ФГБОУ ВО «Пензенский государственный университет», г. Пенза;
ФГКОУ ВО «Воронежский институт МВД России», г. Воронеж;
ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж;
ФГБОУ ВО «Липецкий государственный педагогический университет», г. Липецк;
ФГБОУ ВО «Рязанский радиотехнический университет», г. Рязань;
ФГБОУ ВО «Оренбургский государственный университет», г. Оренбург;
ФГБОУ ВО «МИРЭА – Российский технологический университет», г. Москва;
ФГУП «18-й Центральный научно-исследовательский институт» МО РФ, г. Москва;
ФГАНУ «Институт сверхвысокочастотной полупроводниковой электроники
имени В. Г. Мокерова Российской академии наук» (ИСВЧПЭ РАН), г. Москва;
АО «Пензенский научно-исследовательский электротехнический институт», г. Пенза;
Пензенский филиал АО «Научно-технический центр "Атлас"», г. Пенза;
АО «Научно-производственное предприятие "Рубин"», г. Пенза;
АО «Производственное объединение "Электроприбор"», г. Пенза;
АО «Радиозавод», г. Пенза;
АО «Системы управления», г. Москва;
Общероссийская общественная организация «Российское научно-техническое
общество радиотехники, электроники и связи имени А. С. Попова», г. Тула;
«Научно-исследовательский и конструкторский институт радиоэлектронной техники» филиал
ФГУП НПЦ «Производственное объединение "Старт"» имени М. В. Проценко, г. Заречный;
ФГБОУ ВО «Петербургский государственный университет путей сообщения
императора Александра I», г. Санкт-Петербург;
Филиал АО «ПНИЭИ» Научно-исследовательское предприятие «Аргус», г. Пенза;
ООО «Научно-производственная фирма "Кристалл"», г. Пенза;
Филиал ФГКВОУ ВО «Военная академия Ракетных войск стратегического назначения
имени Петра Великого», г. Серпухов;
Обособленное подразделение ОАО «ИнфоТеКС», г. Пенза;
ООО «НПФ "КРУГ"», г. Пенза;
ООО «Научно-производственное предприятие "БиоКрипт"», г. Пенза;
ООО «АЛГОМАТ», г. Калининград

Безопасность информационных технологий

Сборник научных статей по материалам
III Всероссийской научно-технической конференции
(г. Пенза, 4 июня 2021 г.)

Том 1

Пенза Издательство ПГУ 2021

УДК 681.322
Б39

Безопасность информационных технологий : сб. науч. ст. по Б39 материалам III Всерос. науч.-техн. конф. (г. Пенза, 4 июня 2021 г.) : в 2 т. – Пенза : Изд-во ПГУ, 2021. – Т. 1. – 154 с.

ISBN 978-5-907456-82-2

Рассматриваются различные аспекты безопасности информационных технологий. Публикуемые материалы прошли рецензирование.

Издание предназначено для специалистов по безопасности информационных технологий, преподавателей, аспирантов, докторантов и студентов вузов.

УДК 681.322

URL: https://tsib.pnzgu.ru/BIT

Приказ
о подготовке и проведении Всероссийской научно-технической конференции «Безопасность информационных технологий» № 256/о от 12.04.2021.

ISBN 978-5-907456-82-2

УДК 004.056

О РОЛИ ИНФОРМАЦИОННОЙ И КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ МИРОВОЙ ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

В. И. Волчихин

Пензенский государственный университет, г. Пенза

Аннотация. Основным компонентом цифрового мира являются данные, передающиеся в открытой информационной среде. Современные технологии сопряжены с наиболее опасными угрозами цифровой эпохи – кибератаками. Кроме информационной безопасности, актуальной становится и кибербезопасность.

Ключевые слова: информационная безопасность, кибератака, коронавирус

ON THE ROLE OF INFORMATION AND CYBERSECURITY IN THE CONTEXT OF THE GLOBAL CORONAVIRUS PANDEMIC

V. I. Volchikhin

Penza State University, Penza

Abstract. The main component of the digital world is data transmitted in an open information environment. Modern technologies are associated with the most dangerous threats in the digital age, cyber attacks. In addition to information security, cybersecurity also becomes relevant.

Keywords: information security, cyber attacks, coronavirus

Волчихин В. И., председатель оргкомитета конференции, президент Пензенского государственного университета, заслуженный деятель науки РФ, доктор технических наук, профессор

Не секрет, что в современном мире роль информации, средств ее обработки, передачи и хранения значительно возросла. Средства вычислительной техники сейчас во многом определяют научно-технический потенциал государства, уровень его развития, образа жизни людей [1, 2].

Развитие мировых информационных ресурсов на фоне мировой пандемии коронавирусной инфекции COVID-19 превратило предоставление услуг во всех сферах жизнедеятельности современного общества в быстрорастущий сегмент e-commerce.

Цифровизация общества способствовала тому, что малый бизнес перешел на интернет-площадки, а всемирная пандемия коронавирусной инфекции COVID-19 только усилила эту тенденцию[3].

Переход в цифровой формат – это не только интернет-среда, но и цифровая версия бизнеса с официальными сайтами, аккаунтами в социальных сетях и т.д. При этом цифровой вид e-commerce в интернете стал важным компонентом маркетингового успеха.

В 2020 г. российский рынок e-commerce рос быстрее, чем во всем мире, и составил 58 %. По прогнозам исследователей, к 2024 г. он вырастет еще на 34 %. При этом на протяжении ближайших трех лет Россия, по словам экспертов в данной области, будет самым быстрорастущим рынком в мире [3].

Общее количество заказов во всех сегментах e-commerce выросло на 78 % до 830 млн. руб. Вместе с тем средний чек сократился на 14 % до 3260 руб. По мнению аналитиков, этому было несколько причин: россияне стали совершать в интернете даже самые мелкие покупки; онлайн-покупки стали доступнее за счет бесплатной или дешевой доставки; рост сегментов с низким средним чеком: интернет-аптек, локальных доставок продуктов питания и других [3].

Но технологии в цифровом пространстве сопряжены с угрозами проведения кибератак, и малый бизнес более уязвим перед киберугрозами, поскольку потенциальные хакеры знают, что малый бизнес испытывает нехватку ресурсов, в отличие от крупных корпораций, которые инвестируют в технологии и стратегии безопасности.

Процедуры и политика безопасности, защищающие цифровые сети, быстро меняются, поэтому бизнесу необходимо быть в курсе последних мер кибербезопасности, чтобы лучше защитить свое киберпространство от киберугроз. Некоторые из наиболее распространенных кибератак включают фишинг, нарушение данных и т.д.

На этом фоне отмечается тенденция повышения управления информационными потоками, поэтому складывается мнение, что миром владеет не тот, у кого много ценной информации, а тот, кто умело распоряжается всеми доступными информационными ресурсами и управляет информационными потоками [3–5].

Бытует мнение, что информация носит нематериальный характер, если не загружена на материальный носитель, при этом она способна играть важную роль, став предметом продажи [6]. С развитием информационных технологий появилась возможность неограниченно размножать информацию. Еще недавно для копирования материального носителя информации требовались значительные усилия и время; создавать копии могли в основном только специально подготовленные люди. На данный момент значительный объём информации хранится на цифровых материальных носителях, и копирование информации уже не является дорогостоящим процессом.

Анализ сложившейся ситуации еще раз подчеркнет приоритетность создания защищенных от внешних угроз информационных технологий нового поколения.

Открывая III Всероссийскую научно-техническую конференцию «Безопасность информационных технологий», хочу сказать, что она проходит в смешанном режиме: очно и дистанционно, на этот счет имеется определенный положительный опыт проведения предыдущей конференции в таком формате.

Актуальность докладов, включенных в программу работы конференции, свидетельствует о возрастании роли защиты информации, кибербезопасности, биометрической аутентификации пользователей.

Желаю всем участникам конференции крепкого здоровья и новых творческих успехов.

Список литературы

1. 43 статистических факта про ИБ во время COVID-19. URL: https://habr.com/ru/post/516916/

2. Марков А. Информационная безопасность в условиях пандемии COVID-19. URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnaya-bezopasnost-v-usloviyakh-pandemii-covid-19/?sphrase_id=35369216

3. URL: https://mega-obzor.ru/raznica-mezhdu-kiberbezopasnostyu-i-informacionnoj-bezopasnostyu.html

4. URL: https://performance360.ru/e-commerce-russia-2020-data-insight-2020/

5. URL: https://mega-obzor.ru/raznica-mezhdu-kiberbezopasnostyu-i-informacionnoj-bezopasnostyu.html

6. Атаманов Г. А. О цене и ценности информации. URL: https://bis-expert.ru/

Для цитирования: Волчихин В. И. О роли информационной и кибербезопасности в условиях мировой пандемии коронавирусной инфекции // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 3–6.

УДК 519.2, 004.622

КАЛЬКУЛЯТОР ДЛЯ ВЫЧИСЛЕНИЯ ЭНТРОПИИ КОДОВ 256 БИТ НА МАЛЫХ ВЫБОРКАХ

А. Г. Банных, А. П. Иванов, А. А. Пирогов

Пензенский государственный университет, г. Пенза

Аннотация. Разработанный программный калькулятор способен вычислять энтропию кодов 256 бит на малых выборках. Этого эффекта удается достичь за счет использования табличных значений энтропии, оформленных в виде базы данных пересчета математического ожидания и стандартного отклонения расстояний Хэмминга в энтропию выходных кодов нейросетевого преобразователя по ГОСТ Р 52633.3–2011. Разработанный программный калькулятор позволит заменить коммерческие программные продукты MathCAD, MathLAB и другие, способные выполнять вычисления с высокой разрядностью.

Ключевые слова: программный калькулятор, энтропия кодов 256 бит, математическое ожидание, высокая разрядность

CALCULATOR FOR CALCULATING THE ENTROPY OF 256 BIT CODES IN SMALL SAMPLES

A. G. Bannykh, A. P. Ivanov, A. A. Pirogov

Penza State University, Penza

Abstract. The developed software calculator is capable of calculating the entropy of 256-bit codes on small samples. This effect can be achieved through the use of tabular values of entropy designed in the form of a database for converting the mathematical expectation and standard deviation of Hamming distances into the entropy of the output codes of the neural network converter in accordance with GOST R 52633.3–2011. The developed software calculator will allow replacing commercial software products MathCAD, MathLAB and others capable of performing calculations with high bit depth.

Keywords: software calculator, entropy of 256-bit codes, mathematical expectation, high bit depth

Одной из проблем нейросетевой биометрии является необходимость использования малогабаритной физически и криптографически защищенной доверенной вычислительной среды [1], созданной с использованием малопотребляющих, низкоразрядных контроллеров при ограниченном объеме памяти. Это означает, что на малопо-

требляющих, низкоразрядных контроллерах необходимо точно вычислять интегралы вероятности

$$P \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{1} \exp\left\{ \frac{-\left(E(h)-u\right)^2}{2\left(\sigma(h)\right)^2} \right\} \cdot du. \qquad (1)$$

Вычислить интеграл (1) на процессорах с 32- или 64-разрядной арифметикой несложно. Однако при вычислении интеграла (1) на 4-, 8-разрядном контроллере возникают проблемы из-за низкой разрядности двоичных чисел и отсутствия возможности повышения точности (разрядности) вычислений. Проведенные в [2] исследования показали, что если при 32-разрядных вычислениях зафиксировать стандартное отклонение расстояний Хэмминга σ(h) и изменять только математическое ожидание расстояний Хэмминга $E(h)$, то можно получить почти линейную связь с оцениваемой энтропией (рис. 1). При использовании низкоразрядных контроллеров выгодно применять двумерные таблицы преобразований. В ячейках двухмерной таблицы должны лежать значения энтропии номограммы, отображенной на рис. 1.

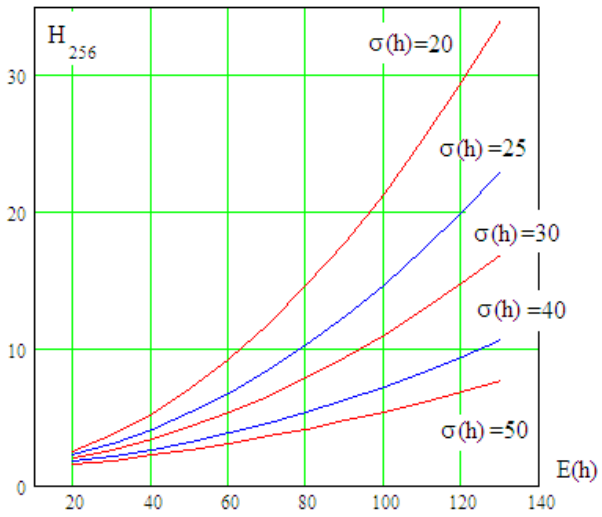


Рис. 1. Связь энтропии с математическим ожиданием расстояний Хэмминга при фиксированном стандартном отклонении

Получается, что вычисления вероятностных интегралов вида (1) можно заменить на табличные вычисления энтропии.

Полученные табличные значения энтропии оформлены в виде базы данных «База данных пересчёта математического ожидания и стандартного отклонения расстояний Хэмминга в энтропию выходных кодов нейросетевого преобразователя по ГОСТ Р 52633.3–2011».

По полученным табличным значениям энтропии [3] можно предложить следующий алгоритм интерполяции. Рассмотрим пример реализации вычислений исходя из условий получение реальных значений $E(h) = 41{,}2$ и $\sigma(h) = 23{,}6$, что соответствует фрагменту таблицы [3], представленному на рис. 2. Алгоритм интерполяции должен по этой таблице найти четыре ближайших значения энтропии, как это показано на рис. 2. Обратившись к таблице рис. 2, мы имеем четыре наиболее близких значения энтропии 4,7 бит, 4,3 бит, 5,5 бит, 4,9 бит. Первым очевидным решением задачи является усреднение, извлеченных из таблицы данных:

$$H\big(E(h),\sigma(h)\big) \approx \frac{4{,}7 + 4{,}3 + 5{,}5 + 4{,}9}{4} = 4{,}85 \text{ бита}.$$

$E(h)$	$\sigma(h)$							
	20	22	24	26	28	30	32	34
30	3,8	3,4	3,1	2,9	2,7	2,6	2,5	2,3
35	4,5	4,0	3,7	3,4	3,2	3,0	2,8	2,7
40	5,3	4,7	4,3	3,9	3,6	3,4	3,2	3,0
45	6,2	5,5	4,9	4,5	4,1	3,8	3,6	3,4
50	7,1	6,3	5,6	5,1	4,6	4,3	4,0	3,7
55	8,2	7,1	6,4	5,7	5,2	4,8	4,4	4,2

Рис. 2. Выделение четырех ближайших значений энтропии наиболее близких к реально полученным данным

В связи с тем, что приведенное преобразование двухмерно шаг используемой таблицы может быть в двое уменьшен интерполяцией ее данных, что эквивалентно растяжению таблицы в полтора раза, как это отображено на рис. 3.

Исходнаятаблица

	22	24	$\sigma(h)$
40	4,7	4,3	
45	5,5	4,9	
$E(h)$			

Растянутаятаблица

	22	23	24	$\sigma(h)$
40	4,7	4,5	4,3	
42,5	5,1	4,85	4,6	
45	5,5	5,2	4,9	
$E(h)$				

Рис. 3. Растяжение исходной таблицы в полтора раза на первом цикле интерполяции

Используя данные растянутой таблицы (см. рис. 3) получаем следующее значение энтропии:

$$H\big(E(h),\sigma(h)\big) = H(41.2, 23.6) \approx \frac{4{,}5 + 4{,}3 + 4{,}85 + 4{,}6}{4} = 4{,}5625 \text{ бита}.$$

Очевидно, что мы можем повторить процедуру увеличения в полтора раза таблицы, еще раз сократив в два раза шаг таблицы. В итоге мы получим растянутую таблицу на второй итерации, отображенную на рис. 4.

	23	24	σ(*h*)
40	4,5	4,3	
42,5	4,85	4,6	
E(*h*)			

Растянутаятаблица

	23	23,5	24	σ(*h*)
40	4,5	4,4	4,3	
41,25	4,675	4,5625	4,45	
42,5	4,85	4,725	4,6	
E(*h*)				

Рис. 4. Растяжение таблицы первой интерполяции в полтора раза на втором цикле интерполяции

Применяя данные второго растяжения таблицы, получим третье приближение таблично вычисленного значения энтропии:

$$H\big(E(h),\sigma(h)\big) = H(41.2, 23.6) \approx \frac{4{,}4 + 4{,}3 + 4{,}5625 + 4{,}45}{4} = \\ = 4{,}428125 \text{ бита}.$$

Подобные табличные итерационные вычисления должны продолжаться ограниченное число раз, так как на каждой шаге между данными таблицы уменьшается в два раза и очень быстро становится много меньше, чем шаги исходной таблицы. Практика подобных вычислений свидетельствует о то, что пяти итераций достаточно.

В соответствии с предложенным алгоритмом интерполяции по табличным значениям было разработано программное обеспечение для вычисления энтропии кодов 256 бит на малых выборках [4]. Программное обеспечение создана с помощью языка программирования C# на платформе .NETFramework 4.7.2. Целевая операционная система: Windows. Табличные данные хранятся в файле базы данных формата SQLite3.

Вначале запущенное приложение будет иметь вид, представленный на рис. 5.

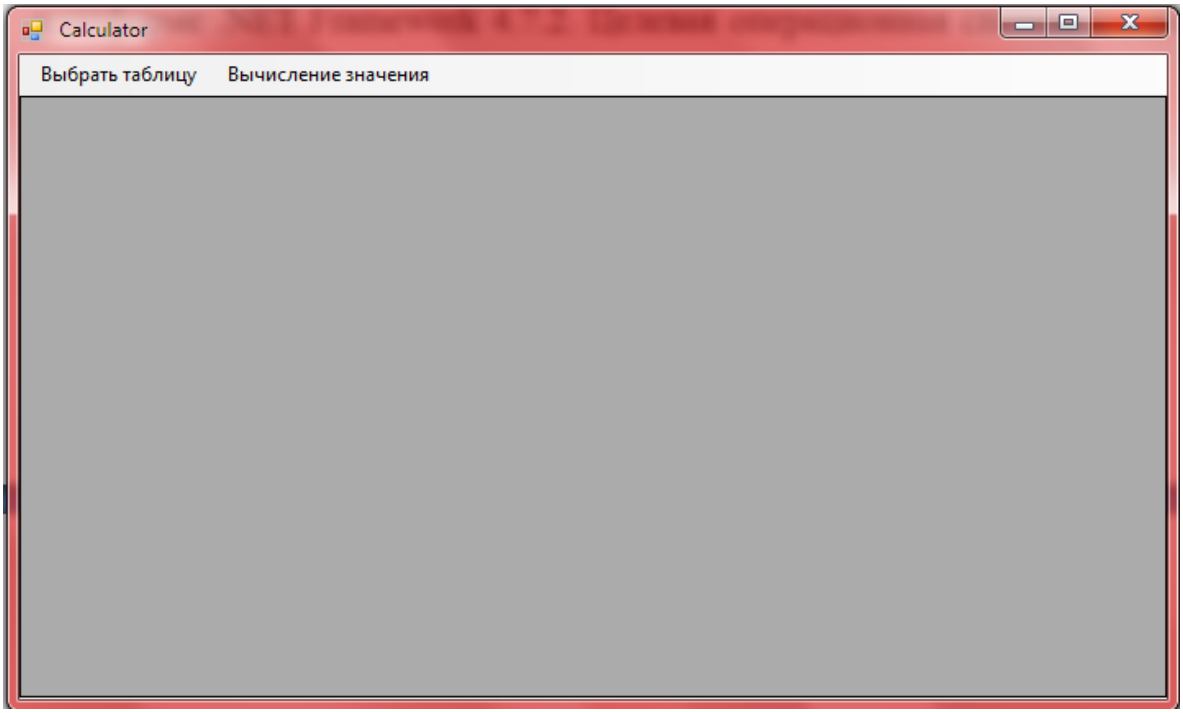
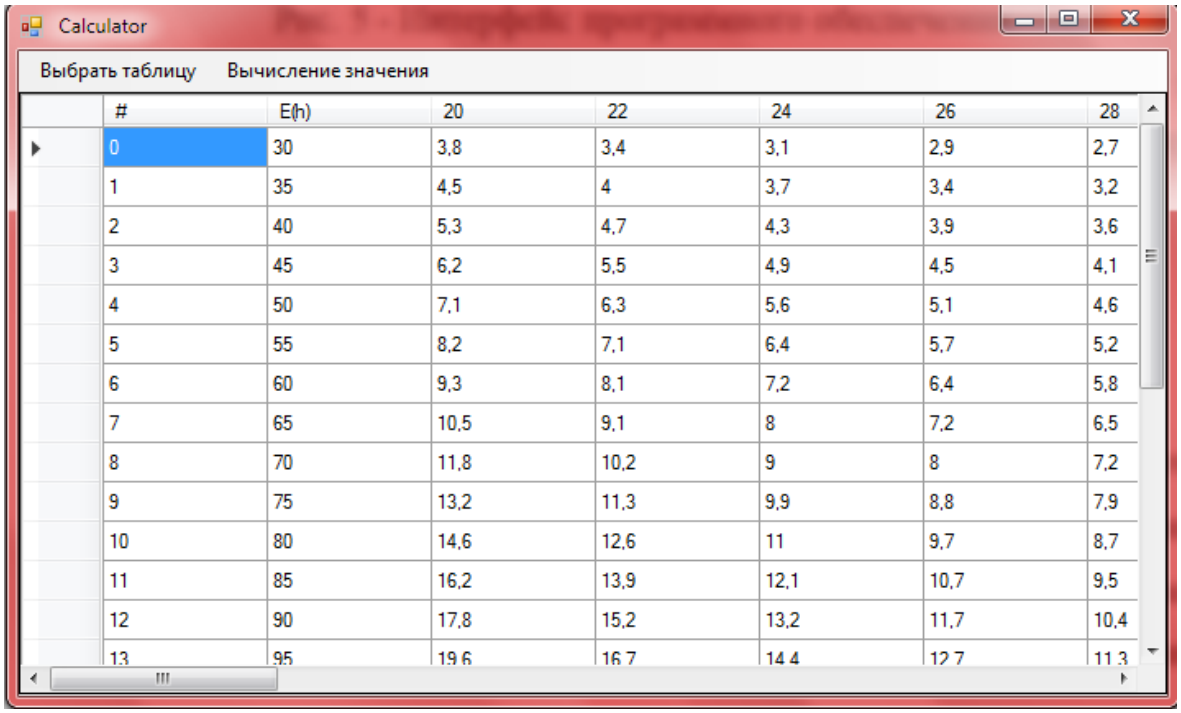


Рис. 5. Интерфейс программного обеспечения

Прежде чем начать вычисления, следует выбрать таблицу. После этого на экране отобразится таблица. Вид загруженной таблицы показан на рис. 6. Чтобы вычислить значение, нажмите на «Вычисление значения» в меню.



#	E(h)	20	22	24	26	28
0	30	3,8	3,4	3,1	2,9	2,7
1	35	4,5	4	3,7	3,4	3,2
2	40	5,3	4,7	4,3	3,9	3,6
3	45	6,2	5,5	4,9	4,5	4,1
4	50	7,1	6,3	5,6	5,1	4,6
5	55	8,2	7,1	6,4	5,7	5,2
6	60	9,3	8,1	7,2	6,4	5,8
7	65	10,5	9,1	8	7,2	6,5
8	70	11,8	10,2	9	8	7,2
9	75	13,2	11,3	9,9	8,8	7,9
10	80	14,6	12,6	11	9,7	8,7
11	85	16,2	13,9	12,1	10,7	9,5
12	90	17,8	15,2	13,2	11,7	10,4
13	95	19,6	16,7	14,4	12,7	11,3

Рис. 6. Загруженные табличные значения энтропии

После чего в диалоговой форме необходимо ввести реальные значения математического ожидания расстояний Хэмминга $E(h)$ и стандартного отклонения $\sigma(h)$ соответственно и нажать кнопку «Начать вычисление». Форма диалогового окна показана на рис. 7.

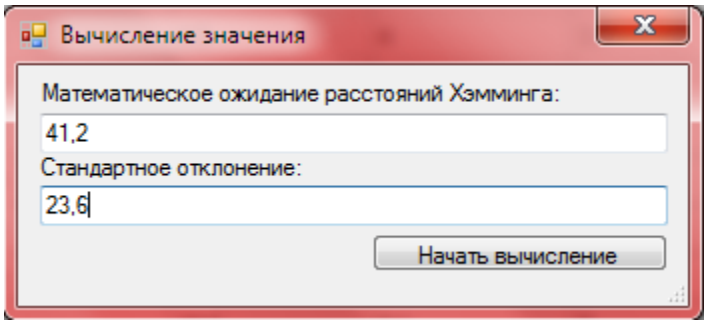


Рис. 7. Форма диалогового окна

Сначала программное обеспечение найдёт в таблице четыре ближайших значения энтропии и выведет их среднее арифметическое в виде сообщения MessageBox, показанного на рис. 8.

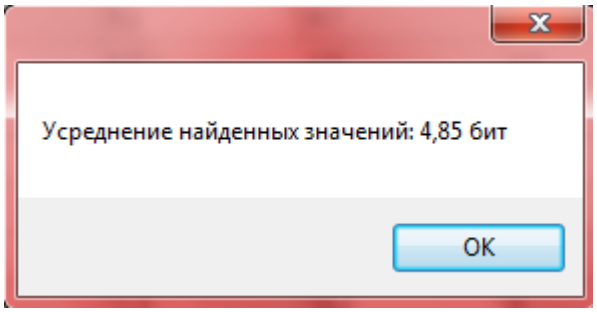


Рис. 8. Сообщение MessageBox

Затем будут произведены итерационные табличные вычисления, результаты которых будут также выведены в виде MessageBox. После каждой итерации предлагается их продолжить, либо остановить вычисления. Пример сообщения после первой итерации показан на рис. 9. После того, как остановятся вычисления, результаты будут записаны в файл отчета формата *txt*, который запустится автоматически. На рис. 10 показано содержимое файла отчета. Как видно из результатов вычисления представленных на рис. 10 они полностью совпадают с результатами выполненными в ручную.

Итак, наличие простой линейной связи между энтропией и стандартным отклонением позволяет создать простые малоразрядные калькуляторы для быстрого и эффективного вычисления энтро-

пии. Простота таких калькуляторов и их низкая разрядность обусловлены том, что они фактически решают задачу интерполяции данных по прошитой в памяти контроллера таблице.

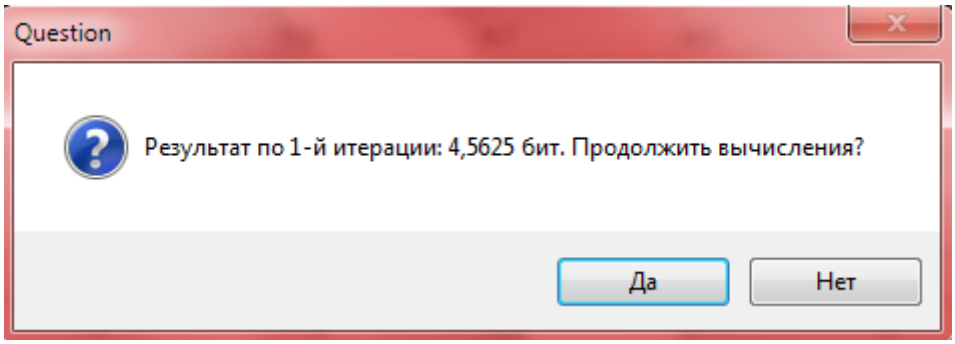


Рис. 9. Сообщение о результате после первой итерации

Усреднение найденных значений: 4,85 бит
Результат по 1-й итерации: 4,5625 бит
Результат по 2-й итерации: 4,428125 бит
Результат по 3-й итерации: 4,49453125 бит
Результат по 4-й итерации: 4,5283203125 бит

Рис. 10. Результаты вычисления

Таким образом, быстрые вычисления энтропии возможно выполнить на 4-, 8-разрядных контроллерах с малым объемом оперативной и долговременной памяти.

