



Введение. Защита информации клиентов остается задачей первостепенной важности для динамично растущих в настоящее время направлений IT-рынка. Международная исследовательская и консалтинговая компания International Data Corporation (IDC) [15] провела исследование, которое показало, что даже с «облачными» технологиями, которые стремительно внедряются в IT-среду, многие компании связывают большие проблемы по части безопасности. Независимая исследовательская организация Portio Research [10] только подтвердила это, указав конкретные цифры: 68 % опрошенных руководителей европейских IT-компаний в целях обеспечения безопасности отказываются использовать «облачные» сервисы [8].

В IT-индустрии одним из способов защиты данных в процессе передачи по сети является построение виртуальных защищенных каналов связи. Они представляют собой соединение в сети, по которому передаются криптографически защищённые пакеты сообщений. Криптографические системы защиты постоянно совершенствуются, часто для этих целей используют сложные математические модели. Так, в последнее время появился цикл работ, посвященных созданию криптографических систем высокой стойкости на основе математического аппарата параметрических решений систем диафантовых уравнений [19].

К сожалению, со временем реализация почти любого способа шифрования все в меньшей степени обеспечивает необходимую защиту конфиденциальных данных. В связи с этим оправданными являются попытки разработки механизма безопасности, способного адаптироваться к сложившейся в канале криптографической ситуации и, при необходимости, динамически изменять

применяемый способ шифрования с целью улучшения безопасности передачи данных. Для создания подобного сложного механизма целесообразно использование современных возможностей искусственного интеллекта [3].

Тема искусственного интеллекта, интеллектуальных алгоритмов и машинного обучения чрезвычайно популярна. Это легко можно увидеть, наблюдая за новостями на различных IT порталах [17]. Среди множества парадигм и подходов в машинном обучении выделяется одна очень интересная область – искусственные нейронные сети (ИНС). Опыт использования ИНС показал их возможности при решении задач, алгоритм которых неизвестен [1]. Например, они используются для анализа сетевого трафика, выявления и определения сетевых атак [4, 5]. Однако в криптографии, связанной с использованием алгоритмов и протоколов, которые обеспечивают секретность и целостность информации, удачных решений на базе ИНС крайне мало.

Впервые взгляд на криптографию как новую область машинного обучения реализовался благодаря исследованиям, проводимым компанией Google (подразделение Google Brain) [9]. Команда данного подразделения предложила оригинальную модель криптографической системы состязательных ИНС. Реализованный в этой модели подход созвучен с последними исследованиями автоматического синтеза криптосистем с использованием таких технологий, как Zoo Crypt [13].

Главная цель исследований на базе машинного обучения – доказать, что ИНС могут научиться защищать конфиденциальность используемых данных от других ИНС. Благодаря состязательному обучению ИНС способны изобретать новые оптимальные формы шифрования и дешифрования без разработки каких-либо специальных алгоритмов для этих целей. В настоящей работе на основе нейросетевой технологии предложен вариант криптосистемы, обеспечивающей устойчивую работу защищенного канала связи. Результаты проведенного численного эксперимента демонстрируют возможности использования искусственного интеллекта для построения адаптивных систем защиты; подтверждают перспективность исследований в данном направлении.

Архитектура используемой нейросистемы. Архитектура предложенной в данной работе криптографической системы соответствует классическому криптографическому сценарию, в котором принимают участие три участника: два собеседника и несанкционированный слушатель [3]. Задача собеседников: обладая секретным ключом, безопасно передавать текст. Задача слушателя: получить исходную информацию из зашифрованного текста, не используя секретный ключ. В качестве критерия защиты коммуникации выбрана только секретность. Злоумышленник является «пассивным злоумышленником», который может перехватывать сообщения, но не может инициировать сеансы, вводить дополнительные сообщения или изменять передаваемые сообщения.

Согласно принятому сценарию в состав модельной системы входят три ИНС. Мы дали им классические для криптографии имена [14]: **A**, **B** и **E**. Каждая система была обучена поддерживать общение с двумя другими. Работа **A** заключается в отправке секретных сообщений **B**. Сеть **B** должна расшифровать сообщение, присланное **A.** Задачей ИНС **E**, в свою очередь, является наблюдение за общением двух других.

На рисунке 1 схематически изображена соответствующая данному сценарию система обмена данными. Компоненты криптосистемы представлены в виде сверточных ИНС, что является традиционным при глубинном обучении [6], позволяет уменьшить количество определяемых параметров при обучении. Все три нейросети состоят из полносвязного слоя и четырех одномерных сверточных слоев [7]. Каждый слой свёртки логически объединен со слоем активации. В качестве функции активации для первых трех сверточных слоев используется функция сигмоида, а для последнего – гиперболический тангенс. Численный эксперимент подтвердил, что выбор таких функций для активации позволяет оптимальным образом определить вероятность наличия характерных признаков.