Список литературы

1. Иванов А. И., Банных А. Г. Быстрая оценка энтропии длинных кодов с зависимыми разрядами на микроконтроллерах с малым потреблением и низкой разрядностью (обзор литературы по снижению размерности задачи) // Инженерные технологии и системы. 2020. Т. 30, № 2. С. 300–312. doi:10.15507/2658-4123.030.202002.300-312

2. Банных А. Г. Восьмибитные таблицы связывания энтропии 256-битных кодов с математическим ожиданием и стандартным отклонением расстояний Хэмминга // Безопасность информационных технологий : сб. науч. ст. по материалам II Всерос. науч.-техн. конф. Пенза : Изд-во ПГУ, 2020. С. 118–123.

3. Свидетельство о государственной регистрации базы данных № 2021621381. База данных пересчета математического ожидания и стандартного отклонения расстояний Хэмминга в энтропию выходных кодов нейросетевого преобразователя по ГОСТ Р 52633.3–2011 / А. Г. Банных, А. И. Иванов, А. П. Иванов, А. А. Пирогов. Заявка № 2021620453 ; заявл. 17.03.2021 ; зарег. 25.06.2021.

4. Свидетельство о государственной регистрации программы для ЭВМ № 2021614767. Калькулятор для вычисления энтропии кодов 256 бит на малых выборках / А. Г. Банных, А. И. Иванов, А. П. Иванов, А. А. Пирогов. Заявка № 2021613966 ; заявл. 26.03.2021 ; зарег. 30.03.2021.

Для цитирования: Банных А. Г., Иванов А. П., Пирогов А. А. Калькулятор для вычисления энтропии кодов 256 бит на малых выборках // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 7–14.

УДК 621.391

РАСЧЕТ НЕОБХОДИМОГО ОБЪЕМА СТАТИСТИЧЕСКОГО ЭКСПЕРИМЕНТА В ЗАДАЧЕ ИССЛЕДОВАНИЯ ВОЗМОЖНОСТЕЙ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ДАННЫХ

Б. В. Султанов, С. Л. Зефиров, В. В. Дорошкевич

Пензенский государственный университет, г. Пенза

Аннотация. Рассмотрена методика расчета объема статистического вычислительного эксперимента по определению вероятности ошибочного приема переданных символов в системе передачи данных.

Ключевые слова: статистический вычислительный эксперимент, вероятность ошибочного приема, система передача данных

CALCULATION OF THE REQUIRED AMOUNT OF STATISTICAL DATA AN EXPERIMENT IN THE TASK OF INVESTIGATING THE POSSIBILITIES OF ENSURING THE INTEGRITY OF INFORMATION DURING DATA TRANSMISSION

B. V. Sultanov, S. L. Zefirov, V. V. Doroshkevich

Penza State University, Penza

Abstract. A method for calculating the volume of a statistical computational experiment to determine the probability of erroneous reception of transmitted symbols in a data transmission system is considered.

Keywords: statistical computational experiment, probability of erroneous reception, data transmission system

Передача данных в настоящее время является одним из наиболее распространенных видов связи. При этом существуют и постоянно обновляются различные методы обработки сигналов в телекоммуникационных системах, обеспечивающие минимально возможные потери информации при известных характеристиках используемого канала связи и скорости передачи.

Для оценки применимости конкретного метода в заданных условиях в отдельных случаях можно воспользоваться существую-

щими результатами теоретических исследований [1], однако более универсальным является подход, основанный на имитационном моделировании исследуемой системы. Результатом такого вычислительного эксперимента обычно является определение вероятности ошибочного приёма переданных символов в рассматриваемых условиях.

Точность и достоверность экспериментальной оценки вероятности ошибки зависят от количества испытаний.

Будем рассматривать передачу каждого символа как одно независимое вероятностное испытание с двумя возможными исходами: правильный прием (вероятность q) и ошибочный прием (вероятность $p = P_{\text{ош}}$). В этом случае необходимый объём испытаний можно вычислить, пользуясь интегральной теоремой Муавра-Лапласа [2], согласно которой справедливо соотношение

$$P_{\text{д}}\left(\left| \frac{m}{n} - p \right| < \varepsilon \right) \approx \Phi\left(\varepsilon \sqrt{\frac{n}{p\,q}} \right), \qquad (1)$$

где m – число произошедших событий (число ошибок);

n – общее число испытаний (объём статистического эксперимента);

p – ожидаемое значение вероятности того, что событие произойдет (вероятности ошибки);

$q = 1 - p$;

$\Phi(x)$ – функция Крампа;

ε – абсолютная погрешность оценки вероятности ошибки (доверительный интервал);

$P_{\text{д}}\left(\left| \frac{m}{n} - p \right| < \varepsilon \right)$ – вероятность того, что отношение $\frac{m}{n}$ будет оценкой p с абсолютной погрешностью меньшей ε (доверительная вероятность).

Значения функции

$$\Phi(x) = \sqrt{\frac{2}{\pi}} \int_0^x e^{\frac{t^2}{2}} dt \qquad (2)$$

(или линейным образом связанных с ней других аналогичных функций) подробно табулированы и приводятся в математических справочниках [3].

Однако в современных условиях для их вычисления удобно воспользоваться возможностями, предоставляемыми компьютером, и, в частности, свободно распространяемым программным пакетом *Scilab*. Присутствующая в этом пакете команда $cdfnor("PQ", x, \mu, D)$ обеспечивает вычисления интеграла вероятностей

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{x-\mu}{\sqrt{D}}} e^{-\frac{t^2}{2}} dt . \qquad (3)$$

Полагая в формуле (3) $\mu = 0$, $D = 1$, и учитывая, что при этих условиях

$$F(0) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{0} e^{-\frac{t^2}{2}} dt = \frac{1}{2},$$

нетрудно показать, что задаваемая выражением (2) функция $\Phi(x)$ связана с $F(x)$ соотношением

$$\Phi(x) = 2 \cdot [F(x) - \frac{1}{2}] = 2F(x) - 1. \qquad (4)$$

С учетом (4) выражение (1) принимает вид:

$$P_{\text{д}}\left(\left| \frac{m}{n} - p \right| < \varepsilon \right) = 2\, F\left(\varepsilon \sqrt{\frac{n}{p\, q}} \right) - 1,$$

откуда

$$F\left(\varepsilon \sqrt{\frac{n}{p\, q}} \right) = \frac{1}{2} \left[P_{\text{д}}\left(\left| \frac{m}{n} - p \right| < \varepsilon \right) + 1 \right]. \qquad (5)$$

Задаваясь значениями доверительного интервала ε и доверительной вероятности $P_{\text{д}}\left(\left| \frac{m}{n} - p \right| < \varepsilon \right)$, при каждом предполагаемом значении p можно найти необходимое значение n. Для этого:

1) по требуемой величине $P_{\text{д}}$ рассчитывается численное значение y, равное правой части выражения (5):

$$y = \frac{1}{2} \left[P_{\text{д}}\left(\left| \frac{m}{n} - p \right| < \varepsilon \right) + 1 \right];$$

2) с помощью таблиц или компьютера определяется значение $x = \varepsilon \sqrt{\frac{n}{p\,q}}$ аргумента функции $F\left(\varepsilon \sqrt{\frac{n}{p\,q}}\right)$, при котором выполняется равенство (5). С использованием компьютера в программном пакете *Scilab* данная процедура реализуется посредством команды $x = cdfnor\,("X", 0, 1, y, 1-y)$, осуществляющей вычисление аргумента x интеграла вероятностей (3) с $\mu = 0$ и $D = 1$, значение которого равно y.

3) из уравнения $x = \varepsilon \sqrt{\frac{n}{p\,q}}$ определяется необходимое значение n:

$$n = \frac{x^2}{\varepsilon^2}\, p\,q = \frac{x^2}{\varepsilon^2}\, p\,(1-p).$$

Величину ε удобно задавать в виде

$$\varepsilon = \gamma\, p,$$

где γ относительная погрешность оценки вероятности ошибки.

При этом выражение для определения n трансформируется к виду:

$$n = \frac{x^2}{(\gamma\, p)^2}\, p\,(1-p) = \frac{x^2}{\gamma^2}\,\frac{(1-p)}{p}.$$

Полученный результат показывает, что с уменьшением значения ожидаемой вероятности ошибки p, объём эксперимента n, необходимый для обеспечения заданных доверительного интервала ε и доверительной вероятности $P_д$ увеличивается.

Поэтому при планировании статистического эксперимента в качестве ожидаемого значения p следует выбирать его предполагаемое минимальное значение $p_{\min}$, которое должен обеспечить исследуемый метод в заданных условиях.

Ниже приводится пример использования описанной методики расчёта.

Пример. Выберем значение доверительного интервала ε и доверительной вероятности $P_д$ равными $\varepsilon = 0,2\ p$ и $P_д\left(\left|\frac{m}{n} - p\right| < \varepsilon\right) = 0,9.$

При этом $y = \frac{1}{2}(0,9+1) = 0,95$; $x = cdfnor\ ("X",0,1,0.95,1-0.95) \approx 1,645$;

при выбранном значении p получаем $n = \frac{1,645^2}{(0,2p)^2} p(1-p) \approx 67,65 \frac{1-p}{p}$.

Список литературы

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение : пер. с англ. / под общ. ред. А. В. Назаренко. М. : Вильямс, 2003. 1104 с.

2. Гмурман В. Е. Теория вероятностей и математическая статистика. М. : Высш. шк., 2003. 480 с.

3. Корн Г., Корн Т. Справочник по математике. Для научных работников и инженеров. М. : Наука, 1974. 832 с.

Для цитирования: Султанов Б. В., Зефиров С. Л., Дорошкевич В. В. Расчет необходимого объема статистического эксперимента в задаче исследования возможностей обеспечения целостности информации при передаче данных // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 15–19.

УДК 621.391

КОРРЕЛЯЦИОННЫЙ ТЕСТ НА БЛИЗОСТЬ К «БЕЛОМУ» ШУМУ ДЛИННЫХ ОСМЫСЛЕННЫХ ПАРОЛЬНЫХ ФРАЗ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПРОГРАММНОГО ГЕНЕРАТОРА

А. В. Строков[1], А. И. Иванов[2]

[1]Организационно-технические решения, г. Москва

[2]Пензенский научно-исследовательский электротехнический институт, г. Пенза

Аннотация. Рассмотрены вопросы проверки качества криптографических ключей, получаемых из нестабильной компоненты биометрических данных.

Ключевые слова: криптографические ключи, биометрические данные, «белый» шум

CORRELATION TEST FOR CLOSENESS TO "WHITE" NOISE OF LONG MEANINGFUL PASSWORD PHRASES AND PSEUDO-RANDOM SEQUENCES OF A SOFTWARE GENERATOR

A. V. Strokov[1], A. I. Ivanov[2]

[1]Organizational and Techological Solutions, Moscow

[2]Penza Research Electrotechnical Institute, Penza

Abstract. The issues of quality control of cryptographic keys obtained from an unstable component of biometric data are considered.

Keywords: cryptographic keys, biometric data, "white noise"

Известно, что длинные осмысленные парольные фразы пользователи легко запоминают, однако такие пароли очень далеки от идеального «белого» шума [1, 2]. Тем не менее, в среде математического моделирования MathCAD мы можем легко воспроизвести достаточно длинную осмысленную парольную фразу из 83 букв, как это показано на рис. 1.

Далее исполняемая программа рис. 1 выполняет перевод в 8-битный код каждый из 83 знаков кириллицы осмысленного пароля.

На рис. 2 представлена программа, которая выполняет сдвиг данных на три бинарные позиции образованной осмысленным паролем бинарной последовательности и вычисляет коэффициент корреляции между исходной последовательностью и тремя последовательностями со сдвигом.

PR := "Рукописная биометрия имеет значительную нестабильную компоненту до 30%_от стабильной"

rr := str2vec(PR) last(rr) = 83

D2B(x) :=
for i ∈ 0..7
  $V_i \leftarrow \mathrm{mod}(x,2)$
  $x \leftarrow \mathrm{floor}\left(\frac{x}{2}\right)$
V

i := 0..last(rr)

$x^{\langle i \rangle} := D2B(rr_i)$

x =

	71	72	73	74	75	76	77	78	79	80	81	82	83
0	0	0	0	1	0	0	1	0	1	0	1	0	1
1	1	1	0	0	1	0	0	0	1	0	0	1	0
2	1	0	0	0	0	0	0	0	0	1	1	1	0
3	1	0	0	0	0	0	0	1	1	1	1	1	1
4	1	0	0	0	0	1	1	1	1	0	1	1	1
5	1	0	1	0	0	1	1	1	1	0	1	1	1
6	0	1	0	1	1	0	0	0	0	1	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	...

Рис. 1. Формирования бинарной последовательности длинной 83 символов в 8-ми битной кодировке

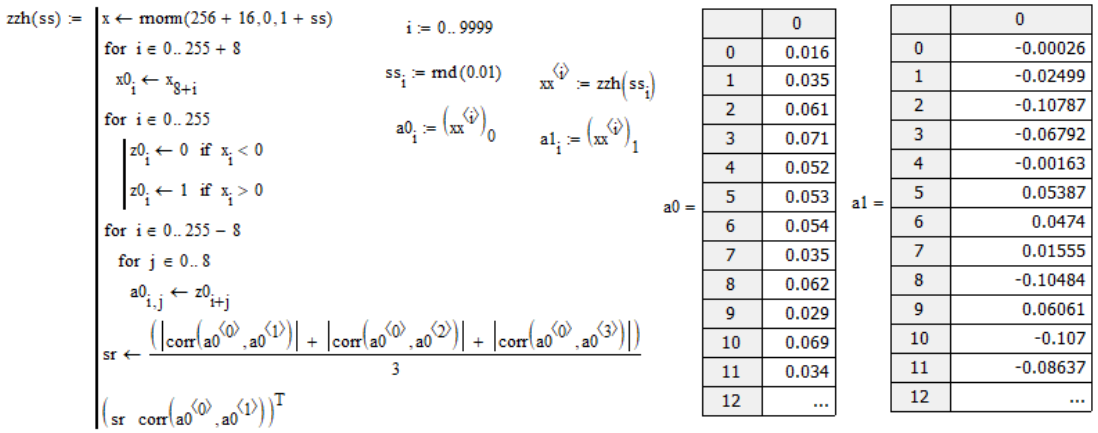
zz1(y) :=
for i ∈ 0..255 − 8
  $z_i \leftarrow y_i$
  $x1_i \leftarrow y_{i+1}$
  $x2_i \leftarrow y_{i+2}$
  $x3_i \leftarrow y_{i+3}$
$skr \leftarrow \frac{(|\mathrm{corr}(z,x1)| + |\mathrm{corr}(z,x2)| + |\mathrm{corr}(z,x3)|)}{3}$

Рис. 2. Формирование сдвигов на 1, 2, 3 бинарных отсчетов и вычисление суммы коэффициентов корреляции

Среднее значение модулей коэффициентов корреляции далее будем рассматривать как новый критерий оценки анализируемой последовательности на ее близость к «белому» шуму. В итоге мы полу-

чаем несколько десятков оценок коррелированности осмысленных паролей, сдвинутых от друг друга на один символ (на 8 бит).

Для того чтобы тот же самый статистический критерий близости к «белому» шуму проверить на данных, полученных от программного генератора псевдослучайных чисел была написана программная реализация численного эксперимента, приведенная на рис. 3.



	0
0	0.016
1	0.035
2	0.061
3	0.071
4	0.052
5	0.053
6	0.054
7	0.035
8	0.062
9	0.029
10	0.069
11	0.034
12	...

	0
0	-0.00026
1	-0.02499
2	-0.10787
3	-0.06792
4	-0.00163
5	0.05387
6	0.0474
7	0.01555
8	-0.10484
9	0.06061
10	-0.107
11	-0.08637
12	...

Рис. 3. Синтез псевдослучайных последовательностей
и вычисление их коэффициентов автокорреляции

Получать псевдослучайные реализации от программного генератора достаточно просто, программа рис. 3 анализирует 10 000 таких реализаций. Также, как и предыдущая программа рис. 2, она выполняет сдвиг данных на один бит и вычисление среднего модулей коэффициентов корреляции (нового статистического критерия).

На рис. 4 представлены данные имитационного моделирования статистических оценок длинных осмысленных паролей и псевдослучайных последовательностей программного генератора.

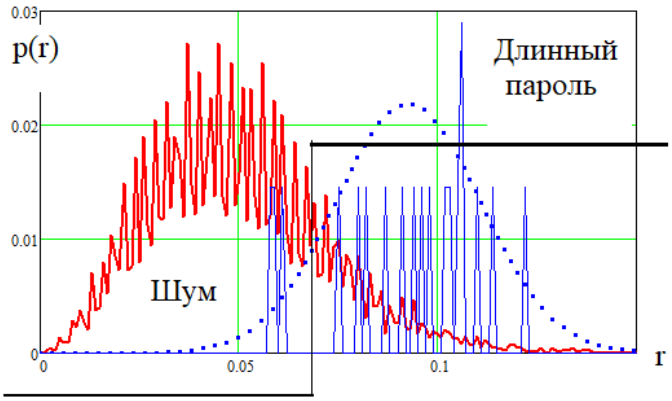


Рис. 4. Линейная разделимость откликов корреляционного критерия
на парольную фразу и псевдослучайную последовательность

Так как данных о значениях нового корреляционного статистического критерия для длинных осмысленных пароле мало, по этим данным вычислено их математическое ожидание и их стандартное отклонение. Далее использована гипотеза нормального распределения исследуемой зависимости.

Из рис. 4 виден эффект хорошей линейной разделимости длинных осмысленных паролей и псевдослучайных последовательностей. Это означает, что мощность нового корреляционного критерия оценки близости к «белому» шуму случайных последовательностей выше, чем у критериев, построенных на вычислении сверток Хэмминга [3–6]. Свертки Хэмминга, вычисленные по разным модулям, с одной стороны, имеют линейную вычислительную сложность, а с другой стороны не обеспечивают линейную разделимость случайных последовательностей и последовательностей с зависимыми разрядами кода.

Таким образом, следует ожидать существенного улучшения проверки качества криптографических ключей, получаемых из нестабильной компоненты биометрических данных [7] если к фильтрам на свертках Хэмминга добавить фильтры, построенные на, предложенном выше корреляционном критерии.

Список литературы

1. Иванов А. И., Фунтиков В. А., Майоров А. В., Надеев Д. Н. Моделирование кодовых последовательностей с энтропией естественных и искусственных биометрических языков // Инфокоммуникационные технологии. 2010. Т. 8, № 4. С. 75–79. URL: //ikt.psuti.ru

2. Малыгина Е. А., Иванов А. И., Язов Ю. К., Надеев Д. Н. Прогнозирование значений энтропии длинных кодовых последовательностей, порождаемых естественными и искусственными языками // Инфокоммуникационные технологии. 2014. Т. 12, № 2. С. 12–15. URL: //ikt.psuti.ru/upload/File/2010/37.pdf

3. Юнин А. П., Иванов А. И., Ратников К. А., Кольчугина Е. А. Оценка качества «белого» шума: реализация теста «стаи обезьян» через множество сверток Хэмминга, построенных на разных системах счисления // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 4 (48). С. 54–64.

4. Волчихин В. И., Иванов А. И., Карпов А. П., Юнин А. П. Условия корректного вычисления энтропии осмысленных длинных паролей в пространстве сверток Хемминга с эталонными текстами на русском и английском языках // Измерение. Мониторинг. Управление. Контроль. 2019. № 3. С. 15–21.

5. Юнин А. П., Иванов А. И., Ратников К. А. Оценка качества «белого шума»: реализация теста «стаи обезьян» через множество сверток Хэмминга для разных систем счисления // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза, 2019. С. 10.

6. Карпов А. П., Юнин А. П. Условия корректного вычисления энтропии осмысленных длинных паролей в пространстве сверток Хэмминга с эталонными текстами на русском и английском языках // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза, 2019. С. 59–65.

7. Иванов А. И., Юнин А. П. Эмбрион искусственного интеллекта: компактная нейросетевая проверка качества случайных последовательностей, полученных из биометрических данных. Пенза : Изд-во ПГУ, 2021. 67 с.

Для цитирования: Строков А. В., Иванов А. И. Корреляционный тест на близость к «белому» шуму длинных осмысленных парольных фраз и псевдослучайных последовательностей программного генератора // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 20–24.

УДК 004.056

СИНТЕЗ КЛЮЧЕЙ ИЗ СЛУЧАЙНОЙ КОМПОНЕНТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ В УСЛОВИЯХ ПРИМЕНЕНИЯ ОГРАНИЧЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ SIM-КАРТ, MICROSD-КАРТ ДЛЯ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ ХЭШИРОВАНИЯ И ТЕСТИРОВАНИЯ

А. П. Юнин[1], С. А. Сомкин[2], А. П. Иванов[3]

[1,2]Пензенский научно-исследовательский электротехнический институт, г. Пенза

[3]Пензенский государственный университет, г. Пенза

Аннотация. Рассматривается проблема формирования нейросетевого искусственного интеллекта, размещенного в доверенную среду с малыми вычислительными ресурсами по памяти, разрядности, потреблению, например, в виде SIM-карт, microSD-карт, RFID-токенов. Показано, что требования к вычислительным ресурсам могут быть значительно снижены при хэшировании данных и при тестировании качества криптографических ключей.

Ключевые слова: синтез ключей, нейросетевой искусственный интеллект, хэширование, тестирование, криптографические ключи

KEY SYNTHESIS FROM A RANDOM COMPONENT OF BIOMETRIC DATA UNDER CONDITIONS OF USING LIMITED COMPUTING RESOURCES OF SIM-CARDS, MICRO SD CARDS TO PERFORM HASHING AND TESTING OPERATIONS

A. P. Yunin[1], S. A. Somkin[2], A. P. Ivanov[3]

[1,2]Penza Research Electrotechnical Institute, Penza

[3]Penza State University, Penza

Abstract. The problem of forming a neural network artificial intelligence placed in a trusted environment with small computing resources in terms of memory, bit depth, and consumption, for example, in the form of SIM cards, micro SD cards, and RFID tokens, is considered. It is shown that the requirements for computing resources can be significantly reduced when hashing data and testing the quality of cryptographic keys.

Keywords: key synthesis, neural network artificial intelligence, hashing, testing, cryptographic keys

Доверенные вычисления, оперирующие с данными биометрии и криптографии должны выполняться в токене. Открытые данные биометрии и данные о криптографическом ключе не должны покидать токен. Создавать личный ключ от программного генератора [1], опираясь на некоторую «соль» зашитую в токен производителем нежелательно. Это может вызывать вопросы у пользователя, так как он не может контролировать производителя и должен верить сертификату на токен.

Доверие к токену растет, если пользователь уверен в том, что он лично создает свой личный ключ своими руками. В качестве источника случайных данных может быть использована случайная компонента биометрии, например, может быть использован рукописный почерк [2]. Пример экранной формы ввода динамики воспроизведения рукописного пароля приведен на рис. 1.

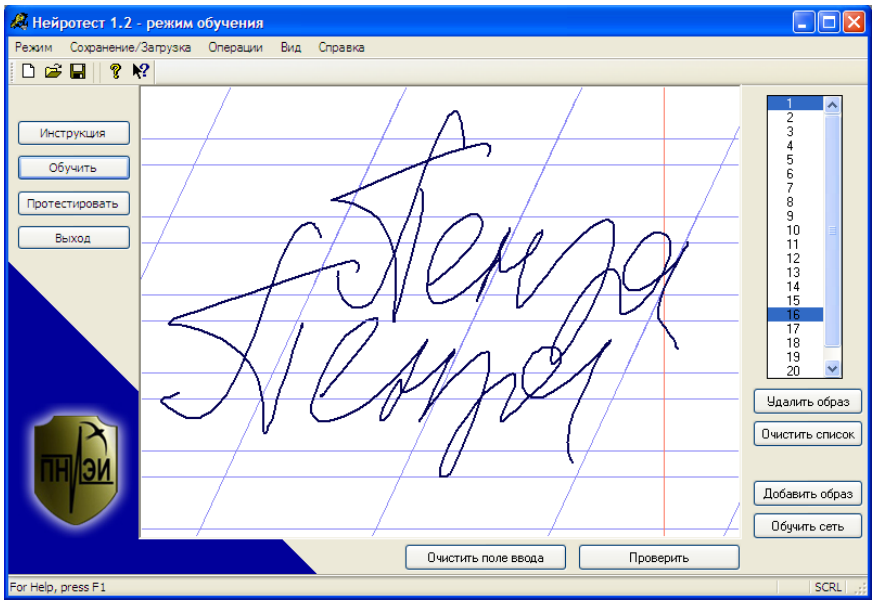


Рис. 1. Естественные различия двух рукописных примеров с номерами 1 и 16 в обучающей выборке среды моделирования «БиоНейроАвтограф» [2]

Очевидным является то, что человек не может однозначно воспроизвести своим почерком рукописное парольное слово. На рис. 1 на одной экранной форме даны два варианта рукописного пароля, используемых при обучении нейросети. Если выполнить полноценное криптографическое хэширование биометрических данных, то из них может быть получен первоначальные заготовки ключей (ключевой материал). Далее необходимо оценить качество ключей, отбросить «плохие» ключи, оставив малую выборку «хороших» ключей. К сожалению, большинство тестов на случайность не могут быть реализованы на мало потребляющих контроллерах доверенной

вычислительной среды, так как имеют экспоненциальную вычислительную сложность.

В частности тест одной «обезьяны», нажимающей клавиши пишущей машинки имеет вычислительную сложность, экспоненциально зависящую от числа букв в эталонном слове. Эта ситуация иллюстрируется данными табл. 1.

Таблица 1

Результаты теста одной «обезьяны» для принятия решения с вероятностью 0,5

Отыскиваемое эталонное слово	«м»	«ма»	«мам»	«мама»	«мамаша»
Вероятность обнаружения в последовател. в 256 бит	0,1233	0,0004	0,000046	10^{-8}	10^{-12}
Длина случ. последоват., где слово обнаруживается с вероятностью 0,5	1024 бит	320 000 бит	512×10^4 бит	…	…

Из табл. 1 видно, что тест одной «обезьяны» для принятия значимого с вероятностью 0.5 решения требует экспоненциального роста длины, проверяемой случайной последовательности. По этой причине тест пригоден для анализа генераторов длинных последовательностей, но не пригоден для анализа ключей длинной в 256 бит.

Упростить тестирование удается, если от анализа обычных кодов перейти к анализу спектров Хэмминга [3, 4], вычисленных по разным модулям 8, 16, 32:

$$"h_3" = \sum_{j=1}^{256-3}\left\{\left[\left("c_j"\right)\oplus\left("x_j"\right)\right]\cdot 1+\left[\left("c_{j+1}"\right)\oplus\left("x_{j+1}"\right)\right]\cdot 2^1+\left[\left("c_{j+2}"\right)\oplus\left("x_{j+2}"\right)\right]\cdot 2^2\right\}, \quad (1)$$

$$"h_4" = \sum_{j=1}^{256-4}\left\{\left[\left("c_j"\right)\oplus\left("x_j"\right)\right]\cdot 2^0+\left[\left("c_{j+1}"\right)\oplus\left("x_{j+1}"\right)\right]\cdot 2^1+\ldots+\left[\left("c_{j+3}"\right)\oplus\left("x_{j+3}"\right)\right]\cdot 2^3\right\}, \quad (2)$$

$$"h_5" = \sum_{j=1}^{256-5}\left\{\left[\left("c_j"\right)\oplus\left("x_j"\right)\right]\cdot 2^0+\left[\left("c_{j+1}"\right)\oplus\left("x_{j+1}"\right)\right]\cdot 2^1+\ldots+\left[\left("c_{j+4}"\right)\oplus\left("x_{j+4}"\right)\right]\cdot 2^4\right\}, \quad (3)$$

::

Описанные выше преобразования, могут быть численно воспроизведены. Результат численного моделирования сверток Хэмминга по модулю 8 (скользящее окно в 3 бита) иллюстрирует рис. 2.

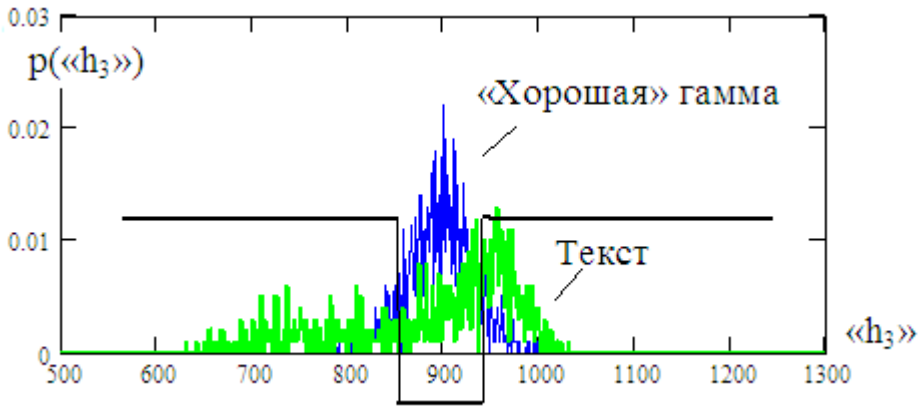


Рис. 2. Искусственный нейрон, анализирующий данные свертки Хэмминга по модулю 8 (скользящее окно в три бита)

Обычный текст на русском языке не является случайным. По этой причине его фрагменты длиной в 256 бит бракуются с вероятностью 0.8. Последовательности, полученные от псевдослучайного программного генератора ближе к «хорошей» гамме, однако мы всегда можем построить искусственный нейрон «бракующий» 50% кодов, попадающих в хвосты нормального распределения, как это показано на рис. 2.

Очевидным является, то что для расстояний Хэмминга по модулю 2, 4, 8, 16, 32. По каждому из модулей Хэмминга может быть построен свой фильтр «плохих» ключей. Все фильтры будут иметь линейную вычислительную сложность. Это позволяет реализовывать сортировку ключей, используя малые ресурсы контроллера доверенной вычислительной среды.

В связи с тем, что проблему тестирования ключей удалось решить, следующей проблемой являются сокращение вычислительных ресурсов, идущих на хэширование случайной компоненты биометрических данных. В этом отношении перспективным является применение рекуррентных процедур вычисления контрольных сумм [5] CRC-4, CRC-5, CRC-6, CRC-7 [6]. Возможно так же использование конгруэнтных генераторов псевдослучайной последовательности, например, генератор Парка-Миллера [7]:

$$X_{k+1} = X_k \cdot 75 \cdot \mathrm{mod}(2^{31} - 1), \qquad (4)$$

где $(2^{31}-1)$ – это длина псевдослучайной последовательности, X_0 – начальное состояние в виде 32 битного случайного числа (ключа для генератора). Возможно и использование других типов конгруэнтных генераторов.

Список литературы

1. URL: //ru.wikipedia.org/wiki/Генератор_псевдослучайных_чисел
2. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: //пниэи.рф/activity/science/noc/bioneuroautograph.zip
3. Юнин А. П., Иванов А. И., Ратников К. А. Оценка качества «белого шума»: реализация теста «стаи обезьян» через множество сверток Хэмминга для разных систем счисления // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза, 2019. С. 10–15.
4. Иванов А. И., Юнин А. П., Бояршинов М. А. Оценка энтропии длинных кодовых слов на выходе нейросетевого преобразователя биометрии в пространствах множества сверток Хэмминга // Интеллектуальные системы в производстве. 2019. Т. 17, № 2. С. 30–36.
5. URL: //ru.wikipedia.org/wiki/Контрольные_суммы
6. URL: //ru.wikipedia.org/wiki/Циклической_избыточный_код
7. Кельтон В., Лоу А. Имитационное моделирование. Классика CS. 3-е изд. СПб. : Питер, 2004. С. 465–487.

Для цитирования: Юнин А. П., Сомкин С. А., Иванов А. П. Синтез ключей из случайной компоненты биометрических данных в условиях применения ограниченных вычислительных ресурсов SIM-карт, микро SD-карт для выполнения операций хэширования и тестирования // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 25–29.

УДК 004.056

ТАБЛИЦА ОЦЕНОК УСКОРЕНИЙ И ЭКОНОМИИ ПАМЯТИ, ДОСТИЖИМЫХ ЗА СЧЕТ ЭФФЕКТА ГИПЕРРАСПАРАЛЛЕЛИВАНИЯ НЕЙРОСЕТЕВЫХ ВЫЧИСЛЕНИЙ, ВОСПРОИЗВОДИМЫХ НА ОДНОЯДЕРНОМ ПРОЦЕССОРЕ

А. И. Иванов[1], И. В. Урнев[2], А. П. Иванов[3], К. А. Ратников[4], С. В. Куликов[5]

[1]Пензенский научно-исследовательский электротехнический институт, г. Пенза

[2,3,4]Пензенский государственный университет, г. Пенза

[5]Лаборатория умных технологий, г. Пенза

Аннотация. Рассматриваются вопросы разработки нейровычислителя для обработки данных в динамическом режиме.

Ключевые слова: эффект гиперраспараллеливания, нейросетевые вычисления**,** одноядерный процессор

TABLE OF ESTIMATES OF SPEEDUPS AND MEMORY SAVINGS ACHIEVED DUE TO THE HYPER-PARALLELIZATION EFFECT OF NEURAL NETWORK CALCULATIONS REPRODUCED ON A SINGLE-CORE PROCESSOR

A. I. Ivanov[1], I. V. Urnev[2], A. P. Ivanov[3], K. A. Ratnikov[4], S. V. Kulikov[5]

[1]Penza Research Electrotechnical Institute, Penza

[2,3,4]Penza State University, Penza

[5]Smart Technologies Laboratory, Penza

Abstract. The article deals with the development of a neurocomputer for data processing in dynamic mode.

Keywords: hyper-parallelization effect, neural network calculations, single-core processor

Нейронные сети и машины Тьюринга начали развиваться примерно в одно и то же время, если считать работу Питтса и Маккалока

[1] как официальный старт в 1943 году развития искусственных нейронных сетей. За прошедшие 77 лет развития произошли серьезные подвижки. Сегодня кажется, что нейросети безнадежно проиграли гонку машинам Тьюрнинга. Нас сегодня окружают машины Тьюринга (часы, сотовые телефоны, ноутбуки, Интернет, …), однако они способны решать только низкоразмерные задачи. При решении двухмерных задач в обычный компьютер приходится ставить специализированный графический ускоритель. При решении трехмерных задач в почти реальном времени приходится использовать станцию из 100 и более графических ускорителей. Такое техническое решение уже нельзя называть компактным, мобильным, низкопотребляющим.

На фоне кубических дециметров, килограммов и киловатов потребления современных графических станций удивительными оказываются способности людей решать в реальном времени (за 0.05 секунды) 10 000 мерные задачи при потреблении нашими естественными нейронами всего 50 ват энергии. Столь высокая входная размерность сетей наших естественных нейронов – это факт подтвержден врачами патологоанатомами. В связи с этим списывать сети искусственных нейронов пока преждевременно. Более того, в 21 веке примерно в одно и то же время в 2006 году появились две практически промышленные технологии применения двух типов искусственных нейронных сетей [2, 3].

Еще одним важным моментом является появление исследований по созданию квантовых компьютеров. Первым идею новых квантовых принципов работы вычислителей высказал в 1980 году М. Ю. Манин [4]. Идея, видимо, витала в воздухе, так как практически то же самое высказали Ричард Фенбаум в 1981 году, Пол Бениофф в 1982 году, Стивен Визнер в 1983 году.

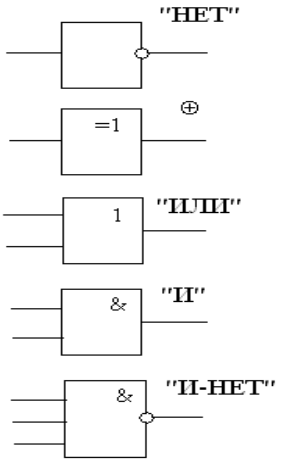
Общая идея квантовых компьютеров в первом приближении может быть сведена к замене обычной логики обычных компьютеров [5, 6] на квантовую логику квантовых компьютеров. Эту ситуацию иллюстрирует табл. 1 обычных и квантовых логических элементов.

Очевидно, что матрицы или их фрагменты (гейты) можно запрограммировать под обычный компьютер, получив тем самым удобные языки для программных симуляторов квантово-матричных вычислений [7].

К сожалению, этот путь является бесперспективным, так как не приводит к ускорению вычислений. Этот путь не более чем экономит время программистов, но этот фактор не является существенным. Промышленного применения таких языков программирования как «Quipper» или «Haskell», скорее всего, не будет.

Таблица 1

Обычные и квантовые логические элементы

Обычная Булева логика или элементы логических цепей	Гейты квантовой логики или элементы квантовых логический цепей
	$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ Вентиль Адамара $\begin{bmatrix} 1 & 0 \\ 0 & e^{j\frac{\pi}{4}} \end{bmatrix}$ Фазовый вентиль $\begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ Вентиль Паули $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ Двухкубитный инвертор

Происходит это по той причине, что квантовые машины, программно- воспроизводящие 10 кубит никому не нужны. В честности для практического применения алгоритма Питера Шора [7] нужно сегодня создавать аппаратно квантовый Фурье процессор на 2048 КуБит. Никакая из современных вычислительных машин Тьюринга программного эмулятора квантового Фурье процессора такой размерности не потянет. Специалистам по применению гейтов и тензоров придется ждать неопределенное время, пока Силиконовая долина, Китай или Сколково не обеспечат их серийно производимыми микросхемами аппаратно-полноценных гейтов квантовой логики или тензоров. Только в этом случае мы все получим предсказанные в теории гиперускорения вычислений.

Нейросетевой преобразователь биометрии в код криптографического ключа (задача извлечения из него знаний)

Одной из проблем информационной безопасности является то, что люди не могут запоминать длинные пароли доступа. Эту проблему США, Китай, страны Евросоюза, Россия пытаются решить применением биометрии. Так как рынок средств информационной безопасности специфичен, международное сообщество с 2002 года по настоящее время в рамках работы технического комитета ISO/IECJTC1 sc37 (Биометрия) разработало примерно 153 стандартов. К сожалению, международные стандарты ориентированы на

применении программной спецификации BioAPI [8, 9], криптографическая защита которой имеет ряд уязвимостей.

В связи с этим обстоятельством Россия вынуждена создавать собственные национальные стандарты, регламентирующие требования к нейросетевой защите персональных данных биометрических приложений искусственного интеллекта. Блок схема реализации нейросетевой защиты персональных биометрических данных приведена на рис. 1.

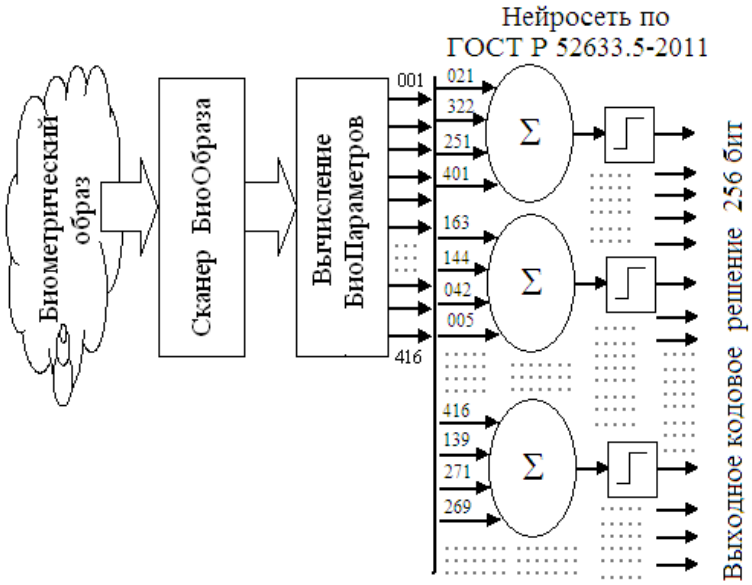


Рис. 1. Нейросетевое преобразование «сырых» биометрических параметров в код длинного криптографического ключа

Из рис. 1 видно, что биометрический образ «Свой» должен быть отсканирован, несколько раз (например, следует получить обучающую выборку, состоящую примерно из 20 примеров образа «Свой»). Далее необходимо запустить автомат обучения, реализованный по ГОСТ Р 52633.5 [10] и дать обучающему автомату криптографический ключ пользователя длинной 256 бит.

Исследования показали, что для сети, состоящей из 256 искусственных нейронов, направленным перебором возможных ее состояний могут быть извлечены знания о криптографическом ключе пользователя.

Отсутствие технической возможности сформировать и хранить полную тестовую базу образов «Чужой» из-за ограниченной памяти современных вычислителей

Для того, что бы организовать атаку силового перебора образов «Чужой» следует первоначально сформировать базу тестовых

образов в соответствии с ГОСТ Р 52633.1 [11], например из 10 000 образов, каждый из которых представлен 20 примерами. Если данные собирать средствами среды моделирования «БиоНейроАвтограф» [12, 13], то один рукописный образ, представленный 20-ю примерами будет иметь объем 100.0 Кбайт. То есть 10 000 подобных образов потребуют памяти 1 Гбайт, что вполне приемлемо.

Если отказаться от хранения полных данных о динамике изменения координат X(t) и Y(t) и перейти к хранению только 416 коэффициентов двухмерного Фурье, то объем памяти на один пример падает до 3.0 Кбайт, соответственно 20 примеров будут занимать 60.0 Кбайт, что обеспечивает сжатие данных примерно на 40%. То есть на хранение базы из 10 000 образов «Чужой» потребуется память объемом в 0.6 Гбайт.

Национальный стандарт ГОСТ Р 52633.2 [14] позволяет размножать образы «Чужой» путем скрещивания морфингом двух образов-родителей и получения от них 1, 2, 3,…, N образов потомков. При этом даже при получении от двух образов-родителей одного образа-потомка полная матрица скрещивания даст очень большое число потомков:

$$\sum_{i=1}^{9999}(10000-i)\approx 50000000 \text{ штук.}$$

Столь значительный объем данных уже невозможно записать на существующих сегодня средствах хранения информации. Таким образом, идеология силового перебора предварительно синтезированных биометрических образов «Чужой» на текущий момент технически не реализуема.

Схема направленного перебора, построенная на экономии памяти с хранением и размножением данных только одного поколения образов «Чужой»

Решить проблему ограниченного объема памяти современных компьютеров удается, сохраняя только одно поколение в 10 000 образов «Чужой». Блок-схема организации направленного подбора приведена на рис. 2.

Ускорение перебора и одновременное сокращение памяти достигаются одновременно за счет перехода от анализа обычных кодов с полем возможных состояний 2^{256} к анализу малого числа в 257 состояний расстояний Хэмминга. Этот технологический прием снижения вычислительной сложности описан в ГОСТ Р 52633.3 [15]. Стандарт

рекомендует при тестировании нейросети переходить в пространство расстояний между анализируемыми кодами и кодом образа «Свой».

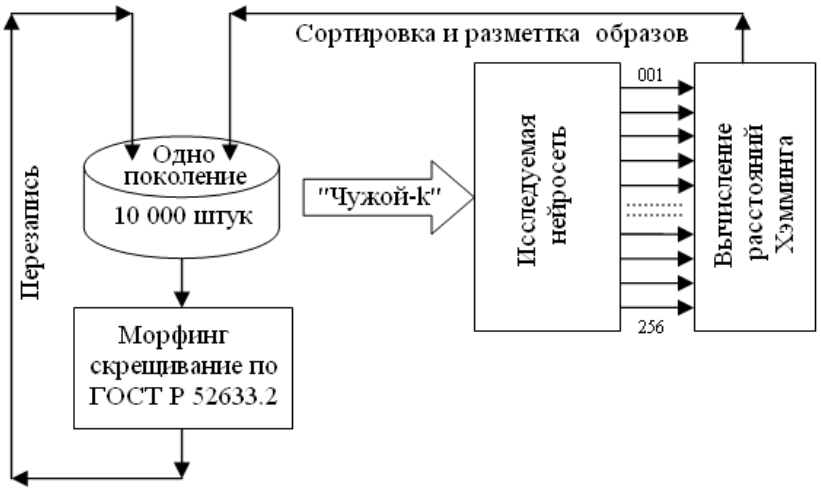


Рис. 2 Снижение требований к памяти компьютера при хранении и использовании одного поколения 10 000 образов «Чужой» при направленном их переборе с наблюдением данных в пространстве расстояний Хэмминга

В случае извлечения знаний из нейросети код образа «Свой» неизвестен, в связи с этим необходимо либо вычислить кодовый центр образа «Чужой-k», либо вычислять автосвертки Хэмминга между кодами-откликами 20 примеров образа «Чужой-k» [16]. Рисунок 3 иллюстрирует наиболее очевидную операцию, вычисления кодового центра кодов-откликов на примеры образа «Чужой-k». При «проявке» кодового центра в каждом разряде кода подсчитывают число состояний «0» и число состояний «1». Решение принимают «голосованием» по большинству обнаруженных состояний.

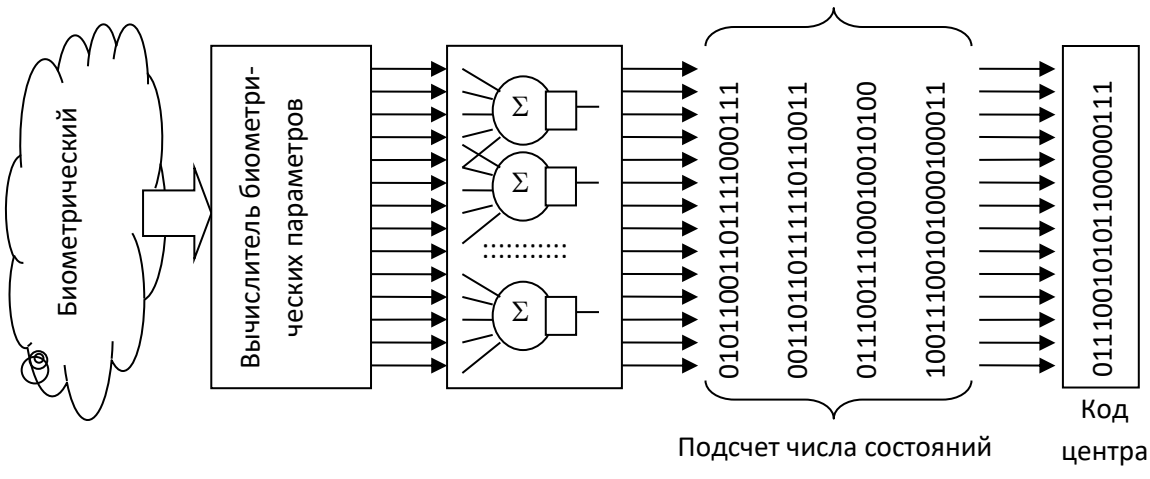


Рис. 3. Поразрядное накапливание состояний кода примеров образа «Чужой-k» при выявлении центра этого множества

После проявки кодового центра можно вычислять относительно него расстояния Хэмминга и анализировать спектр линий Хэмминга, оценивая энтропию кодов исследуемого образа «Чужой-k». На рис. 4 представлены два примера спектров расстояний Хэмминга, полученных для двух разных биометрических образов «Чужой». Спектры Хэмминга расположенные с левой стороны всегда будут иметь более низкую энтропию. Это связано с тем, что примеры образа «Свой» по определению должны давать практически нулевую энтропию (все коды-отклики на примеры образа «Свой» должны быть одинаковы). То есть коды-отклики образа «Свой» любой нейросети должны иметь спектр Хэмминга в виде дельта функции в точке «h»≡0.

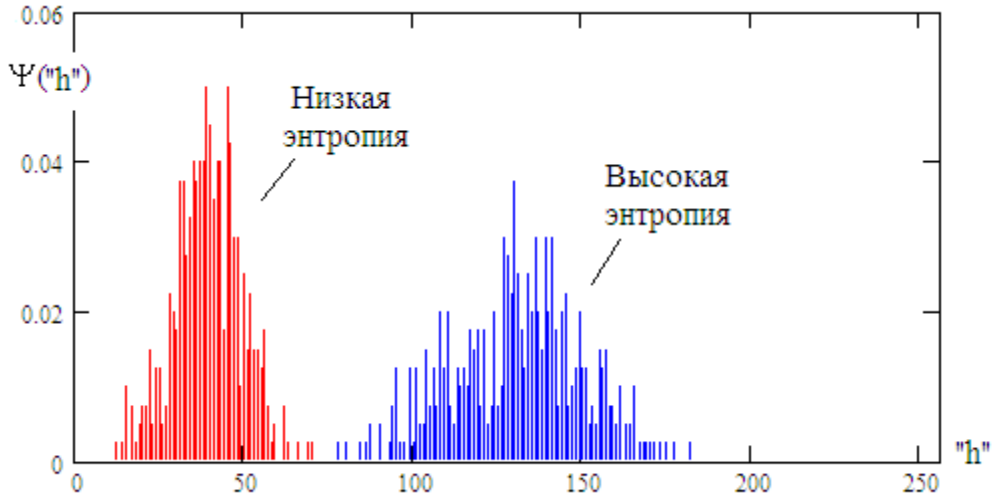


Рис. 4. Примеры образов «Чужой» с разным уровнем энтропии

Одной из особенностей сетей искусственных нейронов с линейным накоплением данных, обученных по ГОСТ Р 52633.5 [10] является то, что они обладают симметрией. Примеры образа «Свой» дают код «Свой», а примеры инверсного образа «Свой» дают инверсный код «Свой». В связи с этим сортировка образов «Чужой» по их энтропии дает распределение в виде «палатки», представленной на рис. 5.

Из рис. 5 видно, что мы имеем в правом и левом «хвостах палатки» образы «Чужой» с минимальной энтропией. При этом одни образы будут близки к образу «Свой», а другие образы будут близки инверсному образу «Свой». Пользуясь этим, мы можем выделить 2 % образов «Чужой», обладающих минимальной энтропией. Все остальные 9 800 образов «Чужой» первого поколения могут быть уничтожены для экономии памяти компьютера (рис. 2).

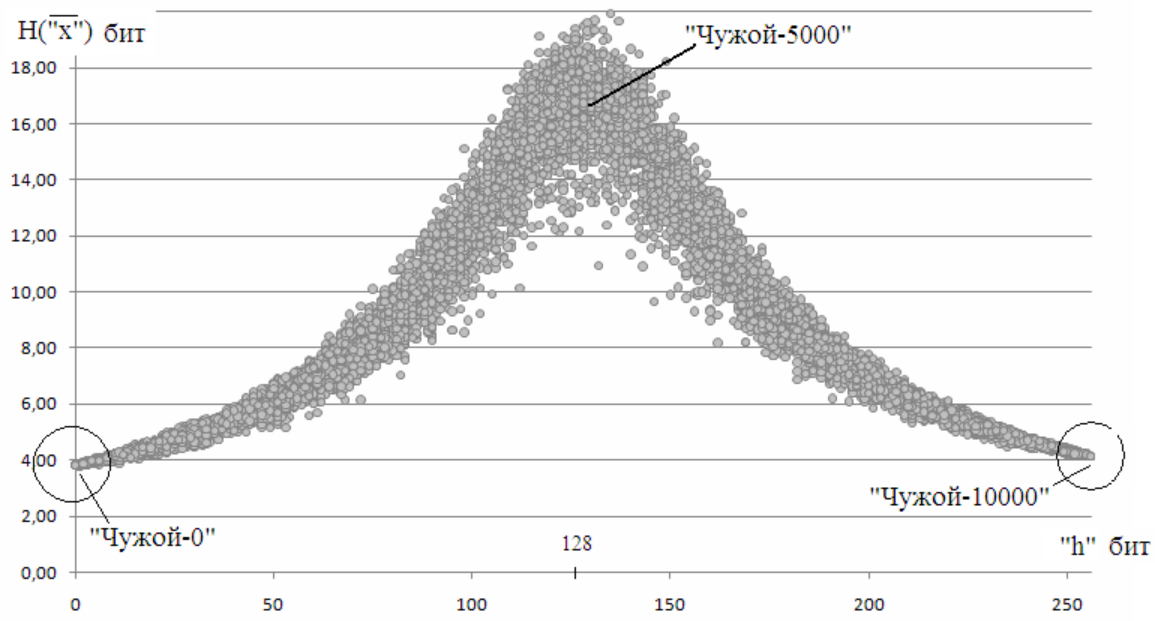


Рис. 5. Пример распределения энтропии упорядоченных образов «Чужой» в первом поколении

Располагая 100 низко энтропийных образов «Чужой» в правой и левой группах, мы можем выполнить их морфинг-скрещивание алгоритмом ГОСТ Р 52633.2 [14] и восстановить численность во втором поколении образов «Чужой» до 10 000 штук. Очевидно так же, что мы можем повторить, описанные выше процедуры многократно. Практика показала, что примерно через 50 поколений удается восстановить параметры биометрического образа «Свой» с доверительной вероятностью 0.97. На обычном компьютере с обычной памятью удается решить обратную задачу нейросетевой биометрии за время от 11 минут до 24 минут. Это стало возможным только из-за экономии памяти и применения 256-ти мерных наблюдателей энтропии спектров Хэмминга.

Оценка ускорений, достижимых при извлечении знаний из таблиц обученной сети искусственных нейронов

Очевидными являются способы линейного распараллеливания нейросетевых вычислений. Если процессор имеет 32 ядра, то всегда мы можем ускорить в 32 раза вычисления, параллельно вычисляя в каждом из ядер отклик одного искусственного нейрона. Сегодня существуют процессоры с 4096 ядрами [15], что позволяет примерно в четыре тысячи раз линейно увеличить скорость вычислений.