На вход сети **A** подается исходное сообщение P и ключ K в виде двух векторов, элементы которых в общем случае могут принимать вещественные значения. Входные данные для решения тестовых задач поставляются из случайного распределения. Если исходное сообщение и ключ имеют одинаковую длину N, а на выходе первого полносвязного слоя имеется 2N нейронов, тогда количество параметров этого слоя равно $2N \times 2N$. Размер зашифрованного текста равен также N. То есть предлагаемый криптосистемой способ шифрования сводится к перестановке и изменению значений исходного текста. Размер ядер последующих сверточных слоев принимались равными 4, 2, 1 и 1, а шаг свертки 1, 2, 1 и 1 соответственно. Сеть **B** на вход принимает шифротекст C и ключ K. Структура слоев сети **B** аналогична структуре слоев **A.** На вход сети **E** принимается только зашифрованный текст C без ключа. В силу чего полносвязный слой этой сети имеет N входов и 2N выходов, а количество параметров этого слоя равно $N \times 2N$.

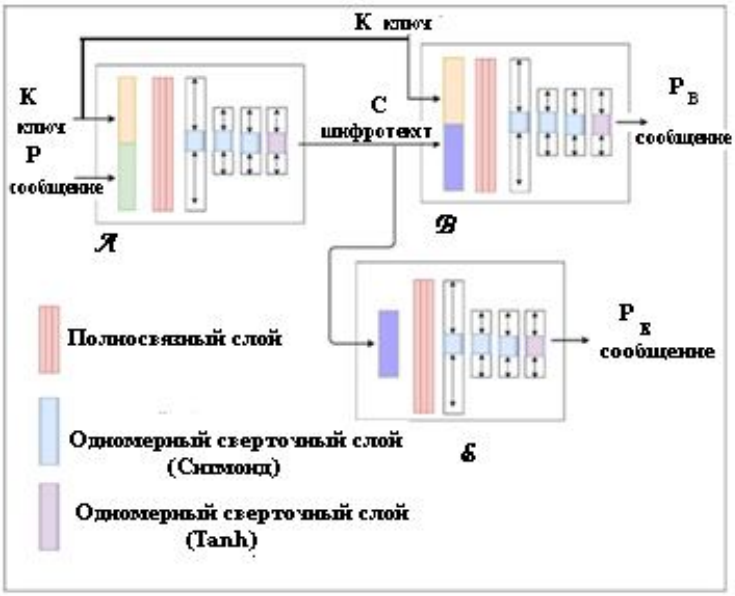


Рисунок 1 – Структура криптосистемы

Сети **B** и **E** получают шифротекст C и пытаются восстановить исходный текст P. Результаты работы сетей **B** и **E** обозначим P_B, P_E соответственно. **A** и **B** имеют преимущество перед **E**, так как обладают секретным ключом K. Для того, чтобы скрыть смысл изначального сообщения, **A** должна конвертировать открытый текст таким образом, чтобы **E** его не понимала. Измененный текст должен быть понятен только **B**. Изначально **A** и **B** должны договориться о том, каким образом нужно изменять текст, чтобы они могли понимать друг друга, а **E** бы его не понимала.

Роли входящих в данную криптосистему ИНС сводятся к следующему: **A** стремится к улучшению шифра, **B** обучается дешифрованию с использованием ключа, а **E**, соответственно, к дешифрованию без ключа. Заметим, что **A** и **B** для безопасной коммуникации заранее не предоставляется пара «сообщение – шифр», реализующая конкретный алгоритм симметричного шифрования. Они должны самостоятельно обучиться защищать информацию в результате тренировок. Наличие **E** стимулирует обучение **A**. Если бы в представленной модели не участвовала **E**, то возможен случай передачи сообщения от **A** к **B** без какой-либо формы шифрования, что является небезопасным.

В ходе тренировок результаты дешифрования криптотекста сетями **B** и **E** используются сетью **A** для изменения своих параметров с целью создать способ шифрования, для которого сеть **B** будет достигать нужной степени точности, а сеть **E** окажется неспособной вскрыть истинный смысл передаваемого зашифрованного сообщения. С течением времени может оказаться, что для сгенерированного сетью **A** шифра сеть **E** может обнаружить значительные успехи в дешифровании. В этом случае сеть **A** меняет шифр, что приводит, как правило, к ухудшению качества дешифрования сетью **E**. В результате такой генеративно-состязательный процесс приводит к безопасной коммуникации.

Математический аппарат. Нейронные сети **A**, **B** и **E** данной криптосистемы в общем случае работают с кортежами чисел с плавающей точкой. Функционирование системы можно описать при помощи следующего математического аппарата [14].

Для используемых данных примем следующие обозначения:

θ_A, θ_B и θ_E – параметры сетей **A**, **B** и **E** соответственно;

K, P, P_B, P_E и C – кортежи чисел с плавающей точкой.

Заметим, что C, P_B, P_E могут состоять из вещественных чисел, даже если P и K состоят только из «0» и «1».