Те процедуры, которые рассмотрены выше, позволяют выполнять гиперраспараллеливание нейросетевых вычислений даже на одном ядре в пространстве расстояний Хэмминга. Мы фактически на одном ядре имеем в каждом поколении 50-ти кратное ускорение (отбрасывается 98 % образов, сохраняется только 2 % образов с минимальной энтропией). Так как эта процедура повторяется в каждом из 50 поколений параллельно с экономией памяти, возникает ускорение вычислений в 50^{50} раз. Столь значительные ускорения трудно воспринимать и сопоставлять. Одним из способов, облегчающих восприятие, является перевод показателей ускорения в «гугл» систему счисления. Один «гугл» составляет 10^{100}, соответственно величина 10^{85} должна составить 0.85-ю часть «гугл», величина 10^{200} должна интерпретироваться как величина соответствующая 2.0-м «гугл» единицам. Исходя из этих представлений, построена таблица оценки достижимых на обычной вычислительной машине ускорений за счет неявного гиперраспараллеливания вычислений на одном ядре процессора.

Таблица 2

Результаты оценки ускорений за счет неявного гиперраспараллеливания вычислений на одном ядре процессора

Число поколений	40	42	44	46	48	50	52	54	56	58	60
Гугл показатель	0,680	0,714	0,748	0,782	0,812	0,85	0,884	0,918	0,951	0,985	1,02

Из данных табл. 2 следует, что уже при 60 поколениях, рассмотренные процедуры гиперраспараллеливания вычислений позволяют получить ускорение в один гугл на обычном компьютере. Именно из-за столь значительного ускорения и удается решать обратные задачи нейросетевой биометрии.

Заключение

В первом разделе данной работы отражены перспективы создания в отдаленном будущем полноценных квантовых вычислителей. По предсказаниям физико-математической общественности полноценные квантовые процессоры смогут достигать в будущем укоренений вычислений, приведенных в таблице 2. При этом сегодняшние «квантовые» схемы вычислений не дают, каких либо ускорений вычислений. Они громоздки, не практичны (требуют заправ-

ки жидким гелием) и создаются ведущими фирмами (IBM, Intel, Googl) только в рекламных целях, якобы подтверждающих высокий уровень этих фирм и их специалистов.

Вместе с тем, каждый из нас думает исключительно в нейродинамике (наши естественные нейроны не могут находиться в статике). При этом мы, распараллеливаем наши нейросетевые вычисления, добиваемся их огромных ускорений и, если это необходимо, мы получаем нейровычисления с огромным уровнем доверия к их решениям. Все это становится возможным только по результатам обучения наших с Вами естественных нейронов на протяжении всей нашей жизни.

Предположительно под каждую из актуальных задач современности можно построить свой нейровычислитель, на описанных в данной статье принципах. При этом обязательным элементом такого нейровычислителя должен быть некоторый модулятор данных, обрабатываемых нейросетью и заставляющий перейти нейросеть из статики в динамику. В нашем случае роль такого модулятора играет база из 10 000 образов «Чужой», постоянно обновляемая и постоянно модифицируемая. Наличие некоторого модулятора данных обязательно для всех нейровычислителей, программно поддерживающих режим нейродинамики [16–18].

Список литературы

1. McCalloc W. C., Pitts W. A logical calculus of ideas immanent in nervous activity // Bull. Mathematical Biophysics. 1943. № 5. P. 115–133.
2. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.
3. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб. : Питер, 2018. 480 с.
4. Манин Ю. И. Вычислимое и невычислимое. М. : Сов. радио, 1980. 51 с.
5. Гуц А. К. Основы квантовой кибернетики. М. : ЛЕНАНД, 2017. 216 с.
6. Перри Р. Элементарное введение в квантовые вычисления : пер. с англ. : учеб. пособие. Долгопрудный : Интеллект, 2015. 208 с.
7. Душкин Р. В. Квантовые вычисления и функциональное программирование. М. : ДМК Пресс, 2015. 232 с.
8. ГОСТ Р ИСО/МЭК 19784-1–2007. Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Ч. 1. Спецификация биометрического программного интерфейса.

9. Руд Б., Коннел Дж. Х., Панканти Ш. [и др.]. Руководство по биометрии : пер. с англ. М. : Техносфера, 2007. 368 с.

10. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

11. ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

12. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: //пниэи.рф/activity/science/noc/bioneuroautograph.zip

13. Иванов А. И. Исследование свойств нейросетевого преобразователя биометрия-код с использованием среды моделирования «БиоНейроАвтограф» : учеб.-метод. пособие. Пенза : Изд-во ПГУ, 2020. 40 с. URL: //tsib.pnzgu.ru/page/39329

14. ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

15. URL: ru.wikipedia.org/wiki/Многоядерный_процессор

16. ГОСТ Р 52633.3-2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

17. Иванов А. И., Иванов А. П., Ратников К. А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга. Пенза : Изд-во ПГУ, 2021. 56 с.

18. Иванов А. И., Малыгина Е. А., Лукин В. С. Компактная графическо-иероглифная система отображения схем многообразных нейросетевых вычислений // Известия высших учебных заведений. Поволжский регион. Технические науки. 2020. № 4. С. 4–8.

Для цитирования: Иванов А. И., Урнев И. В., Иванов А. П., Ратников К. А., Куликов С. В. Таблица оценок ускорений и экономии памяти, достижимых за счет эффекта гиперраспараллеливания нейросетевых вычислений, воспроизводимых на одноядерном процессоре // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 30–40.

УДК 004.056

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ РАЗРАБОТКИ И ВВЕДЕНИЯ В ДЕЙСТВИЕ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ВТОРОГО НАЦИОНАЛЬНОГО СТАНДАРТА ПО БЫСТРОМУ, УСТОЙЧИВОМУ, АВТОМАТИЧЕСКОМУ ОБУЧЕНИЮ СЕТЕЙ КВАДРАТИЧНЫХ НЕЙРОНОВ

Е. А. Малыгина[1], А. И. Иванов[2], И. В. Урнев[3]

[1,3]Пензенский государственный университет, г. Пенза

[2]Пензенский научно-исследовательский электротехнический институт, г. Пенза

Аннотация. Рассматриваются преимущества нейронов, осуществляющих обогащение входных биометрических данных в квадратичном пространстве по сравнению с нейронами, осуществляющих обогащение биометрических данных в линейном пространстве по требованиям ГОСТ Р 52633.5–2011.

Ключевые слова: второй национальный стандарт, квадратичные нейроны, биометрические данные

JUSTIFICATION OF THE NEED TO DEVELOP AND IMPLEMENT THE SECOND NATIONAL STANDARD FOR FAST, STABLE, AUTOMATIC TRAINING OF QUADRATIC NEURON NETWORKS ON THE TERRITORY OF THE RUSSIAN FEDERATION

E. A. Malygina[1], A. I. Ivanov[2], I. V. Urnev[3]

[1,3]Penza State University, Penza

[2]Penza Research Electrotechnical Institute, Penza

Abstract. The advantages of neurons that enrich input biometric data in a quadratic space compared to neurons that enrich biometric data in a linear space according to the requirements of GOST R 52633.5–2011 are considered.

Keywords: second national standard, quadratic neuron networks, biometric data

Следует отметить, что введение в действие на территории РФ первого в мировой практике стандарта по быстрому, устойчивому, автоматическому обучению сетей искусственных нейронов ГОСТ Р 52633.5–2011 [1], является принципиально важным. Этот стандарт касается только сетей искусственных нейронов с накоплением относительно бедных биометрических данных в линейном пространстве (персептронов).

По мере исследований, проводимых в России, были выяснены положительные и отрицательные стороны применения сетей искусственных нейронов с накоплением данных в линейном пространстве. Положительным является то, что сети нейронов с линейным накоплением хорошо зарекомендовали себя в условиях, когда они размещаются в доверенной вычислительной среде (ДВС), к содержанию которой злоумышленник не имеет доступа. В этом случае злоумышленник при организации может наблюдать только входные биометрические параметры и выходные отклики ДВС. То есть в этом случае проблема защиты информации о персональных данных должна сводиться к исключению перехвата данных злоумышленниками на входах и выходах ДВС.

К сожалению, физическое попадание ДВС в руки злоумышленников позволяет им организовать атаку извлечения знаний, описанную в предыдущем докладе на этой конференции [2]. Защититься от этой атаки можно, если ввести внутрь ДВС механизм размножения ошибок [3, 4]. В этом случае внешняя атака извлечения знаний из нейросети линейных нейронов (персептронов) [2] становится невозможной.

Еще одним негативным моментом применения линейных нейронов является их слабость по отношению к атаке Г. Б. Маршалко [5]. В связи с высокой эффективностью атаки извлечения знаний [2] и атаки Г. Б. Маршалко [5] в России ведутся работы по созданию алгоритмов быстрого, устойчивого, автоматического обучению сетей искусственных нейронов с накоплением данных в квадратичных пространствах [6].

Следует отметить, что ранее подобные работы в России не велись. Это было обусловлено неприятным свойством легкого извлечения ключей из ДВС с сетью квадратичных нейронов, имеющих выходные бинарные квантователи. Эта ситуация иллюстрируется рис. 1, где отображены отклики квадратичных нейронов на входные воздействия примерами образов «Чужой».

Если поступать, как это было принято ранее, пользуясь при вычислениях математическими ожиданиями биометрических параметров, то отклики образов «Свой» должны оказаться вблизи вертикальной оси. Для того, что бы отклики образов «Чужой» могли создавать коды с равной вероятностью появления в их разрядами состояний «0» и «1» квантователи нейронов должны иметь порог срабатывания равным значению 9.3, как это показано на рис. 1. Для того, чтобы коды ключа «Свой» имели разные состояния своих разрядов, по классике требуется изменить выходные состояния, находящиеся справа и слева от порога сравнения.

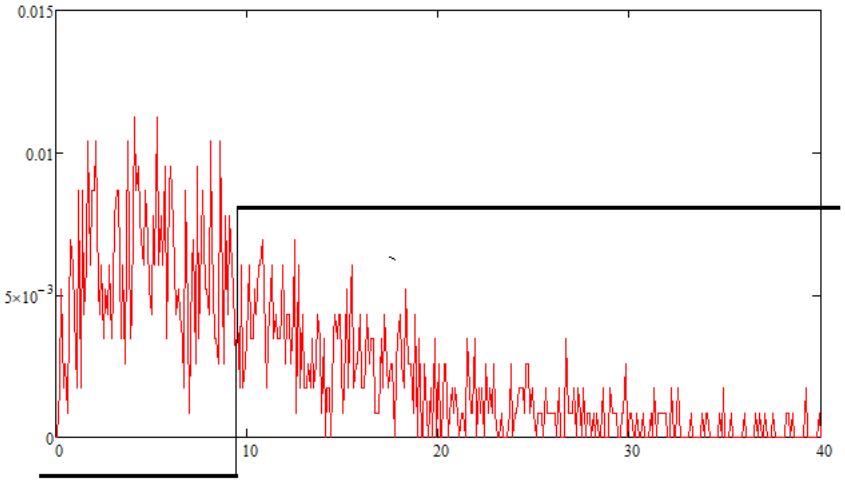


Рис. 1. Пример выходных состояний квадратичных нейронов при воздействии на них примерами образов «Чужой»

При такой, достаточно простой нейросетевой конструкции, код ключа «Свой» оказывается легко извлекаемым из ДВС. Для этого достаточно подавать на входы ДВС редко встречающиеся образы «Чужой», находящиеся на периферии многомерного распределения образов «Чужой». В этом случае редко встречающиеся периферийные образы «Чужой» дают инверсный код ключа «Свой».

Для всех квадратичных нейронов с бинарными квантователями возникают проблемы низкого уровня хэширования данных образов «Чужой», которых нет у нейронов с линейным накоплением. Только в случае использования квантователей с большим, чем два выходных состояний [6, 7] появляется возможность получить эффективное перемешивание (хэширование) разрядов кодовых откликов образов «Чужой». При этом механизм хэширования является табличным (низкоуровневым) и, соответственно, его невозможно отключить. Пример организации таких ссылочных компактных таблиц хэширования приведен ниже. На все нейроны достаточно одной такой ссылочной таблицы.

Таблицы хэш-перестановок выходных состояний квантователей двух рядом стоящих нейронов

Состояния предудущего нейрона

«00»	«01»	«10»	«11»

0	«00»
1	«11»
2	«01»
3	«10»

Хэш - таблица 0

0	«10»
1	«01»
2	«00»
3	«11»

Хэш - таблица 1

0	«01»
1	«10»
2	«11»
4	«00»

Хэш - таблица 2

0	«11»
1	«00»
2	«01»
3	«10»

Хэш - таблица 3

В верхней части таблицы даны выходные состояния квантователя предшествующего нейрона. Ниже приведены варианты хэш-таблицы перестановок выходных состояний квантователя следующего нейрона. Неверное выходное состояние одного нейрона приводит к появлению неверных цепочек кодовых состояний всех последующих нейронов.

Еще одним важнейшим свойством квадратичных нейронов является их высокая выделительная способность данных образа «Свой». Как показано на рис. 2 для надежного выделения типичного двухмерного распределения данных «Свой» требуется как минимум три линейных нейрона, разделяющая линия которых является касательной к эллипсу нормального распределения данных «Свой». В этом отношении квадратичный нейрон с эллиптическим квантователем работает гораздо эффективнее. Как результат появляется теоретическая возможность при переходе от линейных нейронов к квадратичным снизить число входов у нейронов. Формально это позволяет увеличить длину выходного кода «Свой».

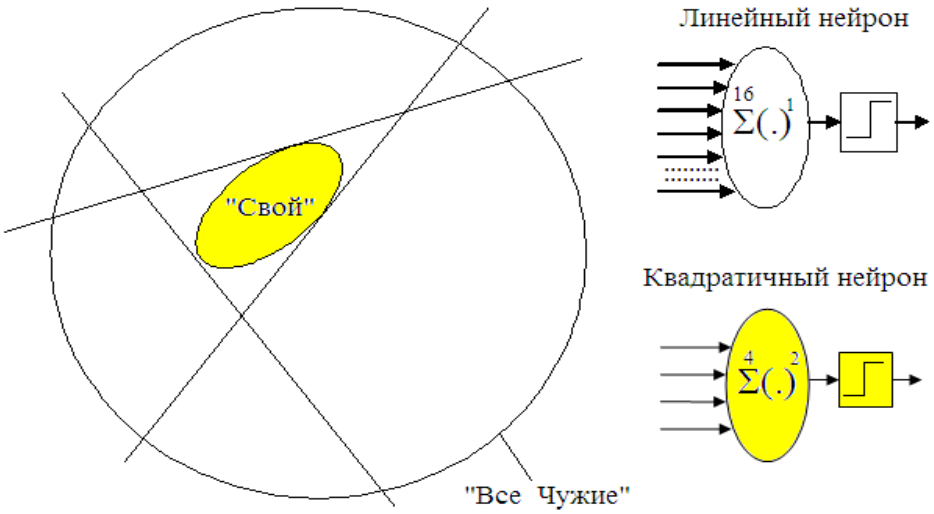


Рис. 2. Высокий уровень эффективности выделения образа «Свой» эллиптическим квантователем единственного квадратичного нейрона по сравнению с тремя линейными нейронами

Следующим (возможно временным) преимуществом перехода к квадратичным нейронам является то, что для сетей квадратичных нейронов с многоуровневыми квантователями пока не создана эффективная машина по извлечению из их кодов знаний. Вполне возможно, что такой машины создать будет технически невозможно. Это обстоятельство на текущий момент является крайне важным.

В случае если подобная машина извлечения знаний будет создана это временное преимущество исчезнет, однако это обстоятельство не должно стать большой проблемой для аппаратно-программных ДВС.

Существующая машина извлечения знаний из нейронов с линейной симметрией построена на существующей у сетей линейных нейронов симметрии [2]. Если удастся построить аналогичную машину извлечения знаний для сетей квадратичных нейронов, то и она будет использовать некоторую радиальную симметрию квадратичных нейронов. Очевидным является то, что симметрии линейных нейронов и квадратичных нейронов различны. То есть машина, извлекающая знания из нейронных сетей, размещенных в ДВС должна опираться на знания о том, какой выходной бит кода принадлежит линейной сети, а какой квадратичной. Это невозможно, так как к содержимому ДВС атакующий не имеет доступа.

Список литературы

1. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

2. Иванов А. И., Урнев И. В., Иванов А. П., Ратников К. А., Куликов С. В. Таблица оценок ускорений и экономии памяти, достижимых за счет эффекта гиперраспараллеливания нейросетевых вычислений, воспроизводимых на одноядерном процессоре // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. Пенза : Изд-во ПГУ, 2021. С. 66–74.

3. Язов Ю. К., Волчихин В. И., Иванов А. И. [и др.]. Нейросетевая защита персональных биометрических данных. М. : Радиотехника, 2012. 157 с.

4. Техническая спецификация «Системы обработки информации. Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов» [принята 19.11.2020 на XXV заседании технического комитета № 26].

5. Marshalko G. B. On the security of a neural network-based biometric authentication scheme // Математические вопросы криптографии. 2014. Т. 5, № 2. С. 87–98.

6. Иванов А. И., Безяев А. В., Малыгина Е. А., Серикова Ю. И. Второй национальный стандарт России по быстрому автоматическому обучению больших искусственных нейронных сетей на малых выборках биометрических данных // Безопасность информационных технологий :

сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза : Изд-во ПГУ, 2019. С. 174–177.

7. Малыгина Е. А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с многоуровневым квантованием биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 114 с.

Для цитирования: Малыгина Е. А., Иванов А. И., Урнев И. В. Обоснование необходимости разработки и введения в действие на территории Российской Федерации второго национального стандарта по быстрому, устойчивому, автоматическому обучению сетей квадратичных нейронов // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 41–46.

УДК 004.056

ОЦЕНКА ИНФОРМАТИВНОСТИ БИОМЕТРИЧЕСКИХ ДАННЫХ ДИНАМИКИ РУКОПИСНОГО ПОЧЕРКА ПРИ ОБОГАЩЕНИИ ИСКУССТВЕННЫМИ НЕЙРОНАМИ В ЛИНЕЙНОМ ПРОСТРАНСТВЕ И КОРРЕЛЯЦИОННЫМИ НЕЙРОНАМИ В КВАДРАТИЧНОМ ПРОСТРАНСТВЕ

А. Е. Сулавко[1], П. С. Ложников[2], А. И. Иванов[3], Т. А. Золотарева[4]

[1]Сибирский государственный автомобильно-дорожный университет, г. Омск

[2]Омский государственный технический университет, г. Омск

[3]Пензенский научно-исследовательский электротехнический институт, г. Пенза

[4]Липецкий государственный педагогический университет имени П. П. Семенова-Тян-Шанского, г. Липецк

Аннотация. Приведена сравнительная оценка информативности рукописных образов при их обогащении нейронами в линейном пространстве и корреляционными нейронами в квадратичном пространстве. Новый класс корреляционных нейронов в квадратичном пространстве ориентирован на работу с уникальностью корреляционных матриц каждого конкретного биометрического образа. В связи с тем, что биометрическими параметрами становятся корреляционные связи, то число анализируемых биометрических параметров многократно увеличивается.

Ключевые слова: биометрические данные, искусственные нейроны, корреляционные нейроны

EVALUATION OF THE INFORMATIVENESS OF BIOMETRIC DATA ON THE DYNAMICS OF HANDWRITING, WHEN ENRICHED WITH ARTIFICIAL NEURONS IN LINEAR SPACE AND CORRELATION NEURONS IN QUADRATIC SPACE

A. E. Sulavko[1], P. S. Lozhnikov[2], A. I. Ivanov[3], T. A. Zolotareva[4]

[1]The Siberian State Automobile and Highway University, Omsk

[2]Omsk State Technical University, Omsk

[3]Penza Research Electrotechnical Institute, Penza

[4]Lipetsk State Pedagogical University named after P. P. Semenov-Tyan-Shansky, Lipetsk

Abstract. A comparative assessment of the information content of handwritten images when they are enriched with neurons in linear space and correlation neurons in quadratic space is given. A new class of correlation neurons in the quadratic space is focused on working with the uniqueness of the correlation matrices of each specific biometric image. Due to the fact that correlations become biometric parameters, the number of analyzed biometric parameters increases many times.
Keywords: biometric data, artificial neurons, correlation neurons

В прошлом веке было принято при решении той или иной технической задачи вручную отыскивать наиболее информативные параметры для того, чтобы использовать далее только их. Такой подход можно сравнить с ручным поиском золотых самородков на дне ручья. Обычно золотой самородок блестит на дне ручья, его легко заметить и взять рукой, однако их очень мало.

Если взять лоток и начать промывать золотоносный песок, то удастся намыть золотого песка в десять раз больше, чем содержится в золотоносной породе достаточно крупных самородков. После каждой удачной промывки на дне промывочного лотка старатель видит крохотные золотые песчинки. Они настолько малы, что их нельзя взять рукой, но по весу их больше чем самородков.

В начале этого 21 века произошла вычислительная революция. Если в прошлом веке приходилось работать вручную, отыскивая достаточно крупные информационные самородки, то в этом веке появились промышленные технологии нейросетевого обогащения относительно бедных данных большого объема. В частности получили широкое применение глубокие нейронные [1, 2] медленного предварительного обучения на больших выборках. Так же появились быстро обучаемые сети искусственных нейронов на малых выборках [3,]. На рис. 1 приведена экранная форма среды моделирования «БиоНейроАвтограф» [4, 5] в режиме обучения динамике рукописного почерка рукописного слова-пароля.

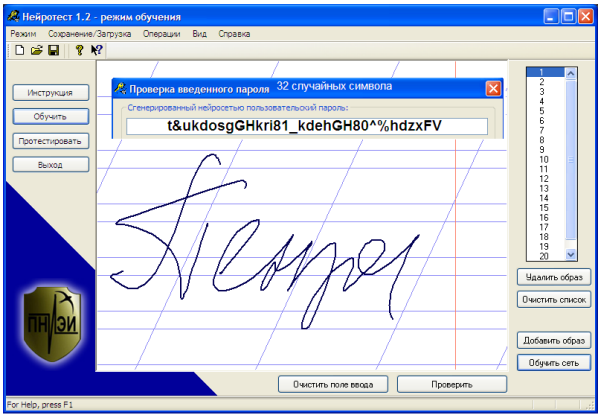


Рис. 1. Экранная форма режима обучения, свободно распространяемой среды моделирования «БиоНейроАвтограф»

На данный момент среда моделирования «БиоНейроАвтограф» является единственным программным продуктом свободного доступа, позволяющим получать достоверные биометрические данные в любых объемах и, пользуясь ими, выполнять лабораторные работы, не нарушая норм законодательства. В России и с других странах сбор, хранение, использование персональных биометрических данных находиться под особым контролем.

Среда моделирования «БиоНейроАвтограф» позволяет преобразовывать динамику рукописного почерка в 416, контролируемых биометрических параметра. Каждый из этих биометрических параметров является двухмерным коэффициентом Фурье, полученным при преобразовании колебаний пера по двум координатам X(t), Y(t) при написании парольного слова.

Следует подчеркнуть, что классическая графологическая экспертиза криминалистики анализирует всего 16 биометрических параметров. По сути дела, ее основы были созданы в начале прошлого века и как раз создавались в парадигме поиска наиболее информативных параметров.

Каждый из 416 биометрических параметров обладает своим математическим ожиданием, которое вычисляется по малой выборке в 20 примеров образа «Свой». Распределение значений математических ожиданий для конкретного биометрического образа приведено на рис. 2.

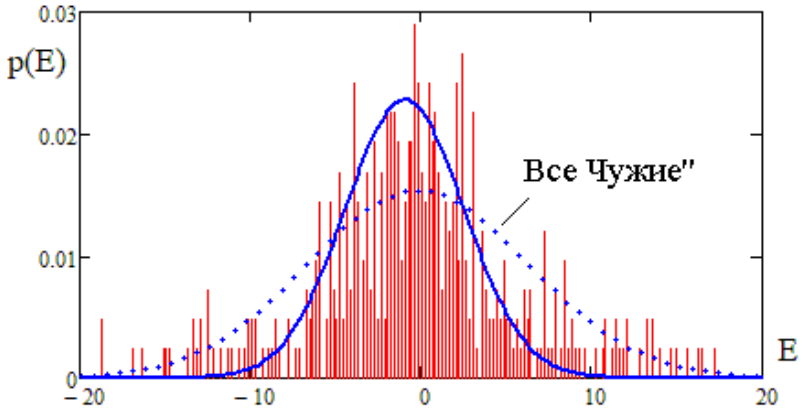


Рис. 2. Реальное распределение математических ожиданий биометрических параметров рукописного образа «*Пенза*»

Каждый конкретный биометрический образ имеет распределение математических ожиданий, существенно отличающееся от нормального (наблюдаются тяжелые «хвосты» «хороших» биометрических параметров). Если же рассматривать не один биометрический

образ, а множество случайно выбранных образов, то закон распределения можно считать нормальным. В соответствии с основной теоремой статистики, сложение (накапливание) данных приводит к их нормализации.

Стандартное отклонение биометрических параметров каждого конкретного образа имеет распределение близкое к смещенному хи-квадрат распределению, как это показано на рис. 3.

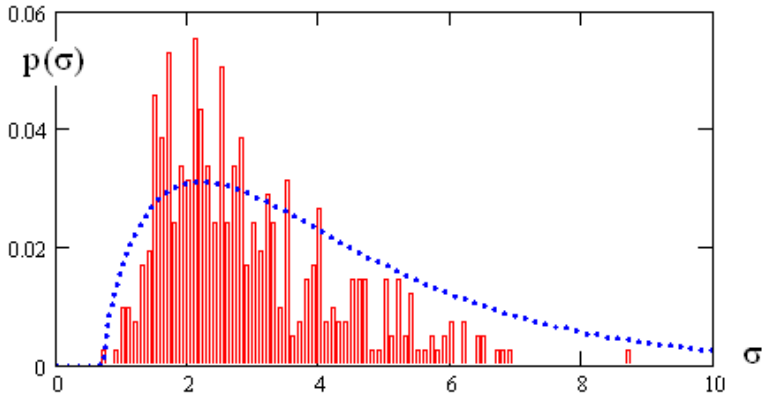


Рис. 3 Реальное распределение значений стандартных отклонений рукописного образа «*Пенза*» хорошо аналитически описывается смещенных хи-квадрат распределением

Очевидно, что информативность каждого биометрического параметра тем выше, чем сильнее его математическое ожидание отклоняется от центра и чем меньше его стандартное отклонение. На рис. 4 приведено распределение биометрических параметров по их информативности.

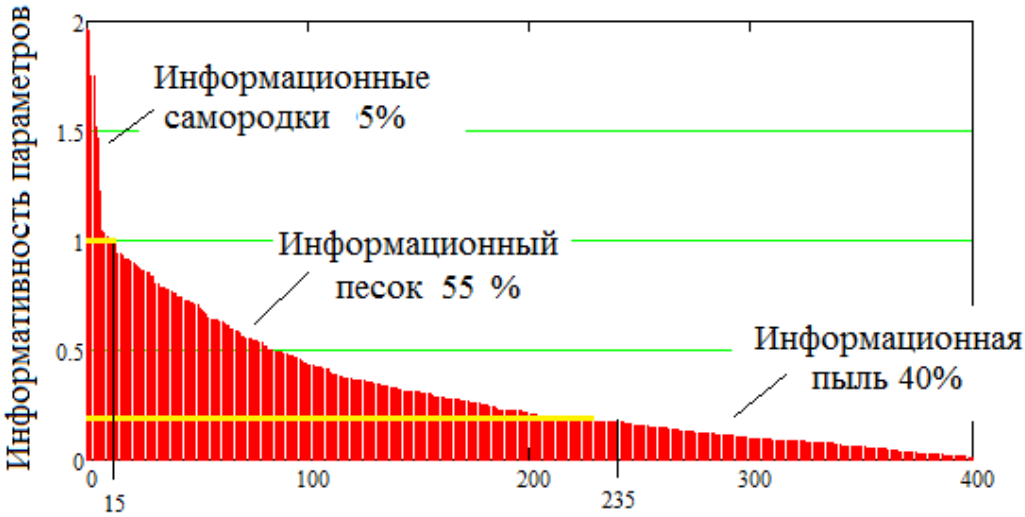


Рис. 4. Деление биометрических параметров по их информативности

Из рис. 4 видно, что примерно 15 биометрических параметров имеют очень высокую информативность, они являются аналогами информационных самородков. Каждый из этих высокоинформативных параметров можно использовать самостоятельно и получать стабильно работающих 15 бит ключа. В интервал от 15 до 235 попадают условно информативные биометрические параметры или информационный песок. Именно учет этих условно информативных биометрических параметров, обученной сетью искусственных нейронов и позволяет получать программе «БиоНейроАвтограф» 256 бит ключа (кода аутентификации).

Далее идут низко информативные параметры, которые нейросеть, обученная по ГОСТ Р 52633.5 [3] не учитывает, так как их весовые коэффициенты оказываются малы. Можно рассматривать эти низко информативные параметры как некоторую информационную пыль, учесть которую современные сети искусственных нейронов не могут.

Следует отметить, что похожая ситуация сложилась и в современной золотодобыче. Кроме самородков и золотого песка в золотоносной породе содержится и золотая пыль. В 21 веке ее научились извлекать. Для этой цели отработанную золотоносную пароду выкладывают на пластик и смачивают цианидами, этот процесс хорошо описан на Wikipedia.org/Золото. Далее растворенное золото улавливают угольными фильтрами. После сжигания угля, золу нагревают в печи, расплавленное золото стекает на дно тигля.

Если считать стандартизованную в России технологию использования сетей искусственных нейронов с линейным обогащением данных аналогом промывки в лотке золотого песка, то в ближайшее время должны появиться нейросетевые технологии, способные работать с информационной пылью биометрических данных.

Скорее всего, в этой роли будут выступать большие сети корреляционных нейронов Байеса [7, 8]. Этот новый класс нейросетевых преобразователей ориентирован на работу с уникальностью корреляционных матриц каждого конкретного биометрического образа. В связи с тем, что биометрическими параметрами становятся корреляционные связи, число анализируемых биометрических параметров многократно увеличивается. Исходные 416 биометрических параметров среды моделирования «БиоНейроАвтограф» дают $416^2/2 - 416 = 86\,112$ биометрических параметров. При этом значения коэффициентов корреляции имеют распределение близкое к нормальному, как это показано на рис. 5.

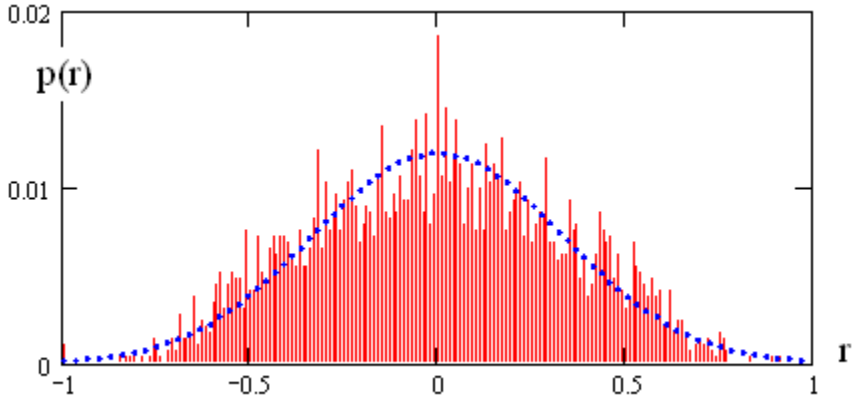


Рис. 5. Распределение коэффициентов корреляции параметров рукописного образа «*Пенза*» близко к нормальному
E(r)≈0,0, σ(r)≈0,334, $\tilde{r}$ ≈0,247

Большинство коэффициентов корреляции оказывается мало, высокие положительные и отрицательные значения коэффициентов корреляции редки (находятся в правом и левом хвостах распределения).

Одной из проблем создания новой технологии более глубокой нейросетевой обработки биометрических данных является проблема оценки коэффициентов корреляции на малых выборках. Классическая формула Пирсона–Эджуорта-Эудлона[10]:

$$r(x,y)=\frac{1}{16}\sum_{i=1}^{16}\frac{(E(x)-x_i)\cdot(E(y)-y_i)}{\sigma(x)\cdot\sigma(y)}. \qquad (1)$$

на малых выборках в 16 опытов дает очень большие погрешности. Примеры распределения значений коэффициентов корреляции для этого случая дан на рис. 6.

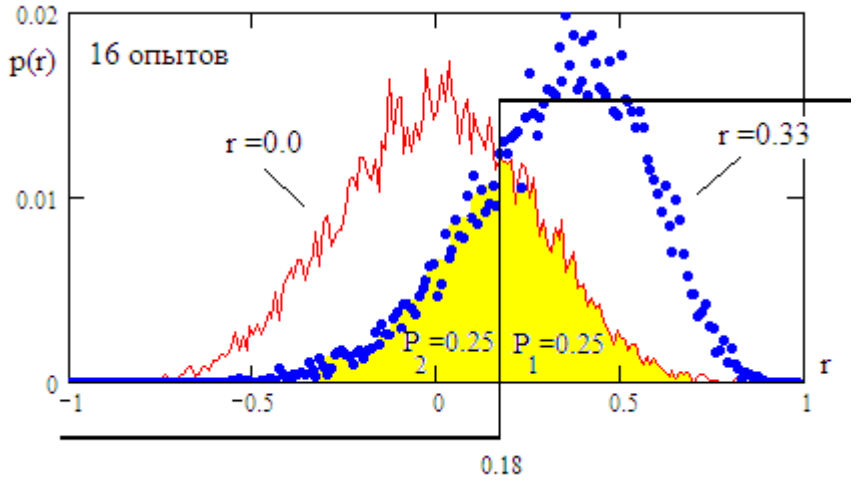


Рис. 6. Вероятности ошибок первого и второго рода корреляционного критерия Пирсона при различении независимых данных малых выборок в 16 опытов и зависимых данных r = 0,33

Из рис. 6 видно, что на малой выборке из 16 опытов при разделении независимых данных r = 0,0 и зависимых данных r = 0,33 вероятности ошибок первого и второго рода значительны $P_1 \approx P_2 \approx 0{,}25$.

Улучшить ситуацию можно двумя способами. Во-первых, можно увеличить число входов у корреляционных нейронов Байеса, во-вторых можно усложнить процедуру обучения, используя множество статистических критериев проверки гипотезы независимости малых выборок [8, 9].

Список литературы

1. Николенко С., Кудрин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Питер, 2018.
2. Чару А. Нейронные сети и глубокое обучение. СПб. : Диалектика, 2020. 756 с.
3. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.
4. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip
5. Иванов А. И. Исследование свойств нейросетевого преобразователя биометрия-код с использованием среды моделирования «БиоНейроАвтограф» : учеб.-метод. пособие. Пенза : Изд-во ПГУ, 2020. 40 с. URL: https://tsib.pnzgu.ru/page/39329
6. Ложников П. С. Биометрическая защита гибридного документооборота : монография / М-во обр. и науки РФ, ФГБОУ ВО «ОмГТУ». Новосибирск : Изд-во СО РАН, 2017. 130 с.
7. Иванов А. И., Сулавко А. Е. Использование сетей корреляционных нейронов с многоуровневым квантованием: защита от извлечения знаний из параметров решающего правила : препринт. Пенза : Изд-во ПГУ, 2020. 48 с.
8. Иванов А. И., Золотарева Т. А. Искусственный интеллект в защищенном исполнении: синтез статистико-нейросетевых автоматов многокритериальной проверки гипотезы независимости малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 105 с.
9. Иванов А. И., Серикова Ю. И., Золотарева Т. А., Полковникова С. А. Многокритериальная нейросетевая оценка коэффициентов корреляции для обработки малых выборок биометрических данных // Известия высших учебных заведений. Поволжский регион. Технические науки. 2021. № 1 (57). С. 13–22.
10. URL: wikipedia.org/Корреляция

Для цитирования: Сулавко А. Е., Ложников П. С., Иванов А. И., Золотарева Т. А. Оценка информативности биометрических данных динамики рукописного почерка при обогащении искусственными нейронами в линейном пространстве и корреляционными нейронами в квадратичном пространстве // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 47–54.

УДК 004.056

БЕСКОМПРОМАТНОЕ ПРИВЛЕЧЕНИЕ СТОРОННИХ РЕСУРСОВ НИЗКОГО ДОВЕРИЯ ДЛЯ ВЫПОЛНЕНИЯ ВЫЧИСЛЕНИЙ ВЫСОКОГО ДОВЕРИЯ В SIM-КАРТАХ И MICROSD-КАРТАХ С ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ БИОМЕТРИЧЕСКИХ ДАННЫХ НЕЙРОГОМОМОРФНЫМ ШИФРОВАНИЕМ

В. С. Князьков[1], А. И. Иванов[2], А. В. Безяев[3], В. С. Лукин[4]

[1,4]Пензенский государственный университет, г. Пенза

[2]Пензенский научно-исследовательский электротехнический институт, г. Пенза

[3]Пензенский филиал научно-технического центра «Атлас», г. Пенза

Аннотация. Рассматривается проблема формирования нейросетевого искусственного интеллекта, размещенного в доверенную среду с малыми вычислительными ресурсами по памяти, по разрядности, по потреблению, например, в виде SIM-карт, microSD-карт, RFID-токенов. Показано, что вычисления остаются доверенными, если используются нейросетевые решающие правила, защищенные гомоморфным шифрованием даже при привлечении внешних недоверенных вычислительных ресурсов. Сформулированы требования к механизмам гибридного нейро-гомоморфного шифрования.

Ключевые слова: вычисления высокого доверия, персональные биометрические данные, нейро-гомоморфное шифрование

UNCOMPROMISING INVOLVEMENT OF THIRD-PARTY LOW-TRUST RESOURCES TO PERFORM HIGH-TRUST CALCULATIONS IN SIM CARDS AND MICRO SD CARDS WITH THE PROTECTION OF PERSONAL BIOMETRIC DATA BY NEURO-HOMOMORPHIC ENCRYPTION

V. S. Knyazkov[1], A. I. Ivanov[2], A. V. Bizyaev[3], V. S. Lukin[4]

[1,4]Penza State University, Penza

[2]Penza Research Electrotechnical Institute, Penza

[3]Penza branch of Scientific and Technical Center "Atlas", Penza

Abstract. The problem of forming a neural network artificial intelligence placed in a trusted environment with small computing resources in memory, bit

depth, and consumption, for example, in the form of SIM cards, micro SD cards, and RFID tokens, is considered. It is shown that calculations remain trusted if neural network decision rules are used, protected by homomorphic encryption, even with the involvement of external non-trusted computing resources. The requirements for the mechanisms of hybrid neuro-homomorphic encryption are formulated.

Keywords: high-trust calculations, personal biometric data, neuro-homomorphic encryption

Первым в мировой практике биометрическим стандартом стал стандарт США FBI-1993, о том, как сжимать рисунки отпечатков пальцев и передавать их по телефонным линиям через модемы. Сегодня содержательная часть этого стандарта США положена в основу ГОСТ Р ИСО/МЭК 19794-4–2006. Еще одним важным для технологий было появления в 1998 году национальной спецификации США BioAPI, которая позднее была переведена в ранг международного стандарта ГОСТ Р ИСО/МЭК 19784-1–2007.

Неприятность во всем этом только одна, уже при первом публичном обсуждении BioAPI, начатого в 1996 году всплыла проблема защиты биометрических шаблонов. При этом разработчикам BioAPI удалось быстро успокоить озабоченную биометрико-криптографическую общественность США перспективами создания в ближайшие два-три года технологии гомоморфного шифрования. К сожалению, развитие новой технологии защиты не стало столь быстрым. Основные вехи развития технологии отражены в табл. 1.

Таблица 1

История развития технологиигомоморфного шифрования

Год создания	Авторы криптосхемы гомоморфного шифрования	Основные характеристики достигнутого уровня гомоморфизма
1	2	3
1978 г.	Рональд Риверст, Леонард Адлеман, Майкл Дертузосом (*авторы криптосхемыRSA, ввели понятие гомоморфное шифрование*).	Высказана идея, схемы шифрования пока нет
1982 г.	ШафриГольдвассер, Сильвио Микали *Частичный гомоморфизм*	Одно умножение.
1998 г.	ТацукиОмато, Сигенори Утиямо. *Частичный гомоморфизм*	Одно умножение.
1999 г.	Паскаль Пэйе. *Частичный гомоморфизм.*	Одно умножение.
2005 г.	Дэн Бонех, Ю ЧжинГо, КобиНиссом. *Частичный гомоморфизм.*	Одно умножение. Неограниченное число сложений.

Окончание табл. 1

1	2	3
2009 г.	КейгДженри *Полный гомоморфизм, очень сложные вычисления,накапливание ошибок*	Неограниченное число сложений. Неограниченное число умножений.
2012 г.	Цвик Бракерски, Крейг Генри, ВидонВайтунакон. *Полный гомоморфизм,приемлемые по сложности вычисления, накапливание ошибок.*	Неограниченное число сложений. Неограниченное число умножений
2019 г.	ISO/IES 18033-6: 2019 IT Security techniques-Encryption algorithms – Part 6: Homomorphic encryption	Присутствует эффект накопления ошибок с ростом размеров решающего правила

Из табл. 1 видно, что работоспособные схемы гомоморфного шифрования появились только в 2012 году (через 12 лет после спецификации BioAPI). После 2012 года должны быть были запущены работы по применению гомоморфного шифрования для защиты биометрических шаблонов BioAPI.

Стандарт по гомоморфному шифрованию появился только в 2019 году, однако на текущий момент пока нет сообщений о положительном опыте применения гомоморфного шифрования для защиты биометрических шаблонов (биометрических данных). Более того ряд зарубежных компаний, ориентирующихся на безопасную обработку биометрических данных с 2014 по 2018 гг. имели разделы по перспективам применения гомоморфного шифрования в их продуктах. На данный момент эти разделы удалены с сайтов компаний.

Причина пробуксовки применения гомоморфного шифрования для защиты биометрии проста: выяснилось, что гомоморфные решающие правила не могут быть как угодно большими. Начиная с некоторого размера гомоморфные шифротексты перестают однозначно расшифровываться. Чем длиннее шифротекст, тем больше вероятность, что гомоморфное решение не сможет верно расшифроваться на гомоморфном ключе. Такая ситуация не возникает в классическом шифровании, классическое шифрование (симметричное или асимметричное) позволяет шифровать и расшифровывать тексты любой длины.

Снять проблему накопления ошибок при гомоморфном шифровании удается, если пользоваться нейросетевыми решающими правилами и раздельно выполнять вычисления для каждого нейрона [1]. Нейросеть из 256 нейронов легко разбить на независимое вычисление каждого из нейронов отдельно. То есть можно заранее

подсчитать число гомоморфных операций для искусственных нейронов разного типа. Так нейроны с линейным накоплением данных, обученные по ГОСТ Р 52633.5–2011 преобразовывать динамику рукописного почерка, должны иметь 16 операций сложения и 16 операций умножения (всего 32 операции):

$$\begin{cases} y \leftarrow \sum_{i=1}^{16} \mu_i \cdot x_i \\ z(y) \leftarrow \text{"0"} \ \textit{если} \ \ y \le k \\ z(y) \leftarrow \text{"1"} \ \textit{если} \ \ y > k \end{cases}. \quad (1) \qquad \begin{cases} y \leftarrow \sum_{i=1}^{4} (c_i - x_i)^2 \\ z(y) \leftarrow \text{"00"} \ \textit{если} \ \ y \le k_1 \\ z(y) \leftarrow \text{"01"} \ \textit{если} \ \ k_1 > y \ge k_2 \\ z(y) \leftarrow \text{"10"} \ \textit{если} \ \ k_2 > y \ge k_3 \\ z(y) \leftarrow \text{"11"} \ \textit{если} \ \ y \ge k_3 \end{cases}. \quad (2)$$

Если перспективная схема гомоморфного шифрования будет неспособна поддерживать 32 операции сложения и умножения, то придется переходить к использованию квадратичных нейронов (2). При этом необходимо разрабатывать второй стандарт по автоматическому обучению сетей квадратичных нейронов [2]. В этом случае перспективная схема гомоморфного шифрования должны поддерживать только 8 операций решающего правила (четыре операции сложения и четыре операции умножения), как это следует из системы функциональных связей (2).

Следует отметить, что в настоящее время существует достаточно многоразличных видов нейронов. Отличаются они видом нелинейного деформирования пространства, в котором выполняется накопление данных тем или иным искусственным нейроном. В этом отношении появляется возможность получить достаточно широкий спектр различных требований к числу операций, поддерживаемых перспективными схемами гомоморфного шифрования. В частности промежуточное положение между линейными и квадратичными нейронами должны занимать нейроны среднего геометрического [3–5], которые требуют 16-ти операций умножения и не требуют применения операций сложения:

$$\begin{cases} y \leftarrow \sqrt[16]{\prod_{i=1}^{16} x_i} \\ z(y) \leftarrow \text{"0"} \ \textit{если} \ \ y \le k \\ z(y) \leftarrow \text{"1"} \ \textit{если} \ \ y > k \end{cases}. \quad (3) \qquad \begin{cases} y \leftarrow \sqrt[32]{\prod_{i=1}^{32} x_i} \Big/ \sum_{i=1}^{32} x_i \\ z(y) \leftarrow \text{"0"} \ \textit{если} \ \ y \le k \\ z(y) \leftarrow \text{"1"} \ \textit{если} \ \ y > k \end{cases}. \quad (4)$$

Гораздо большие требования к перспективным схемам гомоморфного шифрования будут предъявлять нейроны среднего гармонического (4). Нейроны среднего гармонического [6, 7] при анализе биометрии динамики рукописного почерка требуется использование 32 операции сложения и 32 операций умножения (всего 64 операций гомоморфных решающих правил).

Переход на нейросетевую декомпозицию решающих правил приводит к тому, что после гомоморфного шифрования можно привлекать внешние не доверенные вычисления. Схема привлечения внешних не доверенных вычислительных ресурсов для доверенных вычислений нейросетевой биометрии приведена на рис. 1.

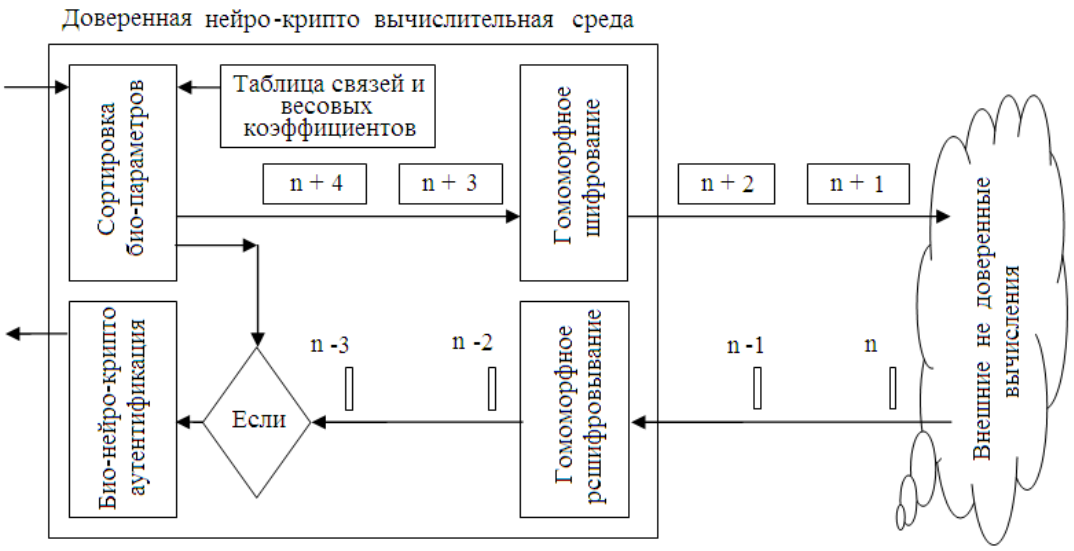


Рис. 1. Доверенные вычисления, ориентированные на привлечение внешнего не доверенного вычислителя при обычном гомоморфном шифровании (гомоморфизм относительно двух типов операций «сложения» и «умножения»)

Из рис. 1 видно, что по простейшей схеме привлечения внешних ресурсов доверенная вычислительная среда должна выполнять как операции гомоморфного шифрования, так и гомоморфного расшифровывания. Ослабить требования к вычислительным ресурсам доверенной вычислительной среды возможно в случае, если перечень гомоморфных операций (сложения и умножения) расширить, добавив в него операции сравнения с порогами. Это должно привести к многократному снижению информационного потока данных от привлеченного внешнего вычислителя обратно в доверенную вычислительную среду. Схема вычислений и обмена данными для этого случая приведена на рис. 2.

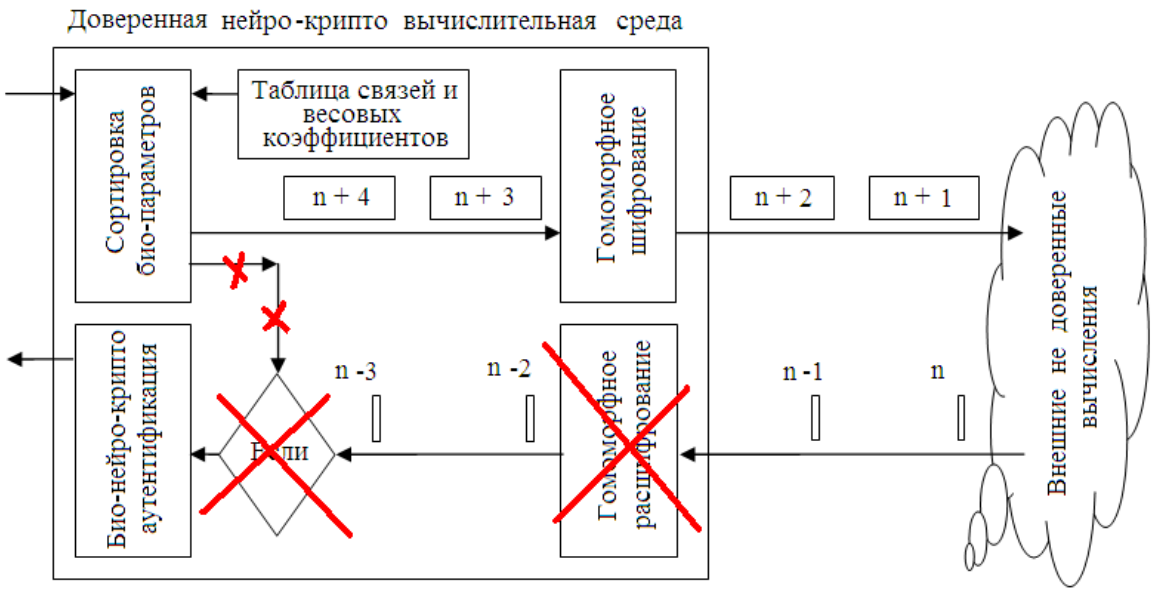


Рис 2. Доверенные вычисления, ориентированные на привлечение внешнего не доверенного вычислителя при обычном гомоморфном шифровании (гомоморфизм относительно трех типов операций «сложения», «умножения», «сравнения с порогами»)

Таким образом, работы по объединению нейронных сетей и схем гомоморфного шифрования являются актуальными. Необходимо выполнять работы в двух направлениях. Первое направление связано с совершенствование сетей искусственных нейронов, снижающих требования к перспективным схемам гомоморфного шифрования. Вторым направлением является совершенствование схем гомоморфного шифрования, способных за счет расширения числа операций, выполняемых в защищенной форме, полностью воспроизводить работу одного или нескольких искусственных нейронов.

В связи с низкой устойчивостью схем гомоморфного шифрования и расшифровывания (смотри таблицу 1) целесообразно как можно сильнее стремиться снизить число операций, выполняемых после выполнения гомоморфного шифрования. Число операций связано с типом применяемого искусственного нейрона (1), (2), (3), (4). На данный момент из рассмотренных в данной работе искусственных нейронов наиболее перспективными являются квадратичные нейроны, так как они могут иметь всего 4 входа (2). Однако на текущий момент времени стандарт по автоматическому обучению квадратичных нейронов с многоуровневым квантованием находится в стадии разработки [2].

Список литературы

1. Князьков В. С., Иванов А. И., Безяев А. В. Необходимость расширения функциональных возможностей гомоморфного шифрования для защиты нейросетевых решающих правил биометрических приложений искусственного интеллекта // Безопасность информационных технологий : сб. науч. ст. по материалам II Всерос. науч.-техн. конф. Пенза : Изд-во ПГУ, 2020. С. 5–10.

2. Иванов А. И., Безяев А. В., Малыгина Е. А., Серикова Ю. И. Второй национальный стандарт России по быстрому автоматическому обучению больших искусственных нейронных сетей на малых выборках биометрических данных // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза, 2019. С. 174–177.

3. Иванов А. И., Перфилов К. А., Малыгина Е. А. Оценка качества малых выборок биометрических данных с использованием дифференциального варианта статистического критерия среднего геометрического // Вестник Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнева. 2016. Т. 17, № 4. С. 864–870. URL: https://cyberleninka.ru/article/n/otsenka-kachestva-malyh-vyborok-biometri-cheskih-dannyh-s-ispolzovaniem-differentsialnogo-varianta-statisticheskogo-kriteriya

4. Иванов А. И., Перфилов К. А., Малыгина Е. А. Многомерный статистический анализ качества биометрических данных на предельно малых выборках с использованием критериев среднего геометрического, вычисленного для анализируемых функций вероятности // Измерение. Мониторинг. Управление. Контроль. 2016. № 2 (16). С. 64–72. URL: https://imuk.pnzgu.ru/IMUK9216

5. Иванов А. И., Малыгина Е. А., Перфилов К. А., Вятчанин С. Е. Сравнение мощности критерия среднего геометрического и критерия Крамера – фон Мизеса на малых выборках биометрических данных // Модели, системы, сети в экономике, технике, природе и обществе. 2016. № 2 (18). С. 155–163. URL: https://mss.pnzgu.ru/mss19216

6. Иванов А. И., Перфилов К. А., Лукин В. С. Нейросетевое обобщение семейства статистических критериев среднего геометрического и среднего гармонического для прецизионного анализа малых выборок биометрических данных // Информационно-управляющие телекоммуникационные системы, средства поражения и их техническое обеспечение : сб. науч. ст. по материалам Всерос. науч.-техн. конф. / под общ. ред. В. С. Безяева. Пенза : АО «НПП "Рубин"», 2019. С. 50–63. URL: https://www.elibrary.ru/item.asp?id=42742831

7. Лукин В. С. Сравнение мощности обычной и логарифмической форм статистических критериев среднего гармонического при использовании для проверки гипотезы нормального распределения данных малой выборки // Известия высших учебных заведений. Поволжский регион. Технические науки. 2020. № 4.