Также определим функциональные зависимости:

$E_A(\theta_A, P, K)$ – шифр сети **A** на сообщение P и ключ K;

$D_B(\theta_B, C, K)$ – расшифровка сетью **B** криптотекста C при наличии ключа K;

$D_E(\theta_E, C)$ – расшифровка сетью **E** криптотекста C без ключа K.

Для оценки степени близости между подлинным текстом и приблизительным значением, полученным при дешифровке, будем использовать дистанцию L_1:

$$d(P, \acute{P}) = \sum_{i=1}^{N} |p_i - \acute{p_i}|,$$

где N – длина текста; p_i – элемент оригинального текста; $\acute{p_i}$ – элемент дешифрованного текста.

Задача сети **E** состоит в том, чтобы точно восстановить текст P. Насколько сильно **E** ошиблась во взломе при исходном тексте P и ключе K, показывает функция ошибок:

$$L_E(\theta_A, \theta_E, \mathrm{P}, \mathrm{K}) = d\left(\mathrm{P}, D_{\mathrm{E}}(\theta_{\mathrm{E}}, E_{\mathrm{A}}(\theta_{\mathrm{A}}, \mathrm{P}, \mathrm{K}))\right).$$

Обобщенная функция ошибок для сети **E** определяется как математическое ожидание над распределением исходных текстов и публичных ключей

$$L_E(\theta_{\mathrm{A}}, \theta_{\mathrm{E}}) = \bar{E}_{P,K}[L_E(\theta_{\mathrm{A}}, \theta_{\mathrm{E}}, P, K)].$$

Оптимальный результат работы сети **E** определяется по формуле:

$$O_E(\theta_A) = argmin_{\theta_E}(L_E(\theta_A, \theta_E,)).$$

Аналогично функция ошибок сети **B** для конкретного текста и ключа представляется в виде:

$$L_B(\theta_{\mathrm{A}}, \theta_B, P, K) = d(P, D_B(\theta_B, E_A(\theta_{\mathrm{A}}, P, K), K)),$$

и математическое ожидание распределения исходных текстов и публичных ключей

$$L_B(\theta_{\mathrm{A}}, \theta_B) = \bar{E}_{P,K}[L_B(\theta_{\mathrm{A}}, \theta_B, P, K)].$$

Основная задача сетей **A** и **B** – корректное общение и при этом сокрытие их коммуникации от **E**, что реализуется минимальной ошибкой для **B** и максимальной для **E**. Таким образом, функция совместной ошибки для сетей **A** и **B** должна включать компоненты, связанные с ошибкой дешифрования **B** и с успехом подслушивающей сети **E**. В качестве такой целевой функции можно предложить суперпозицию функции ошибок **B** L_{B} и оптимального значения L_{E}:

$$L_{AB}(\theta_{\mathrm{A}}, \theta_B) = L_B(\theta_{\mathrm{A}}, \theta_B) - L_E(\theta_{\mathrm{A}}, O_E(\theta_{\mathrm{A}})).$$

Оптимальное состояние системы соответствует точке экстремума указанной целевой функции:

$$(O_A, O_B) = argmin_{(\theta_{\mathrm{A}}, \theta_B)}(L_{AB}(\theta_{\mathrm{A}}, \theta_B)).$$

Опыт обучения сетей **A** и **B** (см. далее) показал, однако, что ошибка восстановления текста для **E** не должна стремиться к максимуму. Если **E** максимально ошиблась при дешифровании криптотекста, то есть неправильно распознала все символы исходного текста, то, выполнив инвертирование всех битов в следующей итерации, она получит корректный исходный тест. В силу чего оптимальным поведением для **A** и **B** является провоцирование сети **E** на создание результатов, близких к случайным. Для реализации описанного поведения в функции ошибок $L_{\mathrm{AB}}(\theta_{\mathrm{A}}, \theta_{\mathrm{B}})$ оставляем первую компоненту как «расстояние» между исходным текстом и результатом дешифровки **B**, а для вычисления второй компоненты предлагается следующая формула:

$$\left(\frac{N}{2} - L_E\right)^2 / \left(\frac{N}{2}\right)^2,$$

где N – размерность текста; L_{E} – функция, описывающая ошибку для **E**.

Такая модификация функции ошибок способствует приближению функционирования сети **E** к случайному угадыванию. Вторая компонента стремится к минимуму, когда половина битов сообщения верная, а вторая – нет. Квадратичный характер последней формулы позволяет делать акцент на том, когда **E** допускает максимальную ошибку, или, если её догадки были верными. Данное уточнение позволяет улучшить надежность обучения безопасной коммуникации сетей **A** и **B**.

Процесс обучения. Процесс обучения ИНС криптографической системы базируется на методе стохастического градиентного спуска. Для больших объемов данных этот метод по скорости превосходит стандартный метод градиентного спуска, известный в теории сетей как метод обратного распространения ошибок [18].

Входной поток данных, используемый для обучения системы, разбит на партии – эпохи, эпоха разбита на серию подпартий-батчей, за одну итерацию проходит один батч [6].

Оптимальное значение для параметров ИНС **E** не вычисляется для данного значения θ_{A}, а аппроксимируется, чередуя тренировки **E** с тренировками **A** и **B**. Для процесса обучения выбран следующий порядок: один батч для тренировки **A** и **B**, затем два батча для тренировки **E.**

Обучение происходит по следующему сценарию. **A** создает шифротекст, который изначально не понимают ни **B**, ни **E**. За несколько эпох **A** и **B** могут найти способ общения, который позволит **B** хотя бы частично расшифровывать сообщения **A**, которое все также остается непонятным для **E**. В частности, **A** и **B** могут использовать для безопасной коммуникации тривиальные преобразования, похожие на rot13 (представляет собой шифр подстановки обычной заменой для алфавита ан-

глийского языка) [23]. После нескольких итераций обучения сеть **E** может начать взламывать шифр **A**. В процессе обучения **A** и **B** могут совершенствовать безопасность обмена данными, создавая новые шифры, приводящие к увеличению ошибок дешифрования для **E**. В итоге **E** не сможет приспособить к новому шифру. Обучение прекращается, когда **A** и **B** создадут достаточно надежную криптосистему (то есть ошибка сети **B** не более 0,05 бит).

Далее подобранный системой шифр проверяется на криптостойкость. Обучаются экземпляры **E**, которые пытаются взломать систему. Параметры сети **E** сбрасываются, и затем она обучается заново 5 раз, при этом фиксируется лучший результат, достигнутый одним из вариантов **E**. Обученные таким образом экземпляры **E** назовем переподготовленными.

Если **A** и **B** не могут достичь необходимой точности за 150000 итераций, то обучение нейросистемы классифицируется как ***неуспешное***. Если переподготовленные для проверки стойкости шифра экземпляры **E** показывают хорошие результаты дешифрования, то обучение системы признается ***ненадежным***. В противном случае результат обучения считается ***успешным***.

Численный эксперимент. На основе описанного метода в среде разработки PyCharm на языке Python была реализована криптосистема, в которой безопасный обмен данными происходит с помощью ИНС.

Для разработки программы использовалась реализация библиотеки TensorFlow на языке Python. TensorFlow – это библиотека программного обеспечения с открытым исходным кодом, разработанная компанией Google и чаще всего использующаяся в задачах машинного обучения, в том числе обучения нейронных сетей [18]. Преимуществом TensorFlow является достаточно высокая скорость работы, особенно при использовании процессоров, имеющих архитектуру параллельных вычислений CUDA [14].

Программное обеспечение разрабатывалось согласно требованиям концепции MVC [11]: логика и интерфейс разделены и реализованы в отдельных модулях.

При инициализации программы пользователь задает необходимые параметры обучения: размер текста для шифрования, размер ключа, коэффициент обучения и количество эпох для обучения. Коэффициент скорости обучения – параметр градиентного метода обучения, позволяющий управлять величиной коррекции весов на каждой итерации. Экспериментально было установлено значение, равное 0?0008, что позволяет сетям **A**, **B** и **E** решительно реагировать на изменения в других компонентах системы, пока не будет достигнуто решение, устойчивое к изменениям в сети **E.**

Обучение проводилось для текста и ключа, размерами в 16 бит (значения 0 или 1). Графики функций ошибок сетей **B** и **E** на рисунке 2 (красная линия – сеть **B,**зеленая линия – сеть **E**) демонстрируют динамику успешного обучения системы при увеличении количества итераций. На горизонтальной оси указано пройденное количество эпох, на вертикальной – количество неверных бит при расшифровке текста. Результат считается идеальным, если количество неверных бит для **B** равно 0, а для **E** – 8 (т.е. половина от размера текста).

Начальный этап обучения (первые 1000 итераций) более детально показан на рисунке 3. Видно, что первые попытки добиться шифрования для безопасной коммуникации были не слишком удачными. Сети **B** на первых порах не удавалось достаточно точно дешифровать сообщения от **A**. Ошибка **E** была близка к ошибке **B**. Обучение проводилось всего за 1000 итераций. Следовательно, из этого можно сделать вывод, что за такое количество итераций, система не способна корректно определить параметры, позволяющие реализовать безопасную коммуникацию сетей **A** и **B.**