Для цитирования: Князьков В. С., Иванов А. И., Безяев А. В., Лукин В. С. Бескомпроматное привлечение сторонних ресурсов низкого доверия для выполнения вычислений высокого доверия в SIM-картах и микро SD-картах с защитой персональных биометрических данных нейро-гомоморфным шифрованием // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 55–62.

УДК 004.056; 004.89; 57.087

ПАКЕТ ТРЕБОВАНИЙ, ОБЕСПЕЧИВАЮЩИХ ДОВЕРИЕ К МАЛЫМ ВЫБОРКАМ ПРИМЕРОВ ОБУЧЕНИЯ НЕЙРОСЕТЕВЫХ ПРИЛОЖЕНИЙ МЕДИЦИНСКОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

М. С. Геращенко, М. В. Маркулева, А. Ю. Щербакова

Пензенский государственный университет, г. Пенза

Аннотация. Рассматриваются вопросы использования искусственных нейронных сетей в медицине. Определен пакет требований при обработке данных.

Ключевые слова: пакет требований, нейросетевые приложения, медицинский искусственный интеллект

A SET OF REQUIREMENTS THAT PROVIDE CONFIDENCE IN SMALL SAMPLES OF TRAINING EXAMPLES FOR NEURAL NETWORK APPLICATIONS OF MEDICAL ARTIFICIAL INTELLIGENCE

M. S. Gerashchenko, M. V. Markuleva, A. Yu. Shcherbakova

Penza State University, Penza

Abstract. The article deals with the use of artificial neural networks in medicine. A set of requirements for data processing is defined.

Keywords: set of requirements, neural network applications, medical artificial intelligence

В настоящее время в соответствии с указом президента В. В. Путина «О развитии искусственного интеллекта в РФ» от 19.10.19 активно ведутся исследования, связанные с применением в медицине сетей искусственных нейронов. Специалисты по медицинской информатике должны обладать компетенциями по обучению, тестированию, применению больших сетей искусственных нейронов.

Для получения навыков нейросетевой обработки студенты медицинского факультета должны уметь самостоятельно выбрать

структуру сети искусственных нейронов, получить данные для ее обучения и тестирования. Далее следует выполнить обучение нейросети, ее тестирование, документирование результатов исследования.

При выборе структуры нейросети желательно заранее знать основные особенности нейронных сетей и уровень их востребованности в медицинских приложений. Так, если студент, пожелает применять на практике большие многослойные сети глубокого обучения [1, 2], то для их обучения должны будут привлекаться значительные вычислительные ресурсы и обучение должно выполняться на обучающих выборках большого объема (сотни и тысячи примеров) под руководством квалифицированного человека.

Напротив, применение однослойных сетей искусственных нейронов может быть выполнено автоматически алгоритмом ГОСТ Р 52633.5 [3] на обучающей выборке в 20 примеров. Далее может быть выполнено быстрое тестирование обученной нейросети алгоритмом ГОСТ Р 52633.3 [4] На малой тестовой выборке из 20 тестовых примеров, не использованных при обучении.

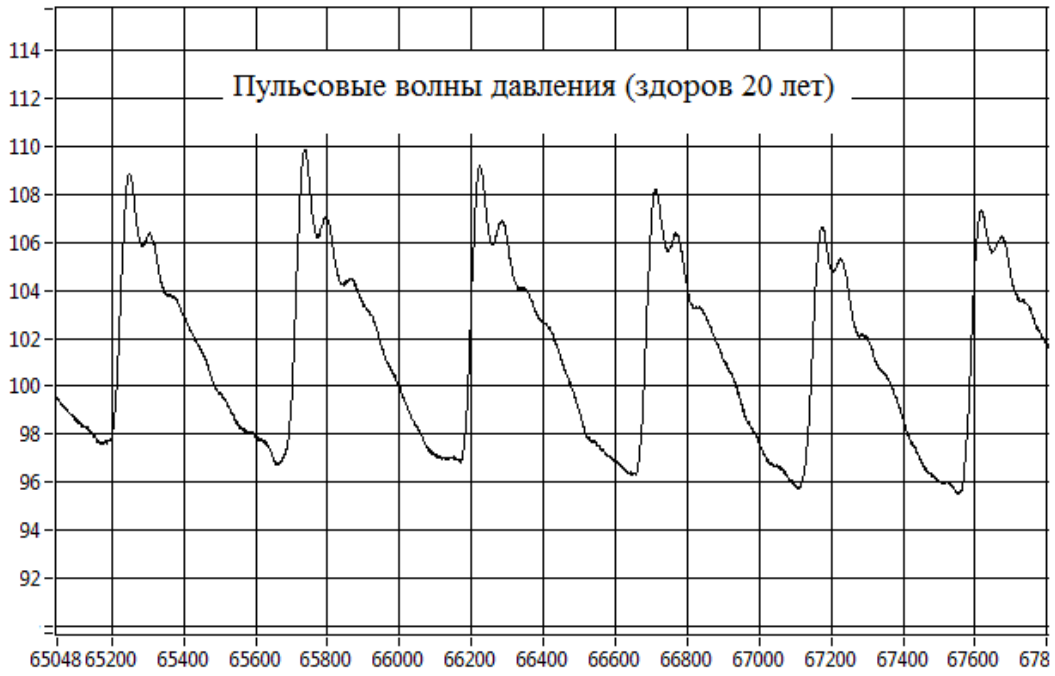


Рис. 1. Пример пульсовой волны нормального давления (здоров 20 лет)

Для использования стандартизованного в России алгоритма обучения должны иметься примеры, либо они должны быть скачены

с сайта университета. В качестве примера рассмотрим особенности нейросетевого анализа пульсовых волн, отображенных на рис. 1 и рис. 2.

Рис. 2. Пример пульсовой волны повышенного давления
(60 лет, утрачена эластичность кровеносных сосудов)

Медицинские приложения нейросетевого искусственного интеллекта должны быть доверенными. Это означает, что при их создании должен быть выполнен пакет требований в соответствии с которым:

- для обучения и тестирования должен быть использован заданный минимально допустимый объем обучающих и тестовых выборок;
- происхождение обучающих и тестовых выборок должно быть известно, а сами файлы с биометрическими данными должны быть подписаны электронной цифровой подписью;
- обучение должно выполняться на предварительно обработанных исходных данных (в нашем случае должна быть выполнена нарезка волн и выделение из них контролируемых биометрических параметров);
- обучение должно выполняться доверенным (сертифицированным) средством обучения;
- тестирование должно выполняться доверенным (сертифицированным) средством тестирования.

Список литературы

1. Николенко С., Кудрин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Питер, 2018.

2. Чару А. Нейронные сети и глубокое обучение. СПб. : Диалектика, 2020. 756 с.

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

4. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

Для цитирования: Геращенко М. С., Маркулева М. В., Щербакова А. Ю. Пакет требований, обеспечивающих доверие к малым выборкам примеров обучения нейросетевых приложений медицинского искусственного интеллекта // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 63–66.

УДК 004.056; 004.89; 57.087

БЫСТРАЯ СХОДИМОСТЬ ПРОЦЕДУР СИММЕТРИЗАЦИИ КОРРЕЛЯЦИОННЫХ СВЯЗЕЙ БИОМЕТРИЧЕСКИХ ДАННЫХ

Ю. И. Серикова[1], Т. А. Золотарева[2], Н. А. Иванова[3]

[1]Пензенский государственный университет, г. Пенза

[2]Липецкий государственный педагогический университет имени П. П. Семенова-Тян-Шанского, г. Липецк

[3]Российское отделение компании «ABBYY», г. Москва

Аннотация. Рассмотрены вопросы симметризации корреляционных связей биометрических данных и их влияние на результат биометрико-нейросетевой аутентификации.

Ключевые слова: симметризация корреляционных связей, биометрические данные, биометрико-нейросетевая аутентификация

FAST CONVERGENCE OF BIOMETRIC DATA CORRELATION SYMMETRIZATION PROCEDURES

Yu. I. Serikova[1], T. A. Zolotareva[2], N. A. Ivanova[3]

[1]Penza State University, Penza

[2]Lipetsk State Pedagogical University named after P. P. Semenov-Tyan-Shansky, Lipetsk

[3]Russian branch of the company "ABBYY", Moscow

Abstract. The issues of symmetrization of biometric data correlations and their influence on the result of biometric-neural network authentication are considered.

Keywords: symmetrization of biometric data correlations, biometric-neural network authentication

Учет влияния коэффициентов корреляции на результат нейросетевой биометрической аутентификации при решении задач высокой входной размерности целесообразно выполнять через симметризацию корреляционных связей [1–3]:

$$\begin{bmatrix} 1 & r_1 & r_2 & \vdots\vdots & r_n \\ r_1 & 1 & r_{n+1} & \vdots\vdots & r_{2n-2} \\ r_2 & r_{n+1} & 1 & \vdots\vdots & r_{3n-3} \\ \vdots\vdots & \vdots\vdots & \vdots\vdots & \vdots\vdots & \vdots\vdots \\ r_n & r_{2n-2} & r_{3n-3} & \vdots\vdots & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & \tilde{r} & \tilde{r} & \vdots\vdots & \tilde{r} \\ \tilde{r} & 1 & \tilde{r} & \vdots\vdots & \tilde{r} \\ \tilde{r} & \tilde{r} & 1 & \vdots\vdots & \tilde{r} \\ \vdots\vdots & \vdots\vdots & \vdots\vdots & \vdots\vdots & \vdots\vdots \\ \tilde{r} & \tilde{r} & \tilde{r} & \vdots\vdots & 1 \end{bmatrix}, \qquad (1)$$

где нумерация коэффициентов корреляции исходной корреляционной матрицы построена исходя симметричности всех корреляционных матриц относительно диагонали (номер коэффициентов монотонно увеличивается при движении слева направо и вниз по строкам).

Формально одинаковые коэффициенты эквивалентной симметричной матрицы могут быть вычислены усреднением модулей коэффициентов корреляции исходной асимметричной матрицы:

$$\tilde{r} \approx \frac{2}{n^2 - n} \cdot \sum_{i=1}^{\frac{n^2-n}{2}} |r_i| \,. \qquad (2)$$

На рис. 1 приведена программная реализация соответствующего численного эксперимента, написанная на языке моделирования MathCAD для корреляционных матриц 4-го порядка.

```
S4(rr) := | x ← rnorm(6,0,0.33 + rr)
          | for i ∈ 0..5
          |   y_i ← |x_i|
          | (mean(y)  stdev(y))^T

i := 0..9999    rr_i := rnd(0.01)
xx^(i) := S4(rr_i)
E4_i := (xx^(i))_0
```

E4 =

	0
0	0.141
1	0.292
2	0.439
3	0.287
4	0.271
5	0.306
6	0.187
7	0.32
8	0.296

Рис. 1. Пример программной реализации вычисления распределения коэффициентов корреляции эквивалентной симметричной корреляционной матрицы

Очевидно, что похожие программные реализации могут быть получены и для корреляционных матриц более высоких размеров. Результаты численного эксперимента для матриц 4, 8, 16, 32 порядков приведены на рис. 2.

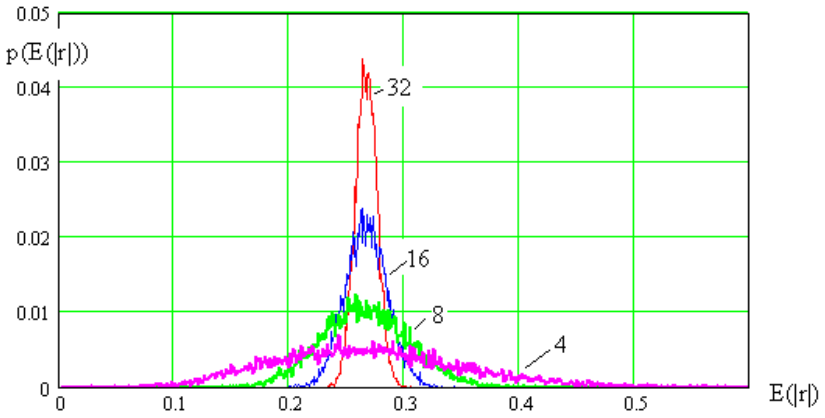


Рис. 2. Быстрое снижение стандартного отклонения среднего значения модулей коэффициентов корреляции с ростом размерности симметризуемой корреляционной матрицы

Из рис. 2 виден эффект быстрого снижения стандартных отклонений распределений среднего модулей коэффициентов корреляции с ростом порядка симметризуемой матрицы. Результаты численного моделирования отражают также то, что процедура симметризации является сильным нормализатором. Даже нормализация матриц 4-го порядка дает почти нормальное распределение.

Список литературы

1. Ivanov A. I., Lozhnikov P. S., Serikova Yu. I. Reducing the Size of a Sample Sufficient for Learning Due to the Symmetrization of Correlation Relationships Between Biometric Data // Cybernetics and Systems Analysis. 2016. № 3. P. 49–56. URL: http://link.springer.com/article/10.1007/s10559-016-9838-x

2. Волчихин В. И., Иванов А. И., Малыгина Е. А., Серикова Ю. И. Обучение сетей квадратичных форм на малых выборках биометрических данных с использованием процедуры симметризации корреляционных связей // Измерение. Мониторинг. Управление. Контроль. 2018. № 1 (23). С. 66–74.

3. Иванов А. И., Банных А. Г., Серикова Ю. И. Учет влияния корреляционных связей через их усреднение по модулю при нейросетевом обобщении статистических критериев для малых выборок // Надежность. 2020. № 20 (2). С. 28–34. URL: //doi.org/10.21683/1729-2646-2020-20-2-28-34

Для цитирования: Серикова Ю. И., Золотарева Т. А., Иванова Н. А. Быстрая сходимость процедур симметризации корреляционных связей биометрических данных // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 67–69.

УДК 681.3.81

АНАЛИЗ ЭКРАНИРОВАНИЯ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ В АППАРАТУРЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

К. А. Ратников, Е. А. Персиков

Пензенский государственный университет, г. Пенза

Аннотация. Рассматривается проблема утечки информативных сигналов по побочным электромагнитным полям и наводкам (ПЭМИН) в аппаратуре защиты информации. Выполнен анализ возможности и эффективности применения сплошных экранов с различными характеристиками для снижения электромагнитных полей, генерируемых аппаратурой.

Ключевые слова: экранирование, электромагнитное поле, ПЭМИН

ANALYSIS OF ELECTROMAGNETIC FIELD SHIELDING IN SPECIAL-PURPOSE EQUIPMENT

K. A. Ratnikov, E. A. Persikov

Penza State University, Penza

Abstract. The problem of leakage of informative signals by transient electromagnetic pulse emanation standard (TEMPEST) in information security equipmentis considered. The analysis of the possibility and efficiency of using solid screens with different characteristics to reduce the electromagnetic fields generated by the equipment is carried out.

Keywords: electromagnetic field, shielding, TEMPEST

Современная мобильная аппаратура специального назначения представляет собой металлический бокс габаритами сравнимыми с системным блоком персонального компьютера. Как и любая другая электронная аппаратура, аппаратура специальной связи излучает электромагнитные поля, перехватив которые может быть раскрыта информация, обрабатываемая аппаратурой. Целью данной работы является анализ достаточности методов по экранированию электромагнитного поля, применяемых в аппаратуре специального назначения.

Защита от ПЭМИН может быть двух типов: пассивная – применяются различные экраны, ослабляющие электромагнитное излучение аппаратуры; активная – средствами активной защиты инфор-

мации от утечки информации за счет ПЭМИН, т.е. генераторами электромагнитного шума. Средства активной защиты информации эффективно скрывают информативное излучение, однако электромагнитное излучение, генерируемое данными средствами защиты, оказывают пагубное влияние на организм [1]. В связи с данным фактом, при разработке аппаратуры защиты информации, разработчики внедряют пассивные средства защиты от ПЭМИН. Только в исключительных случаях внедряются активные средства защиты.

Согласно стандарту I класс экран-камер должен обеспечивать экранирование свыше 80 дБ [2]. В данной работе установлен более жесткий критерий экранирования свыше 100 дБ.

В данной работе проведен анализ исключительно основного прибора. Периферийные модули и каналы связи, выходящие за пределы основного прибора, но входящие в его непосредственный состав в данной работе не рассмотрены.

Для анализа примем следующие характеристики прибора за базовые:

основной вычислитель – «Эльбрус-8с» с тактовой частотой 1,3 ГГц;

шина PCI Express 1.1 ГГц;

контроллеры ввода-вывода информации – «К19869х» с тактовой частотой 4 МГц;

связь между контроллерами ввода-вывода по интерфейсу UARTс частотой 115,2 КГц;

линии USB 2.0 с частотой 12 МГц;

корпус прибора – алюминий 2 мм;

габариты прибора Д*Ш*В:0,50*0,15*0,30 м;

стыки составных частей корпуса, технологические дверцы проклеены по периметру экранирующей лентой;

блоки ввода-вывода информации отделены от основного вычислителя корпусом из алюминия 2 мм.

Для расчета эффективности экранирования корпуса прибора следует определить некоторые переменные.

Экранирующие действие материала корпуса прибора, определяется величиной, называемой эквивалентной глубиной проникновения Δ [3].

$$\Delta = 0{,}52\sqrt{\frac{\rho}{\mu_r f}}, \qquad (1)$$

где ρ – удельное сопротивление материала корпуса, для алюминия равное $0{,}28*10^{-7}$ Ом*м; μ_r – относительная магнитная проницаемость материала экрана, для алюминия равное 1,000023; f – частота, МГц;

Для экранов разных форм вводится обобщенный параметр $R_э$, который рассчитывается по формуле:

$$R_э = \sqrt[3]{\frac{3}{4\pi}abc}, \quad (2)$$

где a – длина экрана; b – ширина экрана;с – высота экрана.

Для рассматриваемого прибора $R_э$ = 0,17512.

Эффективность экранирования рассчитывается по формуле:

$$Э_{0E(H)} = \sqrt{\frac{\Delta}{\rho}Z_E(H)}\sqrt[3]{\frac{\lambda}{R_э}e^{\left(\frac{2\pi d}{m}\right)}}\left(1-\frac{\pi m}{\lambda}\right)^6, \quad (3)$$

где Δ – глубина проникновения, м;ρ – удельное сопротивление материала корпуса, Ом*мм^2/м; $Z_E(H)$ – волновое сопротивление электрического поля; $R_э$ – эквивалентный радиус экрана, м; m – наибольший размер щели в экране, м; d – толщина материала экрана, м.

Эффективность экранирования в дБ рассчитывается по формуле:

$$A = 20 \lg Э_{0E(H)}. \quad (4)$$

Аргумент m, т.е. размер щели приравнен к 0.0001 м, т.к. щели в приборе, а также открывающиеся части корпуса проклеены экранирующей лентой.

Для всех частот в приборе рассчитано экранирующие действие материала корпуса прибора, рассчитана длина электромагнитной волны, генерируемой источником, рассчитана эффективность экранирования. Данные сведены в табл. 1.

Как видно из табл. 1 эффективность экранирования корпуса прибора крайне высокая. Корпус полностью гасит электромагнитные поля, создаваемые элементами прибора. Причем с уменьшением частоты эффективность экранирования увеличивается.

Рассмотрим зависимости эффективности экранирования от толщины корпуса и максимального размера щели. Расчеты приведем для частот 1300 МГц,10 МГц, 0.1 МГц. Зависимость эффективности экранирования от размера щели при корпусе из алюминия 2мм приведена в таблице 2. Зависимость эффективности экраниро-

вания от толщины корпуса при размере щели в корпусе 0,0005 м приведена в табл. 2.

Таблица 1

Эффективность экранирования электромагнитного поля корпусом прибора

Элемент, генерирующий электромагнитный сигнал	Частота, МГц	Эквивалентная глубина проникновения, м	Длина генерируемой электромагнитной волны, м	Эффективность экранирования, дБ
Эльбрус-8с	1300	$2,4*10^{-6}$	0,2306	777,7 дБ
Шина PCI-e	1100	$2,6*10^{-6}$	0,2725	778,1 дБ
Линии USB 2.0	12	$2,5*10^{-5}$	24,9827	787,9 дБ
К19869х (контроллеры ввода-вывода)	4	$4,4*10^{-5}$	74,9481	790,4 дБ
Интерфейс UART (основной вычислитель – контроллеры ввода-вывода)	0,1152	$2,6*10^{-4}$	2602,37	798,1 дБ

Таблица 2

Зависимость эффективности экранирования корпуса прибора от размера щели

Размер щели, м	Частота, МГц	Эффективность экранирования	Эффективность экранирования, дБ
0,0005	1300	$5,8*10^{8}$	195,3
	10	$2,05*10^{10}$	206,2
	0,1	$6,5*10^{10}$	216,3
0,001	1300	$1,3*10^{6}$	122,3
	10	$4,7*10^{6}$	133,4
	0,1	$1,5*10^{7}$	143,5
0,005	1300	1126	61
	10	5790	75,3
	0,1	18367	85,3
0,01	1300	309	49,8
	10	2497	67,9
	0,1	7947	78
0,05	1300	0	0
	10	1246	61,9
	0,1	4064	72,2

Таблица 3

Зависимость эффективности экранирования от толщины материала корпуса (алюминий)

Толщина корпуса, м,	Частота, МГц	Эффективность экранирования	Эффективность экранирования, дБ
0,002	1300	$5{,}8*10^{9}$	195,3
	10	$2*10^{10}$	206
	0,1	$6{,}5*10^{10}$	216,3
0,001	1300	$1{,}3*10^{6}$	122,3
	10	$4{,}7*10^{6}$	133,4
	0,1	$1{,}5*10^{7}$	143,5
0,0005	1300	20382	86,2
	10	71681	97,1
	0,1	226747	107,1
0,0001	1300	714	57,1
	10	2512	68
	0,1	7948	78

На основе табл. 2 и 3 составлены графики зависимости эффективности экранирования от размера щели в корпусе из алюминия 2 мм – рис. 1, и зависимость эффективности экранирования от толщины корпуса при размере щели в корпусе 0,0005 м – рис. 1.

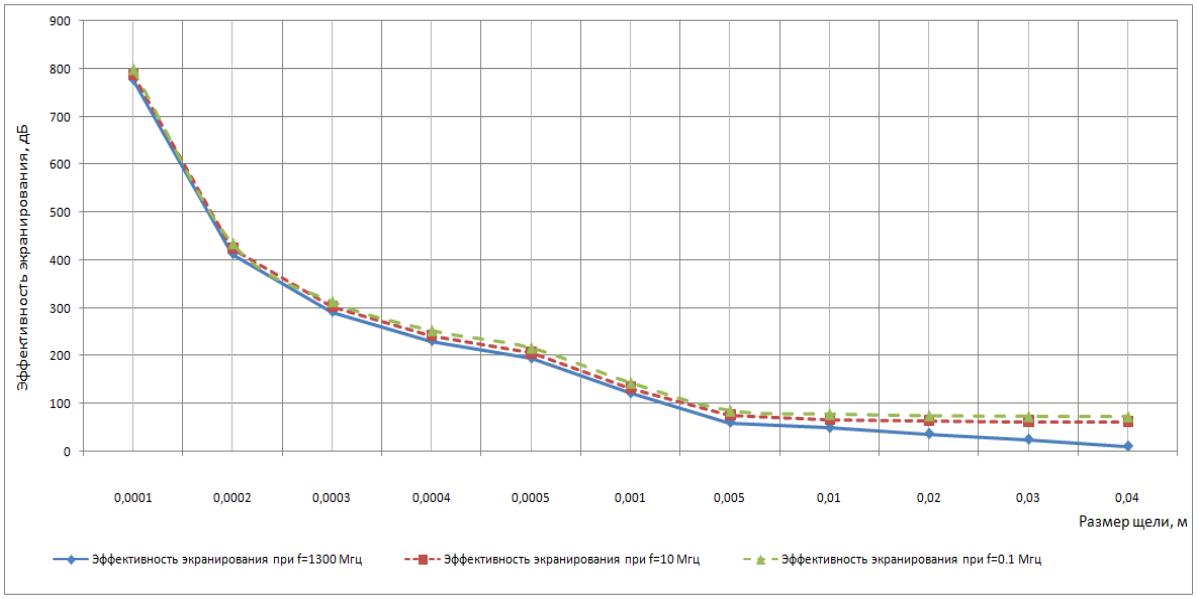


Рис. 1. Зависимость эффективности экранирования от размера щели при толщине алюминия корпуса 2 мм

Как видно из графиков, показанных на рис. 1 и 2, эффективность экранирования зависит в большей степени от наличия и размера щелей экрана, чем от толщины экрана из алюминия. Так при толщине экрана всего 10 микрон, что сравнимо с толщиной фольги для запекания, эффективность экранирования электромагнитного поля для частоты 1300 МГц составляет 51 дБ, для частоты 10 МГц 62 дБ, а для частоты 0,1 МГц 72 дБ. Следует отметить, что последующее уменьшение толщины материала не оказывают заметного влияния на эффективность экранирования.

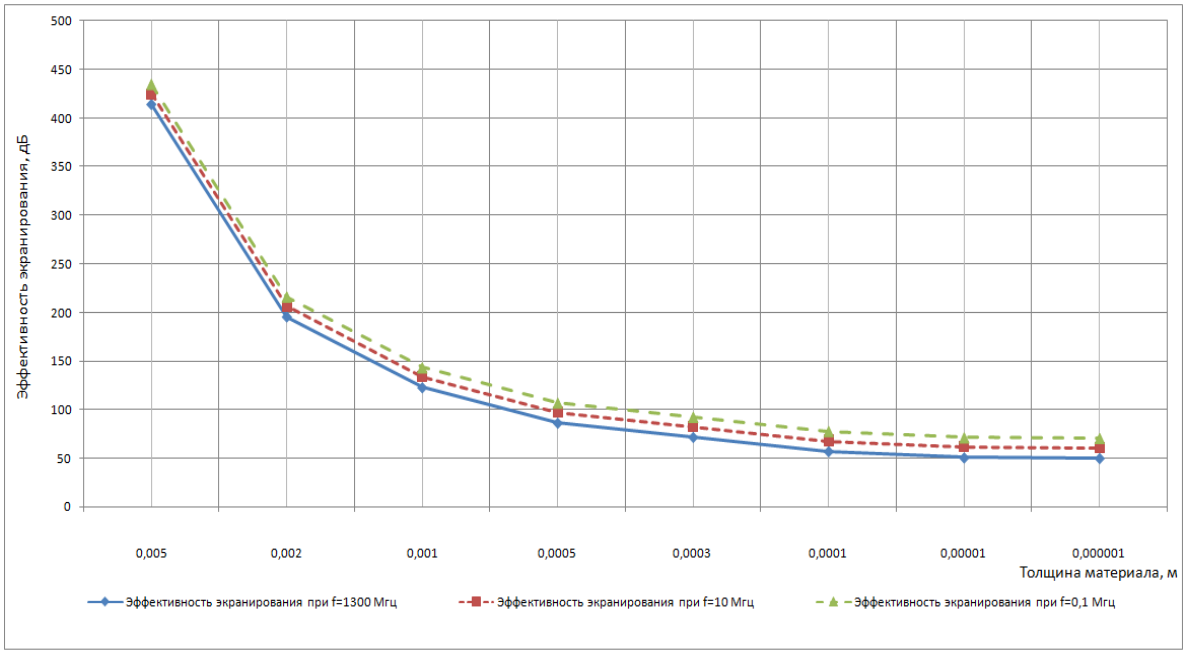


Рис. 2. Зависимость эффективности экранирования от толщины алюминия при максимальном размере щели 0,0005 м

Таким образом, видно, что для эффективности электромагнитного экранирования свыше 100 дБ при толщине корпуса из алюминия 2 мм размер щели не должен превышать 1,4 мм. Также, в случае если максимальный размер щели не превышает 0,5 мм, толщина корпуса может быть равна 0,7 мм.

Что показывает практика? Сплошные экраны из алюминия эффективно экранируют электрическую составляющую электромагнитного поля. Однако магнитная составляющая практически не экранируется алюминиевыми корпусами аппаратуры, особенно неэффективно такое экранирование для низкочастотной составляющей (0–5 кГц). Для уменьшения магнитного поля применяются различные схемотехнические решения, например уменьшение силы тока в сигнальной цепи до предельно малых значений.

Список литературы

1. Влияние электромагнитных полей на здоровье человека и способы защиты от их вредного воздействия. URL: http://13.rospotrebnadzor.ru/center/services/zdorov_obraz/135871

2. ГОСТ Р 50414–92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Классы, основные параметры, технические требования и методы испытаний.

3. Парфенов Е. М., Усачев В. П., Шерстнев В. В. Экранирование в ЭВА и РЭА. М. : РИО МВТУ, 1986.

Для цитирования: Ратников К. А., Персиков Е. А. Анализ экранирования электромагнитного поля в аппаратуре специального назначения // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 70–76.

УДК 681.3.81

ОСОБЕННОСТИ РАЗРАБОТКИ ЗАЩИЩЕННОЙ КЛАВИАТУРЫ, ПРИМЕНЯЕМОЙ В АППАРАТУРЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

К. А. Ратников

Пензенский государственный университет, г. Пенза

Аннотация. Рассмотрена проблема создания защищенной клавиатуры для аппаратуры защиты информации. Рассмотрены методы и решения для защиты от утечки информации по визуальному, виброакустическому, электромагнитному каналам, применяемые в клавиатурах аппаратуры защиты информации.

Ключевые слова: защищенная клавиатура, утечка информации, защита информации

DEVELOPMENT FEATURES OF A PROTECTED KEYBOARD USED IN SPETIAL-PURPOSE EQUIPMENT

K. A. Ratnikov

Penza State University, Penza

Abstract. The problem of creating a protected keyboard for information security equipment is considered. Methods and solutions for protection against information leakage through visual, vibro-acoustic, electromagnetic channels, used in keyboards of information security equipment, are considered.

Keywords: protected keyboard, against information leakage, information security

Как любой персональный компьютер аппаратура специального назначения имеет в своём составе множество устройств ввода-вывода информации. Эти устройства можно разделить на две категории: устройства, к которым предъявляются специальные требования по защите обрабатываемой информации и устройства, к которым данные требования не предъявляются.

Предъявление требований по защите информации зависит от того какую информацию устройства обрабатывают. Требования будут применены, если блок обрабатывает исходную (открытую) и ключевую информацию (далее ОИ и КИ соответственно). Причем

требования для КИ более строгие, нежели для ОИ, т.к. раскрытие ключа приведет к раскрытию всей зашифрованной на данном ключе информации.

Так, например «мышь» является устройством ввода, однако она не обрабатывает ни ОИ, ни КИ, поэтому данное устройство не требует применение мер по защите обрабатываемой информации. Клавиатура же наоборот обрабатывает как ключевую, так и открытую информацию, поэтому для неё требуется применение специальных защитных мер, направленных на защиту информации от утечки.

В общем случае выделим следующие каналы утечки информации для клавиатуры: визуальный, виброакустический, электромагнитный [1, 2]. Применение тех или иных мер по защите информации от утечки по названным каналам зависят от модели нарушителя и могут применяться как в комплексе, так и раздельно. Также следует отметить, что клавиатура может быть как встроенная, так и внешняя. В зависимости от этого появляется/отпадает необходимость в защите канала связи между клавиатурой и хостом.

При использовании визуального канала утечки информации нарушитель ведет наблюдение за действиями легитимного пользователя. К мерам защиты от утечки информации по визуальному каналу относятся организационные методы противодействия. К таким мерам относятся:

– ограничение количества лиц, находящихся в помещении при работе со специальной аппаратурой;

– ограничение видимости клавиатурного поля.

Виброакустический канал утечки информации обуславливается звуком, возникающим при нажатии клавиш клавиатуры. Если записать данный звук, то для каждой клавиши будет свой уникальный аудио сигнал. К данному способу перехвата информации особенно уязвима семантически нагруженная ОИ, т.к. после набора определенного количества аудио сигналов можно, на основании таблиц частоты использования букв алфавита, восстановить исходный текст [3]. Чем больше звуков нажатия клавиш удастся перехватить, тем более точно можно восстановить исходную информацию.

Для защиты информации, набираемой на клавиатуре, от перехвата по виброакустическому каналу используется несколько методов. Первый метод относится к пассивной защите и состоит в том, что клавиши делаются из резины, тем самым характерный «клацающий» звук сводится к минимуму. К недостаткам данного метода относится практически полное отсутствие тактильности у таких

клавиатур. Скоростной набор текста из-за достаточно высокой упругости клавиш становится затруднен. Однако к основному недостатку данного метода относится то, что даже с использованием резиновой матрицы звук нажатия клавиш полностью не исчезает и возможность перехвата звука нажатия остается.

К методу лишенного указанных недостатков относится активный метод противодействия через систему постановки виброакустических и акустических помех. При использовании данного метода на клавиатуре располагается переключатель, который активирует систему виброакустических помех. Только при включенной системе активного зашумления контроллер клавиатуры пересылает на хост пакеты с кодами нажатых клавиш. Также при работе генератора шума проверяется корректность его генератора. Контроллеры клавиатуры и генератора находятся в постоянном взаимодействии и, если генерируемый шум не удовлетворяет требованиям, работа клавиатуры немедленно прекращается. Если рассматривать данный метод исключительно со стороны защиты от утечки информации по виброакустическому каналу, то он практически лишен недостатков. Основным недостатком является неудобство работы персонала в условиях постановки виброакустического шума.

Постановка виброакустических и акустических помех совместно с применением резиновой матрицы делают клавиатуру защищенной от утечки информации по виброакустическому и акустическому каналу.

Электромагнитный канал утечки информации. В общем виде клавиатурную матрицу можно представить так, как показано на рис. 1.

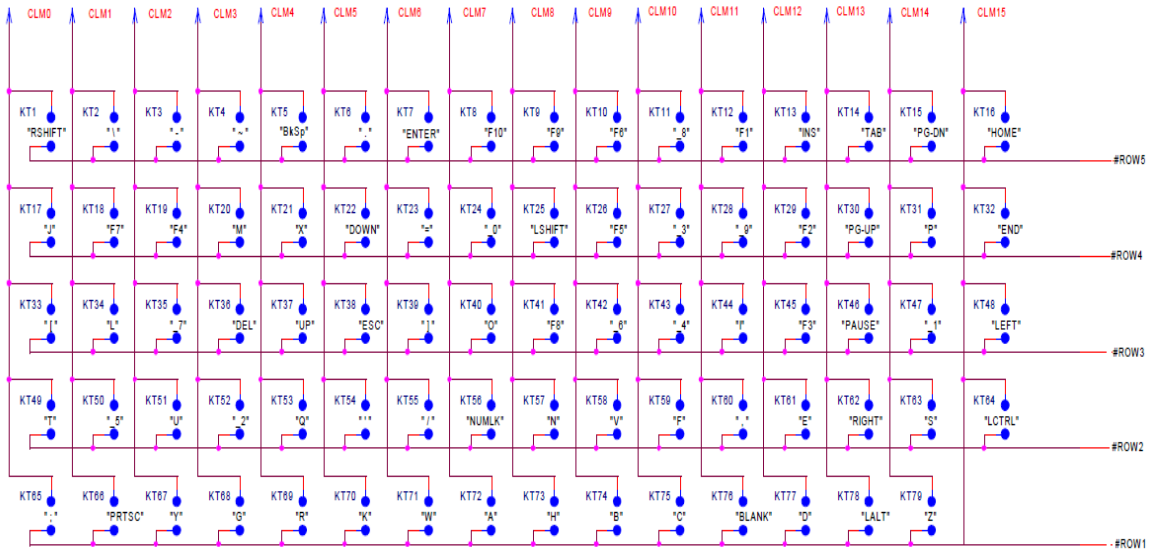


Рис. 1. Схема клавиатурной матрицы

Кнопки формируют сетку матрицы, где каждая кнопка имеет свою уникальную координату [CLMx; ROWy]. Таким образом минимальное количество контактов (пинов) микроконтроллера, требуемое для обработки клавиатурной матрицы равно $2\sqrt{N}$, где N – количество клавиш в клавиатуре. Если корень из N не равен целому числу, то минимальное число требуемых контактов микроконтроллера округляется до целого числа в большую сторону. Алгоритм обработки нажатия клавиши также достаточно прост. По столбцам контроллер запускает «бегущий ноль» или «бегущую единицу» (зависит от подтяжки на принимающей стороне), а на строках анализируется состояние пина.

Например, исходя из схемы, представленной на рис. 1, по столбцам (CLM) запускается «бегущий ноль», на строках(ROW) смотрится состояние пина. На CLM2 подается логический 0, при этом анализируется состояние строк (ROW), если на строку ROW4 пришёл логический 0, это означает о нажатии клавиши "F4".

Данная схема организации клавиатуры хорошо работает, при этом количество задействованных пинов микроконтроллера минимально. Однако при работе на клавиатурной матрице генерируется низкочастотное поле (0,1–10 кГц), генерируемое «бегущим нулем» или «бегущей единицей». Электромагнитное поле с данной частотой не экранируется сетчатыми экранами. Экранирование возможно лишь сплошным экраном, при этом толщина экрана может быть минимальной [4]. В связи с этим защищенная клавиатура состоит из нескольких слоев: нижний экран (корпус клавиатуры), клавиатурная матрица, упругий сплошной экран, резиновая мембрана с клавишами.

Применяемое экранирование эффективно экранирует электрическую составляющую электромагнитного поля, однако магнитная составляющая экранируется недостаточно эффективно.

Для снижения электромагнитного поля схема с «бегущим нулем» или «бегущей единицей» не применяется. В данном случае каждой кнопке назначается свой пин микроконтроллера. Соответственно количество требуемых входов контроллера равно количеству клавиш клавиатуры. Для снижения магнитной составляющей в цепи клавиш устанавливаются токоограничивающие резисторы с номиналом, обеспечивающим минимально возможный ток, т.к. магнитный поток, проходящий через контур пропорционален силе тока в контуре. Помимо резистора в цепь устанавливается керамический конденсатор, обеспечивающий подавление паразитных

импульсов, а также сглаживание прямоугольных импульсов, образуемых при нажатии клавиши. Схемотехнически данная схема выглядит так, как показано на рис. 2, где К1 – пин микроконтроллера привязанный к определенной клавише. В разомкнутом состоянии на пин К1 приходит логическая единица – клавиша не нажата, при нажатии клавиши на пине К1 образуется логический ноль.

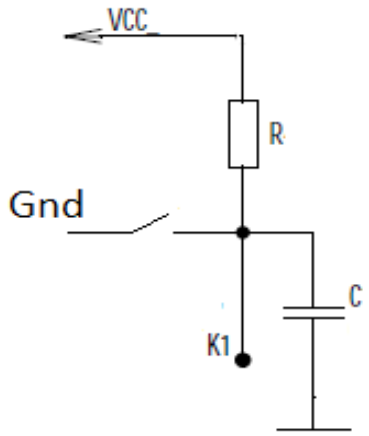


Рис. 2. Схема подключения клавиши к микроконтроллеру

К недостаткам данного метода относится большое количество задействованных пинов микроконтроллера (стандартная клавиатура Windows содержит 104 клавиши), что сильно ограничивает модельный ряд доступных для данной задачи контроллеров. Также ограничивается многозадачность микроконтроллера, при таком подходе контроллер выполняет только задачу обработки матрицы и последующее транслирование скан-кодов в канал связи.

Если клавиатура не является встроенной в аппаратуру, т.е. если клавиатура находится вне защитного контура основного прибора, то появляется необходимость в защите канала связи между клавиатурой и основным прибором. При канале связи, использующего для передачи информации, электрический ток, образуется электромагнитное поле, содержащее информативный сигнал. Для устранения данного канала утечки информации применяется волоконно-оптический кабель (ВОЛС). Применение оптоволокна для канала связи полностью устраняет появление электромагнитного поля.

Список литературы

1. Хорев А. А. Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации. М. : Гостехкомиссия РФ, 1998. 320 с.

2. Виброакустические каналы утечки информации. URL: http://ru.bmstu.wiki/Виброакустические_каналы_утечки_информации

3. Частотный анализ. URL: https://ru.wikipedia.org/wiki/Частотный_анализ

4. Ратников К. А., Персиков Е. А. Анализ экранирования электромагнитного поля в аппаратуре специального назначения сплошными экранами // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. Пенза : Изд-во ПГУ, 2021. С. 99–103.

Для цитирования: Ратников К. А. Особенности разработки защищенной клавиатуры, применяемой в аппаратуре специального назначения // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 77–82.

УДК 004.056

НЕЙРОСЕТЕВАЯ БИОМЕТРИЯ: ПОДТВЕРЖДЕНИЕ ГИПОТЕЗЫ ОБРАТНЫХ ШКАЛ ДЛЯ МЕТРИКИ КОРРЕЛЯЦИОННОЙ СЦЕПЛЕННОСТИ И МЕТРИКИ РАССТОЯНИЙ ХЭММИНГА ПРИ ИХ ПРИМЕНЕНИИ К КЛЮЧАМ-ОТКЛИКАМ НА ПРИМЕРЫ ОДНОГО ОБРАЗА «ЧУЖОЙ»

К. А. Горбунов[1], В. В. Никитин[2]

[1]Пензенский государственный университет, г. Пенза

[2]Радиозавод, г. Пенза

Аннотация. Рассматриваются обратные шкалы для корреляционной сцепленности и расстояний Хэмминга при их применении к ключам-откликам на примеры образа «Чужой» в среде моделирования «БиоНейроАвтограф».

Ключевые слова: нейросетевая биометрия, гипотеза обратных шкал, корреляционная сцепленность, расстояния Хэмминга, ключи-отклики

NEURAL NETWORK BIOMETRICS: CONFIRMATION OF THE HYPOTHESIS OF INVERSE SCALES FOR THE CORRELATION COUPLING METRIC AND THE HAMMING DISTANCE METRIC WHEN APPLIED TO KEY RESPONSES TO EXAMPLES OF A SINGLE "ALIEN" IMAGE

K. A. Gorbunov[1], V. V. Nikitin[2]

[1]Penza State University, Penza

[2]Radiozavod, Penza

Abstract. Inverse scales for correlation coupling and Hamming distances are considered when they are applied to key responses to examples of the "Alien" image in the "BioNeiroAutograph" modeling environment.

Keywords: neural network biometrics, hypothesis of inverse scales, correlation coupling, Hamming distances, key responses

При тестировании стойкости к атакам подбора рукописных образов среды моделирования «БиоНейроАвтограф» [1, 2] могут быть выбраны разные образы «Чужой». Например, если мы выбираем при тестировании 21 пример рукописного образа «*Хопер*», то по-

лучаем математическое ожидание коэффициентов корреляционной сцепленности E(r) ≈ 0,43, что отображено в левой части рис. 1.

Если выполнять тестирование на примерах рукописного образа «Сура», то порождаемые этим образом ключи (длина ключа 256 бит) имеют более высокий уровень корреляционной сцепленности E(r) ≈ 0,59. Это означает, что примеры образа «*Сура*» ближе к образу «Свой», так как образ «Свой» обладает предельно высокой корреляционной сцепленностью с единичным математическим ожиданием E(r) ≈ 1,0. Эта ситуация отображена на рис. 1.

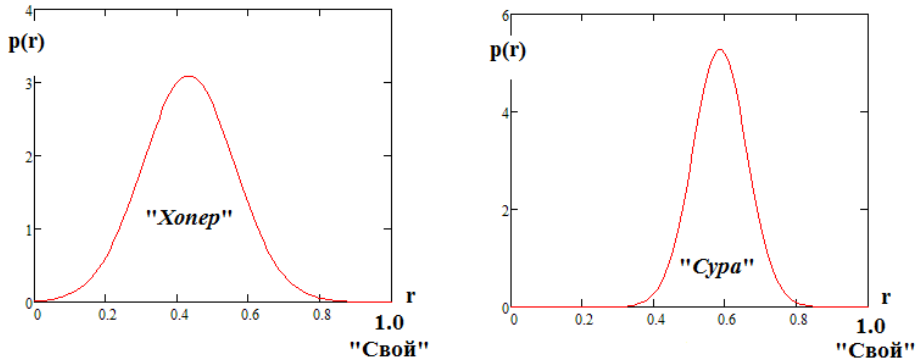


Рис. 1. Распределение расстояний корреляционной сцепленности между ключами от примеров образа «*Хопер*» (предельное значение корреляции «Свой» в правой части рисунка r = 1,0)

При вычислениях данных рис. 1 корреляционная метрика вычислялась как функция corr(xj, xi), где i, j – номера примеров, порождающих коды отклики тестируемых образов.

Совершенно иная ситуация возникает, если мы будем рассматривать кодовые ключи отклики на тестовые образы в пространстве расстояний Хэмминга (в пространстве автосверток Хэмминга [3]). Эта ситуация отображена на рис. 2.

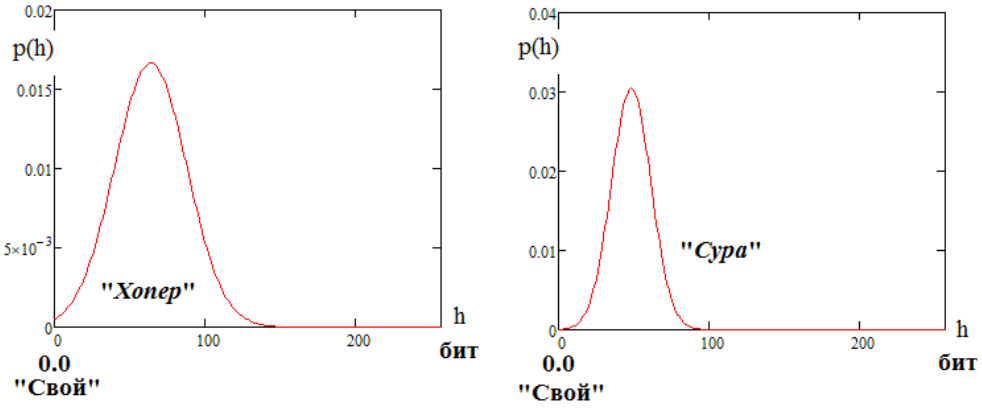


Рис. 2. Распределение расстояний Хемминга между ключами от примеров образа Хопер (предельное значение «Свой» в левой части рисунка h = 0,0)

Из рис. 2 видно, что две рассматриваемые метрики обратны. Математическое ожидание хэмминговых автосверток составляет E(h) ≈ 86 бит для примеров образа «*Хопер*». Для 21 примера образа «*Сура*» математическое ожидание сверток Хэмминга существенно меньше E(h) ≈ 86 бит. В целом метрика корреляционной сцепленности (рис. 1) и метрика автосверток Хэмминга ведут себя похоже, однако образ «Свой» E(r) ≈ 1,0 и E(h) ≈ 0,0 находятся с разных сторон по отношению к математическим ожиданиям двух разных метрик. Фактически рассматриваемые метрики обладают обратными шкалами, то есть являются слабо независимыми.

Список литературы

1. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip

2. Иванов А. И. Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях : учеб. пособие. Пенза, 2013. 30 с. URL: http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf

3. Иванов А. И., Иванов А. П., Ратников К. А. Статистико-нейросетевой анализ биометрических образов в пространствах сверток и автосверток Хэмминга : препринт. Пенза : Изд-во ПГУ, 2021. 56 с.

Для цитирования: Горбунов К. А., Никитин В. В. Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний Хэмминга при их применении к ключам-откликам на примеры одного образа «Чужой» // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 83–85.

УДК 004.056

ВОЗДЕЙСТВИЯ, ПРИВОДЯЩИЕ К НАРУШЕНИЮ ДОСТУПНОСТИ ПЕРЕДАВАЕМЫХ ДАННЫХ В ВОЛОКОННО-ОПТИЧЕСКИХ КАНАЛАХ СВЯЗИ

Р. В. Ерёменко, Н. Ю. Птицын

Пензенский государственный университет, г. Пенза

Аннотация. Целью работы является рассмотрение воздействий, приводящих к нарушению доступности передаваемых данных в волоконно-оптических каналах связи. Проанализированы воздействия, приводящие к нарушению доступности передаваемых данных в волоконно-оптических каналах связи.

Ключевые слова: нарушение доступности, данные, волоконно-оптические каналы связи

IMPACTS LEADING TO A VIOLATION OF THE AVAILABILITY OF TRANSMITTED DATA IN FIBER-OPTIC COMMUNICATION CHANNELS

R. V. Eremenko, N. Yu. Ptitsyn

Penza State University, Penza

Abstract. The aim of the work is to consider the impact that leads to a violation of the availability of transmitted data in fiber-optic communication channels. The impacts that lead to a violation of the availability of transmitted data in fiber-optic communication channels are analyzed.

Keywords: violation of the availability, data, fiber-optic communication channels

Волоконно-оптическая связь – способ передачи информации, использующий в качестве носителя информационного сигнала электромагнитное излучение оптического (ближнего инфракрасного) диапазона, а в качестве направляющих систем – волоконно-оптические кабели. Благодаря высокой несущей частоте и широким возможностям мультиплексирования пропускная способность волоконно-оптических линий многократно превышает пропускную способность всех других систем связи и может измеряться терабитами

в секунду. Малое затухание света в оптическом волокне позволяет применять волоконно-оптическую связь на значительных расстояниях без использования усилителей. Волоконно-оптическая связь свободна от электромагнитных помех и труднодоступна для несанкционированного использования: незаметно перехватить сигнал, передаваемый по оптическому кабелю, технически крайне сложно [1].

В основе волоконно-оптической связи лежит явление полного внутреннего отражения электромагнитных волн на границе раздела диэлектриков с разными показателями преломления. Оптическое волокно состоит из двух элементов – сердцевины, являющейся непосредственным световодом, и оболочки. Показатель преломления сердцевины несколько больше показателя преломления оболочки, благодаря чему луч света, испытывая многократные переотражения на границе сердцевина-оболочка, распространяется в сердцевине, не покидая её.

В работе, посвященной защите информации в ВОЛС [2], авторы рассматривают возможные потери в ОВ и различные способы реализации несанкционированных воздействий в ВОЛС.

Оптический сигнал, передаваемый по волоконно-оптической линии связи (ВОЛС), распространяется согласно закону полного внутреннего отражения, поэтому считается, что ВОЛС имеет повышенную защищенность. В то же время оптическое волокно (ОВ) обладает затуханием, вызванным целым рядом причин: френелевское отражение, собственное поглощение, поглощение на ионах ОН-, излучение на микро- и макроизгибах и др. Используя эти явления в своих целях, злоумышленник может осуществлять различные виды несанкционированных воздействий на передаваемую информацию.

За счет макроизгиба можно добиться преобразования направляемых мод в вытекающие, что приведет к выводу части мощности оптического волокна за пределы оболочки. Тем самым злоумышленник получит несанкционированный доступ к сигналу. Кроме того, есть опасность использования вытекающих мод в местах стыковки О В между собой или с оптическим развет-вителем. Это обусловлено тем, что для ВОЛС такой отбор мощности является незаметным из-за «естественной» утечки мод. Другие способы, описанные в статье, предусматривают внедрение фотодетектирующих элементов в оболочку ОВ или использование механических и термических способов воздействия на ОВ для создания микроизгиба, который и приведет к ответвлению части мощности из ОВ.

Виды несанкционированных воздействий

Все несанкционированные воздействия злоумышленника можно представить шестью областями, каждую из которых отличают следующие цели:

- анализ трафика;
- подслушивание;
- умышленная задержка информации;
- отказ в обслуживании;
- изменение характеристик качества обслуживания QoS;
- спуфинг, то есть передача злоумышленником информации в сеть от имени другого лица.

Еще в одной работе [3] список рассматриваемых видов несанкционированных воздействий был сокращен путем объединения между собой некоторых из них:

- несанкционированные воздействия двух видов «анализ трафика» и «подслушивание» имеют схожие характеристики и могут рассматриваться как один вид;
- оптические сети из-за отсутствия в них оптической памяти защищены от несанкционированного воздействия «задержка информации», следовательно, этот вид не рассматривается;
- проблема спуфинга может быть решена с помощью использования методов криптографии, что уже решено в некоторых реализациях технологии PON, и не рассматривается;
- «изменение параметров QoS» и «отказ в обслуживании» в некотором приближении могут рассматриваться как один вид несанкционированного воздействия, объединенного общим названием «нарушение сервиса».

Таким образом, количество возможных несанкционированных воздействий в сети PON сократилось до двух: подслушивание (анализ трафика) и «нарушение сервиса».

Список несанкционированных воздействий можно расширить, но они будут относиться к сетевым протоколам, системам управления, тогда как нас интересуют несанкционированные воздействия, связанные с инфраструктурой сети PON.

«Подслушивание»

«Подслушивание» может быть реализовано злоумышленником путем ответвления части оптической мощности передаваемого оптического сигнала через О В или оптический разветвитель. Данный вид воздействия можно применить двумя способами: разрывным

или безразрывным. В случае разрывного способа производится обрыв оптического волокна и подсоединение оптического ответвителя. Несовершенство этого способа заключается в большом вносимом затухании и неизбежном прерывании связи на время подключения ответвителя, что может быть легко обнаружено. В случае безразрывного способа часть оптической мощности можно получить в месте изгиба оптического волокна.

«Нарушение услуги»

Второй вид несанкционированного воздействия – «нарушение услуги» может быть реализован через оптическое волокно или приемопередающее оборудование на стороне абонента либо через оптический разветвитель. В данном случае злоумышленник осуществляет ввод в оптическое волокно сигнала, в результате чего происходит ухудшение характеристик услуги или ее нарушение. Технические средства подключения к оптической среде бывают различными: злоумышленник может использовать мощный источник лазерного излучения и меньший радиус изгиба оптического волокна, что позволит оказывать воздействие на полезный сигнал не за счет сильного изменения его мощности, а за счет влияния сигнала злоумышленника на полезный сигнал [4].

На основе выше сказанного можно сделать вывод, что ошибки в сети, ухудшение показателей передачи могут быть вызваны естественными процессами (старение компонентов оптической сети), а также несанкционированными воздействиями на сеть со стороны злоумышленника. В последнее время задача защиты и обнаружения несанкционированных воздействий становится приоритетной. Каждый из рассмотренных выше методов не позволяет обнаружить все виды несанкционированных воздействий и с высокой достоверностью отличить факт несанкционированного воздействия от ошибок, возникающих во время эксплуатации ВОЛС, что приводит к невозможности предоставления высоконадежной и высокозащищенной системы связи.

На магистральных оптических сетях могут применяться дорогостоящие решения защиты информации, обеспечивающие надежную и безопасную передачу данных. Но применение на сетях PON тех же самых решений свело бы на нет все преимущества данной технологии, которые заключаются в предоставлении широкому кругу потребителей широкополосных услуг [5].