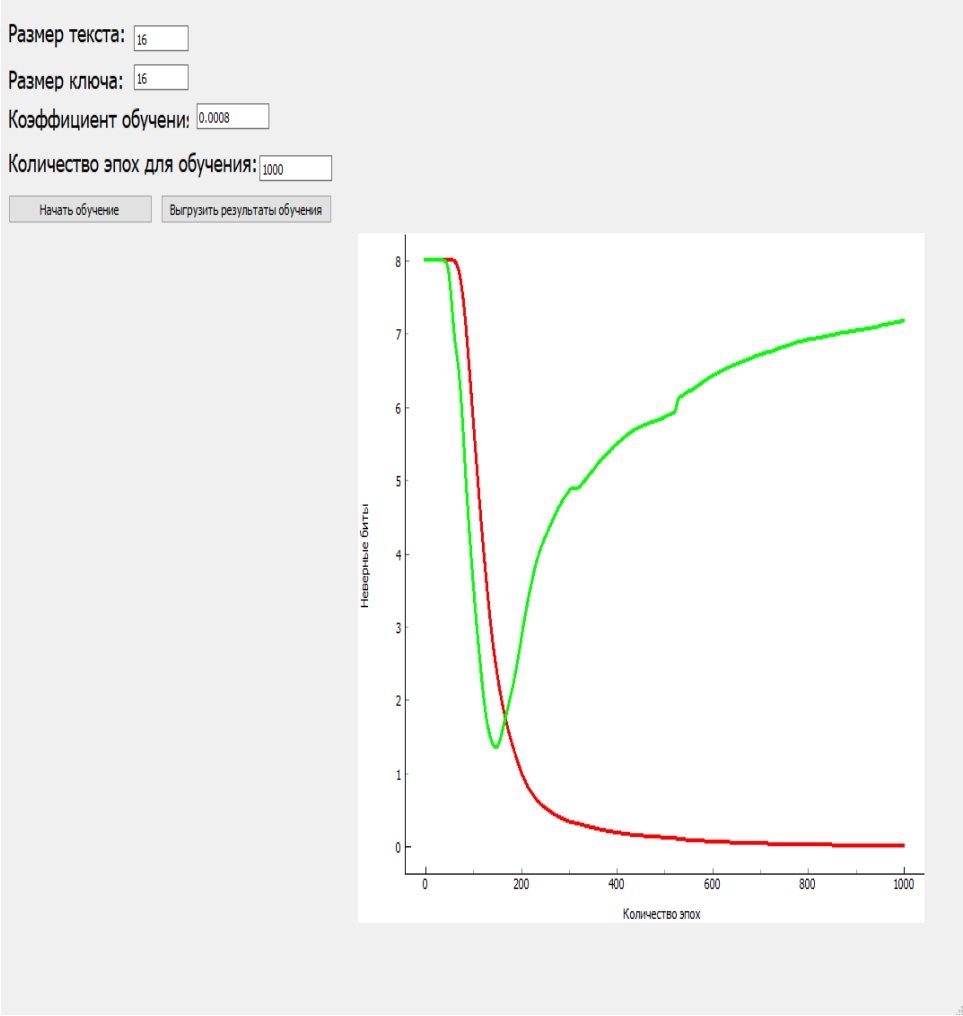


Рисунок 2 – Результаты обучения сетей **B** и **E**

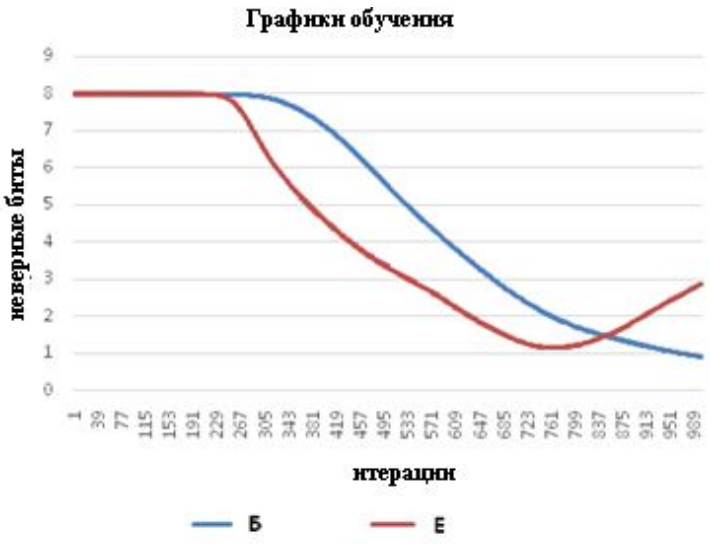


Рисунок 3 – Начальный этап обучения

Однако в процессе обучения (рис. 4) при увеличении количества эпох **A** и **B** начинают взаимодействовать намного лучше. После 10000 итераций успехи **B** превосходят успехи **E.**

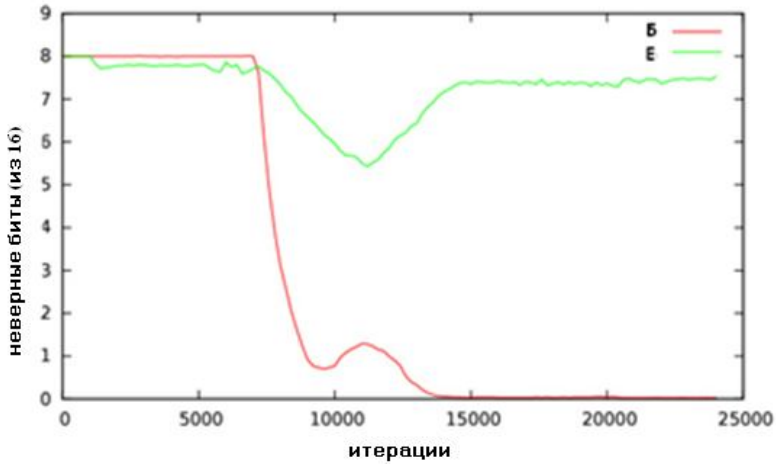


Рисунок 4 – Изменение количества ошибок дешифрования текста **B** и **E** во время обучения

Эксперимент подтвердил, что обучение не всегда является успешным. Так при N = 16 шесть из двадцати попыток создания оптимального метода коммуникации заканчивались неудачей. Иными словами, ошибка дешифрования для **B** не падала ниже порога 0,05, а ошибка дешифрования **E** была выше 7,3.

В четырнадцати успешных случаях сети **A** удалось разработать надежный метод передачи, который был понятен **B**, но **E** при этом не могла расшифровать сообщения. Если иногда сети **E** удавалось раскрыть систему шифрования сообщений двух других ИНС, то те после каждой удачной попытки **E** вновь модифицировали метод шифрования.

На рисунке 5, где представлены результаты обучения за более длительный период (до 150000 итераций), явно заметны «скачки» в процессе обучения. Представленный на рисунке график обучения не похож на типичный результат для ИНС, где он обычно изменяется монотонно. Это связано с тем, что когда **E** адаптируется к шифру **A**, то **A** снова перестраивает свой метод шифрования. Это снова увеличивает ошибку расшифрования для **E**, а ошибку **B**, наоборот, снижает до минимума.

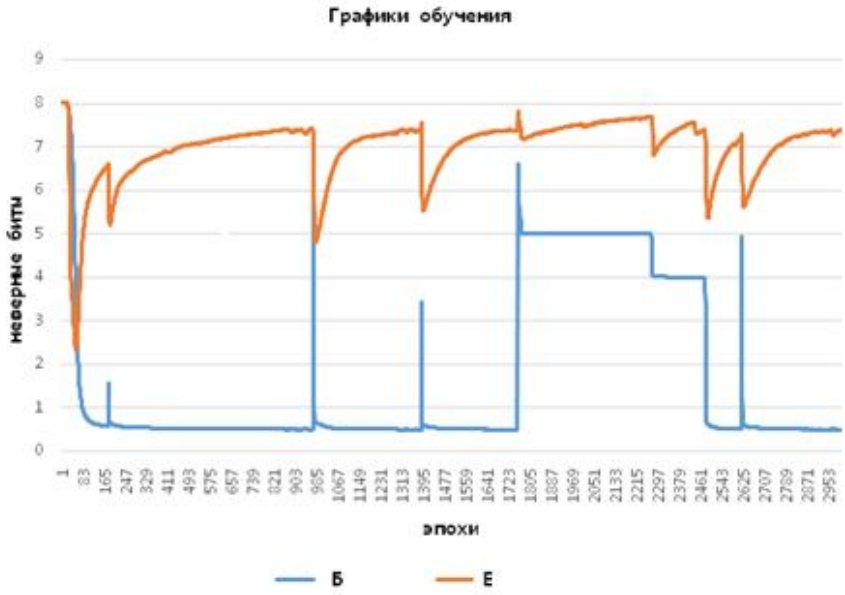


Рисунок 5 – Период длительного обучения

Таким образом, в данной работе показано, что при определенной организации генеративно-состязательного функционирования компонентов (ИНС) нейро-криптосистемы возможно автоматически поддерживать безопасную коммуникацию по защищенному каналу.

Заключение. Рассматриваемый в настоящей работе вариант механизма автоматической генерации нейросетями метода безопасной коммуникации представляется достаточно интересным для будущих разработок применением методов машинного обучения в криптографии. Результаты про-

веденных вычислительных экспериментов на основе модели состязательных ИНС свидетельствуют об их способности адаптироваться к криптографической ситуации в канале и автоматически разрабатывать простые способы шифрования сообщений, что согласуется с выводами работы [12].

Машинное обучение, применяемое в данном проекте, позволяет получить результат, но не демонстрирует путь его разработки. Поэтому точно не понятен алгоритм полученного метода шифрования.

Данный модельный проект можно усовершенствовать, если в основу его положить более сложный криптографический сценарий, гарантирующий не только секретность, но и, например, целостность передаваемой информации. Это вызовет включение в систему дополнительных компонент, например, **M** (Мэллори – "active attacker") – активного злоумышленника, способного изменять, подменять сообщения [3] в канале. Увеличение требований к системе безопасности, несомненно, приведет к усложнению ее логики и потребует значительного увеличения времени для получения необходимых результатов. Необходимым условием преодоления этих проблем можно считать возможность распараллеливания и высокую скорость вычислений в современных многопроцессорных системах.

Занимающийся вопросами шифрования специалист из компании PKWARE Джо Стуронас [20] подчеркивает, что «*методы работы с нейронными сетями начали развиваться на текущем уровне в последние несколько лет, поэтому мы лишь в начале пути*». Пока что человек без труда может взломать систему защиты информации, разработанной нейронными системами. Возможно, через некоторое время машины научатся создавать более надежные системы шифрования данных, на взлом которых человеку придется потратить немало времени, если он будет вообще в состоянии понять результат работы машин.

Библиографический список

1. Барский А. Б. Нейронные сети: распознавание, управление, принятие решений / А. Б. Барский. – Москва : Финансы и статистика, 2004 – 176 с.
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва : Директ-Медиа, 2015. – 253 с.
3. Защита информации и ЭПО. – Режим доступа: http://www.yztm.ru/ 2018/02/08/alicebk/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.10.2019).
4. Кочетов Д. А. Нейросетевая технология обнаружения сетевых вторжений / Д. А. Кочетов, Е. П. Лукащик // Прикаспийский журнал: управление и высокие технологии. – 2018. – №. 2 (42). – С. 104–112.
5. Лукащик Е. П. Применение нейронных сетей для обнаружения сетевых атак / Е. П. Лукащик, Д. А. Кочетов // Традиционная и инновационная наука: история, современное состояние, перспективы : сборник статей Международной научно-практической конференции (Уфа, 21.08.2017 г.). – Стерлитамак : АМИ, 2017. – С. 24–27.
6. Никоненко С. Глубокое обучение. Погружение в мир нейронных сетей / С. Никоненко, А. Кадурин, Е. Архангельская. – Санкт-Петербург : Питер, 2018. – 480 с.
7. Сверточные нейронные сети: взгляд изнутри. – Режим доступа: http://ru.datasides.com/code/cnn-convolutional-neural-networks/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 17.01.2020).
8. Сравнение безопасности популярных облачных хранилищ. – Режим доступа: https://falcongaze.ru/pressroom/publications/articles/compare-security-of-popular-cloud-services.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.02.2020).
9. Стельмах С. Нейронная сеть Google изобрела собственный протокол шифрования / С. Стельмах. – Режим доступа: https://www.itweek.ru, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 30.01.2020).
10. Шифрование облачных сервисов в компаниях и организациях**.** Блог компании КиберСофт, Информационная безопасность. – Режим доступа: https://habr.com/ru/company/cybersafe/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 13.12.2019).
11. Что такое MVC: базовые концепции и пример приложения. – Режим доступа: https://skillbox.ru/media/code/chto takoe mvc_bazovye_kontseptsii_i_primer_prilozheniya/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 24.02.2020).
12. Abadi M. Learning to protect communications with adversarial neural cryptography / M. Abadi, D. G. Andersen. – Режим доступа: http://arxiv.org/abs/1610.0698, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 07.04.2019).
13. Barthe Gilles. Fully automated analysis of padding-based encryption in the computational model / Barthe Gilles, Juan Manuel Crespo, Benjamin Gr. Egoire, C. Esar Kunz, Yassine Lakhnech, Benedikt Schmidt, and Santiago Zanella-B. Eguelin // Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications security, CCS'13. – NY, USA, 2013. – P. 1247–1260.
14. Ferguson Niels. Practical Cryptography / Ferguson Niels, Schneier Bruce. – Wiley Publishing, Inc., 2003. – 432 p.
15. IDC: The premier global market intelligence firm. – Режим доступа: https://www.idc.com, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 15.02.2020).
16. Mirza M. Conditional generative adversarial nets / M. Mirza, S. Osindero. – Режим доступа: https://arxiv.org/pdf/1411.1784.pdf, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 04.08.2019).
17. Nano news net. – Режим доступа: http://www.nanonewsnet.ru/ news/2016, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 24.05.2019).
18. Neelakantan A. Neural programmer: Inducing latent programs with gradient descent. CoRR, abs/1511.04834, 2015 / A. Neelakantan, Q. Le and I. Sutskever. – Режим доступа: http://arxiv.org/abs/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 14.04.2019).

19. Osipyan V. O. Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems / V. O. Osipyan, K. I. Litvinov, R. Kh. Bagdasaryan, E. P. Lukashchik, S. G. Sinitsa, A. S. Zhuk. – ACM Press, 2019. – P. 1–8.

20. Pkware Blog. – Режим доступа: http://www.pkware.com, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 25.12.2019).

21. Portio Research. The home of mobile messaging research. – Режим доступа: https://www.crunchbase.com/organization/portio-research, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 08.6.2019).

22. Rivest R. L. A method for obtaining digital signatures and public key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communication of the ACM. – 1978, Feb. – Vol. 21, issue 2. – P. 120–126.

23. Rot-13 Encryptor & Decryptor. – Режим доступа: http://www.decode.org/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 15.07.2019).

References

1. Barskiy A. B. *Neuronnye seti: raspoznavanie, upravlenie, prinyatie resheniy* [Neural nets: discernment, management, decision making]. Moscow, Finansy i statistika Publ., 2004. 176 p.

2. Ziginaylov Yu. N. *Teoriya informatsionnoy bezopasnosty i metodologiya zashchity informatsii : uchebnoe posobie* [Information security theory and information protection methodology : tutorial]. Moscow, Direkt-Media Publ., 2015. 253 p.

3. *Zashchita informatsii i EPO* [Information protection and EPO]. Available at: http://www.YZTM.ru/2018/02/08/alicebk/ (accessed 12.10.2019).

4. Kochetov D. A., Lukashchik E. P. Neyrosetevaya tekhnologiya obnaruzheniya setevykh vtorzheniy [Neural network technology to detect network intrusions]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2018, no. 2 (42), pp. 104–112.

5. Lukashchik E. P., Kochetov D. A. Primenenie neuronnyh setey dlya obnaruzheniya setevyh atak [Use of neural networks to detect network attacks]. *Traditsionnaya i innovatsionnaya nauka: istoriya, sovremennoye sostoyaniye, perspektivy : sbopnik statey mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Traditional and innovativescience: history, current status, prospects : proceeding of the international scientific-practical conference] (Ufa, 21.08.2017). Cterlitamak, AMI Publ., 2017, pp. 24–27.

6. Nikonenko S., Kadurin A., Arkhangelskaya E. *Glubokoe obuchenie. Pogruzhenie v mir neyronykh setey* [Deep learning. Dive into the world of neural networks]. Saint Petersburg, Piter Publ., 2018. 480 p.

7. *Svertochnye neyronye seti: vzglyad iznutri* [Convolutional neural networks: an inside view]. Available at: http://ru.datasides.com/code/cnn-convolutional-neural-networks/ (accessed 17.01.2020).

8. *Sravnenie bezopasnosty populyarnykh oblachnykh khranilishch* [Comparison of the security of popular cloud storage]. Available at: https://falcongaze.ru/pressroom/publications/articles/compare-security-of-popular-cloud-services.html (accessed 18.02.2020).

9. Stelmah S. *Neuronnya set Google uzobrela sobstvennyy protokol shifrovaniya* [Google neural network invents own encryption protocol]. Available at:https://www.itweek.ru (accessed 30.01.20).

10.*Shifrovanie oblachnykh servisov v kompaniyakh i organizatsiyakh. Blog kompanii KiberSoft. Informatsionaya bezopasnost* [Encryption of cloud services in companies and organizations. CyberSoft company blog, Information security]. Available at: https://habr.com/ru/company/cybersafe/ (accessed 13.12.2019).

11.*Chto takoe MVC: bazovye konceptsii i primer prilozeniya* [What is MVC: basic concepts and an example application]. Available at: https://skillbox.ru/media/code/chto_takoe_mvc_bazovye_kontseptsii_ i_primer_ prilozheniya/ (accessed 24.02.2020).

12. Abadi M., Andersen D. G. *Learning to protect communications with adversarial neural cryptography.* Available at: http://arxiv.org/abs/1610.0698 (accessed 7.04.2019).

13. Barthe Gilles, Juan Manuel Crespo, Benjamin Gr. Egoire, C. Esar Kunz, Yassine Lakhnech, Benedikt Schmidt, and Santiago Zanella-B.Eguelin. Fully automated analysis of padding-based encryption in the computational model. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications security, CCS'13.* NY, USA, 2013, pp. 1247–1260.

14. Ferguson Niels, Schneier Bruce. *Practical Cryptography*. Wiley Publishing, Inc., 2003. 432 p.

15. *IDC: The premier global market intelligence firm.* Available at: https://www.idc.com. (accessed 15.02.2020).

16. Mirza M., Osindero S. *Conditional generative adversarial nets*. Available at: https://arxiv.org/pdf /1411.1784.pdf/ (accessed 4.08.2019).

17. *Nano news net*. Available at: http://www.nanonewsnet.ru/ news/2016 (accessed 24.05.2019).

18. Neelakantan A., Le Q., and Sutskever I. *Neural programmer: Inducing latent programs with gradient descent. CoRR, abs/1511.04834, 2015.* Available at: http://arxiv.org/abs/ (accessed 14.04.2019).

19. Osipyan V. O., Litvinov K. I., Bagdasaryan R. Kh., Lukashchik E. P., Sinitsa S. G., Zhuk A. S. *Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems.* 2019, ACM Press, pp. 1–8.

20. *Pkware. Blog.* Available at: http://www.pkware.com (accessed 25.12.2019).

21. *Portio Research. The home of mobile messaging research.* Available at: https://www.crunchbase.com/organization/portio-research (accessed 08.06.2019).

22. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public key cryptosystems. *Communication of the ACM*, 1978, Feb., vol. 21, issue 2, pp. 120–126.

23. *Rot-13 Encryptor & Decryptor.* Available at: http://www.decode.org/ (accessed 15.07.2019).