Список литературы

1. Kapron F. P., Keck D. B., Maurer R. D. Radiation losses in glass optical waveguides // Appl. Phys. Lett. 1970. № 17. P. 423.

2. Манько А., Каток В., Задорожний М. Защита информации на волоконно-оптических линиях связи от несанкционированного доступа. URL: http://bezpeka.com/ru/lib/spec/

3. Medard M., Marquis D., Chinn S. R. Attack detection methods for all-optical networks // Network and Distributed System Security Symposium, sponsored by the Internet Society, 1998, session 3, paper 1.

4. WDM Networks: Past Lessons and Path Ahead. Kluwer Academic Publishers, 2004.

5. URL: http://lib.tssonline.ru/articles2/in-ch-sec/vopr_inf_bezopasn_setey_pon

Для цитирования: Ерёменко Р. В., Птицын Н. Ю. Воздействия, приводящие к нарушению доступности передаваемых данных в волоконно-оптических каналах связи // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 86–90.

УДК 004.056

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ ПЕРЕДАВАЕМЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛОВ TCP/IP

Р. В. Ерёменко

Пензенский государственный университет, г. Пенза

Аннотация. Целью работы является рассмотрение проблемы обеспечения доступности передаваемых данных при использовании протоколов TCP/IP. Приведено описание и анализ серии протоколов TCP/IP, предназначенных для создания программного обеспечения, необходимых для взаимодействия по по сети Интернет.

Ключевые слова: обеспечение доступности, протоколы TCP/IP, программное обеспечение

THE PROMLEM OF ENSURING THE AVAILABILITY OF TRANSMITTED DATA WHEN USING THE TCP/IP PROTOCOLS

R. V. Eremenko

Penza State University, Penza

Abstract. The purpose of the work is to consider the problem of ensuring the availability of transmitted data when using the TCP/IP protocols. The description and analysis of a series of TCP/IP protocols designed to create software required for interaction over the Internet is given.

Keywords: ensuring the availability, TCP/IP protocols, software

TCP/IP – сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается правилом (протоколом передачи). Наборы правил, решающих задачу по передаче данных, составляют стек протоколов передачи данных, на которых базируется Интернет. Набор интернет-протоколов – это концептуальная модель и набор коммуникационных протоколов, используемых в Интернете и подобных компью-

терных сетях. Он широко известен как TCP/IP, поскольку базовые протоколы в пакете – это протокол управления передачей (TCP) и интернет-протокол (IP). Его иногда называют моделью Министерства обороны (MO), поскольку разработка сетевого метода финансировалась Министерством обороны Соединенных Штатов через DARPA.

Этот набор обеспечивает сквозную передачу данных, определяющую, как данные должны пакетироваться, обрабатываться, передаваться, маршрутизироваться и приниматься. Эта функциональность организована в четыре слоя абстракции, которые классифицируют все связанные протоколы в соответствии с объемом задействованных сетей. От самого низкого до самого высокого уровня – это уровень связи, содержащий методы связи для данных, которые остаются в пределах одного сегмента сети; интернет-уровень, обеспечивающий межсетевое взаимодействие между независимыми сетями; транспортный уровень, обрабатывающий связь между хостами; и прикладной уровень, который обеспечивает обмен данными между процессами для приложений.[1]

Как указанно в источнике[2], серия протоколов TCP/IP – яркий пример открытой системы в том смысле, что, в отличие от протоколов, используемых в коммуникационных системах разных поставщиков, все спецификации этого стека протоколов и многие из его реализаций общедоступны. Это позволяет любому разработчику создавать свое программное обеспечение, необходимое для взаимодействия по Internet. TCP/IP привлекает своей масштабируемостью, предоставляя одинаковые возможности глобальным и локальным сетям.

Семейство протоколов TCP/IP позволяет построить универсальную сеть, реализующую принципы, которые рассмотрены в предыдущем разделе, и включает в себя 4 уровня стека протоколов

- Прикладной: Telnet, FTP, e-mail и тд.
- Транспортный: TCP,UDP
- Сетевой: (вспомогательные протоколы, вроде ICMP и IGMP, работают поверх IP, но тоже относятся к сетевому уровню; протокол ARP является самостоятельным вспомогательным протоколом, работающим поверх канального уровня)
- Сетевой интерфейс: драйвер устройства и сетевая платформа

InternetProtocol (IP) – основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения. Он используется

обоими протоколами транспортного уровня. IP определяет базовую единицу передачи данных в internet, IP-дейтаграмму, указывая точный формат всей информации, проходящей по сети TCP/IP. Программное обеспечение IP выполняет функции маршрутизации, выбирая путь данных по паутине физических сетей. Для определения маршрута поддерживаются специальные таблицы; выбор осуществляется на основе адреса сети, к которой подключен компьютер-адресат. Протокол IP определяет маршрут отдельно для каждого пакета данных, не гарантируя надежной доставки в нужном порядке. Он задает непосредственное отображение данных на нижележащий физический уровень передачи и реализует тем самым высокоэффективную доставку пакетов.

Изучив материал из источника[3], можно сделать вывод, что одним из недостатков протокола TCP/IP является риск потери сообщения из-за возможности утери одного из его пакетов

Рассмотри более подробно 3 уровень стека протоколов (Сетевой).

Кроме IP, на сетевом уровне используются также протоколы ICMP и IGMP, которые находятся в сетевом уровне стека протоколов. (Протокол ICMP описан в RFC 792 [4] от 1981 года JonPostel (с дополнениями в RFC 950)[5].) ICMP является стандартом Интернета (входит в стандарт STD 5 вместе с IP). Хотя формально протокол использует IP (ICMP-пакеты инкапсулируются в IP пакеты), он является неотъемлемой частью IP и обязателен при реализации стека TCP/IP.

Из источника [6] известно, что в основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции (services).

ICMP-сообщение строится из IP-пакетов, сгенерировавших ICMP-ответ. Протокол IP инкапсулирует соответствующее ICMP-сообщение с новым заголовком IP (чтобы отправить ICMP-сообщение обратно отправителю) и передает полученные пакеты дальше.

То есть передача данных напрямую зависит от ICMP-пакета. В случае потери этого пакета генерация нового не произойдет и сообщение или данные будут утеряны. (Правила генерации ICMP-пакетов [6]).

На основе выше сказанного можно сделать вывод, что открытость масштабируемость, универсальность и простота использования – неоспоримые преимущества TCP/IP, но у этого семейства протоколов есть и недостатки. Столь привлекательная простота доступа оборачивается для Internet серьезнейшей проблемой защиты информации, которая приобретает особую остроту сейчас, когда мировая Сеть все активнее используется для электронной коммерции. Неупорядоченность передачи пакетов и невозможность отследить маршрут их продвижения также представляют собой важные проблемы, поскольку препятствуют реализации таких необходимых в современных коммуникациях возможностей, как передача мультимедийных данных в реальном времени. Наконец, как уже упоминалось, предоставляемый нынешней версией протокола IP объем адресного пространства, особенно в связи с его неэффективным использованием, уже с большим трудом позволяет удовлетворять потребности гигантской и все более разрастающейся Сети. Методы решения каждой из этих проблем заслуживают подробного обсуждения [1].

Список литературы

1. Модели OSI и TCP/IP. База знаний osLogic.ru. URL: https://www.oslogic.ru/knowledge/245/modeli-osi-i-tcp-ip/
2. URL: https://www.osp.ru/nets/1997/02/142173
3. URL: https://www.seonews.ru/glossary/tcpip/
4. URL: https://datatracker.ietf.org/doc/html/rfc792
5. URL: https://datatracker.ietf.org/doc/html/rfc950
6. URL: https://ru.wikipedia.org/wiki/ICMP

Для цитирования: Ерёменко Р. В. Проблема обеспечения доступности передаваемых данных при использовании протоколов TCP/IP // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 91–94.

УДК 004.056.53

ПРИНЦИПЫ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Н. А. Постников

Пензенский научно-исследовательский электротехнический институт, г. Пенза

Аннотация. Рассматривается анализ и синтез принципов безопасной разработки программного обеспечения в соответствии с жизненным циклом безопасной разработки программного обеспечения и требованиями стандарта ГОСТ Р 56939–2016. Актуальность работы заключается в возросшем количестве угроз информационной безопасности, появлении новых требований безопасной разработки регулирующих органов Российской Федерации и использовании методов безопасной разработки программного обеспечения. Основной целью работы является повышение уровня защищенности программного обеспечения.

Ключевые слова: безопасная разработка, программное обеспечение, информационная безопасность

PRINCIPLES OF SECURE SOFTWARE DEVELOPMENT

N. A. Postnikov

Penza Research Electrotechnical Institute, Penza

Abstract. The article is devoted to the analysis and synthesis of the principles of secure software development in accordance with the life cycle of secure software development and the requirements of the GOST R 56939–2016 standard. The relevance of the work lies in the increased number of threats to information security, the emergence of new requirements for the safe development of regulatory bodies of the Russian Federation and the use of methods of secure software development. The main goal of the work is to increase the level of software security.

Keywords: secure software development, information security

Сокращения:

– ПО – Программное обеспечение;
– ИБ – Информационная безопасность;
– ИС – Информационная система;
– ЗИ – Защита информации.

Введение

Ввиду возрастающей сложности ИС актуальными становятся угрозы ИБ, связанные с наличием уязвимостей ПО (уязвимостей

кода), используемых в составе ИС [1]. По данным ресурса cvedetails.com, год за годом отмечается тенденция роста количества уязвимостей ПО [2].

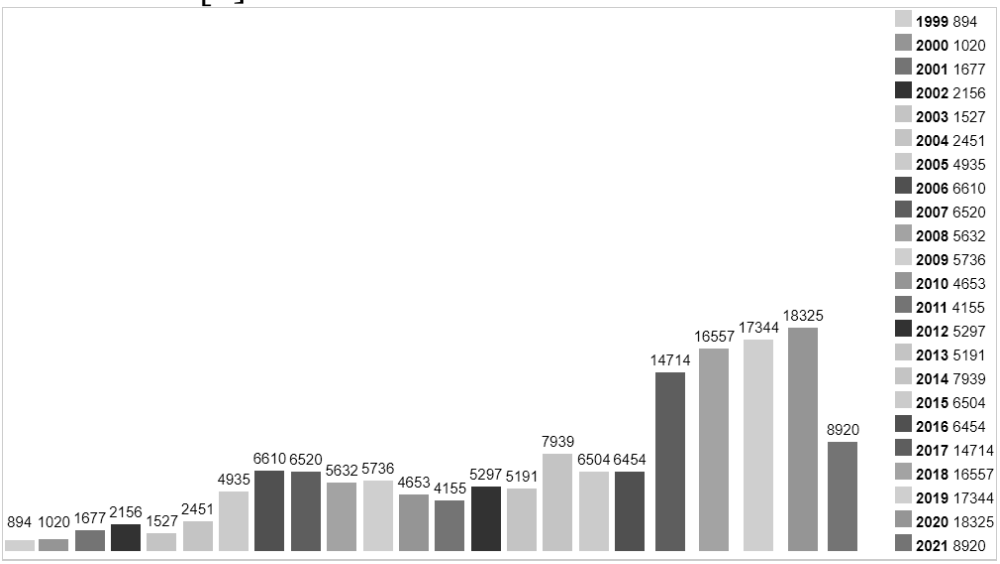


Рис. 1. Количество уязвимостей ПО

Для противодействия угрозам разработчики часто предлагают методы ЗИ, используемые при эксплуатации и сопровождении ПО. В то же время для обеспечения необходимого уровня защищенности требуется интеграция комплекса мер, направленного на предотвращение появления и устранение уязвимостей ПО в процессах всего жизненного цикла ПО, связанных с проектированием, реализацией и тестированием. Однако, реализация подобных мер на поздних этапах жизненного цикла требует бóльших временных, а значит и финансовых трат [9]. Пример графика зависимости стоимости устранения дефекта ПО относительно различных этапов жизненного цикла приведен на рис. 2.

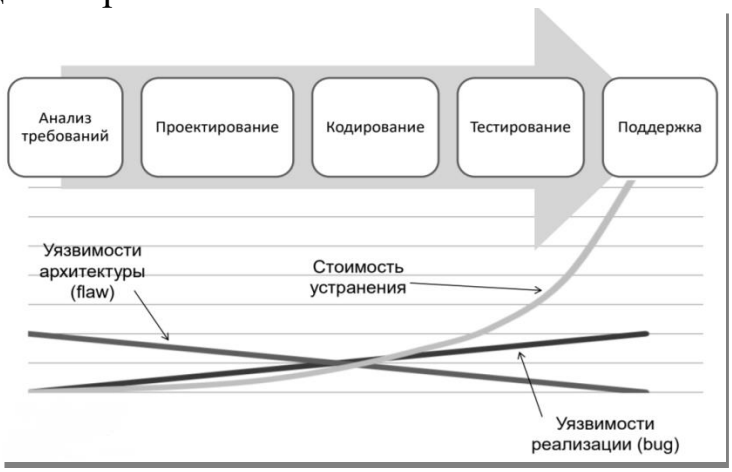


Рис. 2. Зависимость стоимости устранения дефекта ПО относительно различных этапов жизненного цикла

Таким образом, возникает проблема обеспечения требуемого уровня защищённости ПО на всех этапах жизненного цикла ПО при возможности снижения затрат на разработку и поддержку ПО. Устранить проблему может использование принципов безопасной разработки ПО, рассматриваемых в статье.

Жизненный цикл безопасной разработки ПО

Для решения задачи оптимизации затрат на разработку, снижения вероятности появления уязвимостей и систематизации требований по разработке безопасного ПО различные компании представили свои собственные стандарты, методы, методологии и подходы разработки безопасного ПО. Некоторые из них представлены на рис. 3.

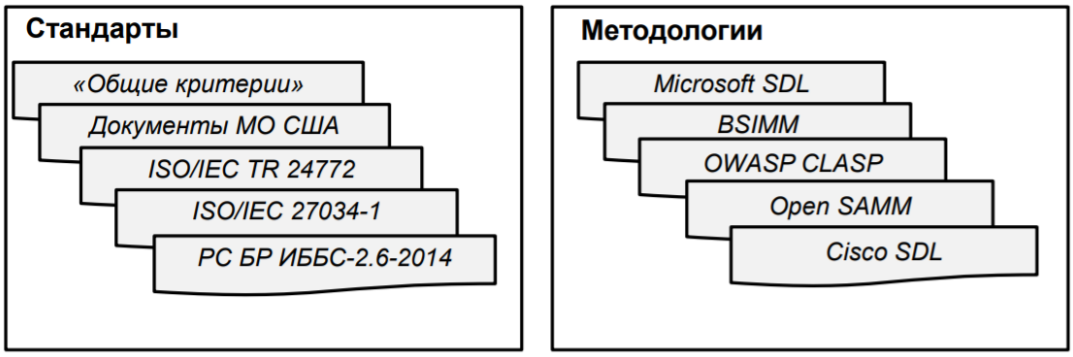


Рис. 3. Стандарты и методологии безопасной разработки ПО

Результатом труда компании Microsoft является Secure Software Development Lifecycle (SSDL) – это процесс разработки безопасного программного обеспечения, созданный и обнародованный компанией еще в январе 2004 года. По словам Microsoft, SSDL позволяет убедиться в необходимом уровне безопасности разрабатываемого ПО и, согласно статистике использования, компании удалось добиться повышения качества продукции и снижения затрат на разработку [3].

SSDL базируется на основе практик, направленных на обучение команды, подготовку отчетности и других непосредственных действий, связанных с анализом безопасности разрабатываемой системы. Эти практики в виде конкретных шагов легко ложатся на привычный спиральный цикл разработки программного обеспечения. Все члены команды, перед тем как непосредственно начать разработку, должны пройти тренинг по безопасности и изучить важные моменты, связанные с текущими трендами в области ИБ. Этапы SSDL представлены на рис. 4.

Рис. 4. Этапы Microsoft Security Development Lifecycle

Внедрение процедур безопасной разработки позволяет сократить совокупную стоимость разработки за счет более раннего обнаружения и устранения уязвимостей. По мнению Национального института стандартов и технологий США, финансовые затраты на устранение уязвимостей на этапе проектирования могут быть более чем в 30 раз ниже затрат на устранение таких же уязвимостей после выпуска программного продукта [4]. Secure Software Development Life Cycle – это классический риск-ориентированный подход. Внедрение SDL не устраняет уязвимости полностью, они снижаются до минимально приемлемого уровня. Применение этих практик в рамках процесса разработки позволяет значительно улучшить результат и снизить затраты на разработку программного обеспечения [10].

Национальный стандарт по разработке безопасного программного обеспечения ГОСТ Р 56939–2016

Использование принципов безопасной разработки носило рекомендательных характер, к тому же имелся ряд предпосылок [5] для создания национального стандарта, обязывающего разработчиков ПО следовать ему.

Среди предпосылок создания можно выделить:

– Создание и поддержка базы данных уязвимостей ПО;

– Проведение анализа уязвимостей в рамках сертификации (ISO/IEC TR 20004);

– Нормативные правовые акты нового поколения;

– Создание ГОСТ Р по уязвимостям ИС и др.

Федеральным агентством по техническому регулированию и метрологии (Росстандартом России) был утвержден национальный стандарт ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (далее –

Стандарт), разработанный ЗАО «НПО «ЭШЕЛОН. Стандарт вступил в силу с 1 июля 2017 года. Он регламентирует содержание и порядок выполнения работ по созданию надежного ПО и формированию среды для оперативного устранения выявленных пользователями ошибок и уязвимостей [8]. В стандарте можно выделить следующие ключевые моменты:

– Стандарт устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного ПО. Детали соответствующих процессов Стандартом не регламентируются;

– Меры по разработке безопасного ПО применяются в течение всего жизненного цикла ПО. Есть связь с процессами, описанными в ИСО/МЭК 12207–2010;

– Стандартом вводится базовый набор мер по разработке безопасного ПО. При невозможности реализации в среде разработки ПО отдельных мер из базового набора, разработчик имеет право реализовать компенсирующие меры.

В стандарте предусмотрено целых 6 видов испытаний ПО: статический анализ и экспертиза кода, функциональное тестирование программы, тестирование на проникновение, динамический анализ кода и фаззинг-тестирование. Учитывается необходимость защиты инфраструктуры среды разработки ПО и обеспечения конфиденциальности информации, получаемой в ходе анализа кода и тестирования ПО. Сравнение статического и динамического анализов приведены табл. 1.

Таблица 1

Сравнение статического и динамического анализов

Статический анализ	Динамический анализ
Не требует выполнения исследуемой программы	Может проводиться без исходных кодов
В простых программах – наиболее эффективный подход	В ряде случаев временные затраты значительно меньше
Требует проведения дополнительных тестов	Возможно исследовать динамически-генерируемый код
Требует больших временных затрат	Позволяет проверять логическую составляющую программы
Требует знания основных интерфейсов/подсистем/модулей исследуемого объекта и принципов их функционирования	Тестовая процедура может быть разработана некорректно, ошибки и уязвимости выявлены не будут

Всего в Стандарте описано 23 меры. По каждой мере четко описаны цели, результат реализации, а также требования к реализации меры.

Базовый набор мер Стандарта выглядит следующим образом:

1. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении анализа требований к программному обеспечению:

1.1. При выполнении анализа требований к ПО разработчик ПО должен определить требования по безопасности, предъявляемые к разрабатываемому ПО.

2. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении проектирования архитектуры программы:

2.1. Моделирование угроз безопасности информации.

2.2. Уточнение проекта архитектуры программы с учетом результатов моделирования угроз безопасности информации.

3. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении конструирования и комплексирования программного обеспечения:

3.1. Использование при разработке ПО идентифицированных инструментальных средств.

3.2. Создание программы на основе уточненного проекта архитектуры программы.

3.3. Создание (выбор) и использование при создании программы порядка оформления исходного кода программы.

3.4. Статический анализ исходного кода программы.

3.5. Экспертиза исходного кода программы.

4. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении квалификационного тестирования программного обеспечения:

4.1. Функциональное тестирование программы.

4.2. Тестирование на проникновение.

4.3. Динамический анализ кода программы.

4.4. Фаззинг-тестирование программы.

5. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении инсталляции программы и поддержки приемки программного обеспечения:

5.1. Обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности в процессе его передачи пользователю.

5.2. Поставка пользователю эксплуатационных документов.

6. Меры по разработке безопасного программного обеспечения, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации:

6.1. Реализация и использование процедуры отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы.

6.2. Систематический поиск уязвимости программы.

7. Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента документацией и конфигурацией программы:

7.1. Реализация и использование процедуры уникальной маркировки каждой версии ПО.

7.2. Использование системы управления конфигурацией ПО.

8. Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента инфраструктурой среды разработки программного обеспечения:

8.1. Защита от несанкционированного доступа к элементам конфигурации.

8.2. Резервное копирование элементов конфигурации.

8.3. Регистрация событий, связанных с фактами изменения элементов конфигурации.

9. Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента людскими ресурсами

9.1. Периодическое обучение сотрудников.

9.2. Периодический анализ программы обучения сотрудников.

В соответствии со Стандартом в наличии должен быть следующий набор документов:

– Политика информационной безопасности в соответствии с ИСО/МЭК 27001.

– Руководство по разработке безопасного ПО.

– Перечень требований по безопасности (могут быть включены в ТЗ).

– Модель угроз безопасности.

– Проект архитектуры программы (логическая структура программы).

– Перечень инструментальных средств разработки ПО.

– Описание проектных решений, обеспечивающих выполнение требований по безопасности;

– Порядок оформления исходного кода программы.

– Регламент и протоколы статического тестирования программы.

– Регламент и протоколы экспертизы исходного кода программы.

– Регламент и протоколы функционального тестирования программы.

– Регламент и протоколы тестирования на проникновение.

– Регламент и протоколы динамического анализа кода программы.

– Регламент и протоколы фаззинг-тестирования программы.

– Эксплуатационная документация.

– Регламент передачи ПО пользователю.

– Регламент отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы.

– Регламент приема и обработки сообщений от пользователей об ошибках ПО и уязвимостях программы.

– Регламент доведения до пользователей информации об уязвимости программы и рекомендаций по их устранению.

– Журнал ошибок и уязвимостей программы.

– Регламент экстренного выпуска обновлений ПО.

– Регламент, протоколы и журналы поиска уязвимостей программы.

– Регламент доведения до пользователей сведений об уязвимостях программы.

– Регламент маркировки версий ПО.

– Регламент управления конфигурацией ПО.

– Регламент защиты инфраструктуры среды разработки ПО.

– Регламент резервного копирования конфигурации ПО.

– Регламент регистрации событий изменений конфигурации ПО.

– Журнал регистрации изменений конфигурации ПО.

– Программа обучения сотрудников в области разработки безопасного ПО.

– Журнал обучения сотрудников в области разработки безопасного ПО.

Таким образом, схематично ГОСТ Р 56939-2016 представлен на рис. 5.

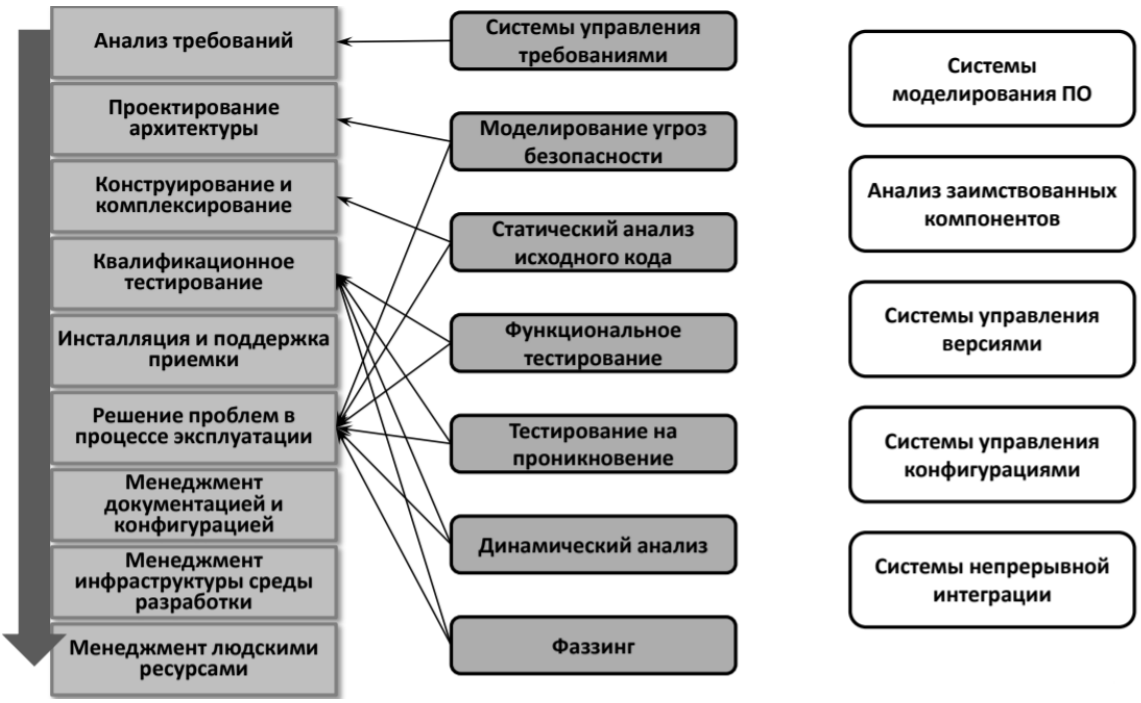


Рис. 5. ГОСТ Р 56939-2016

Достоинствами Стандарта являются:

– набор мер четко сформулирован и научно обоснован коллективом авторов;

– каждая мера детально описана, что облегчает применение Стандарта на практике;

– предусмотрено использование компенсирующих мер в случае обоснованной невозможности применения мер из Стандарта;

– предусмотрен широкий перечень проверок кода и тестирования разрабатываемого программного обеспечения;

– предусмотрена связь с ГОСТ Р ИСО/МЭК 15408 и ИСО/МЭК 12207-2010 [7].

Среди недостатков можно отметить недостаточную гибкость Стандарта и высокий порог вхождения.

По заявлению АО «ИнфоТеКС», после внедрения ГОСТ Р 56939–2016 расширилось число используемых инструментальных средств сборки и анализа ПО, затраты на продуктовые проекты стали более прозрачными, снизилось количество уязвимостей ПО [6].

Вывод. В статье был произведен анализ и синтез принципов безопасной разработки ПО в соответствии с жизненным циклом безопасной разработки и требованиями стандарта ГОСТ Р 56939–2016, выделены достоинства и недостатки стандарта ГОСТ Р 56939–2016.

Список литературы

1. ГОСТ Р 56939–2016. URL: https://docs.cntd.ru/document/1200135525 (дата обращения: 23.03.2021).

2. CVEDetails. URL: https://www.cvedetails.com/browse-by-date.php (дата обращения: 23.03.2021).

3. MSDN. URL: https://docs.microsoft.com/en-us/previous-versions/ms995349(v=msdn.10)?redirectedfrom=MSDN (дата обращения: 23.06.2021).

4. Внедрение процедур безопасной разработки программного обеспечения (Secure SDLC). URL: https://amonitoring.ru/service/secure-development/ (дата обращения: 23.03.2021).

5. Как мы писали ГОСТ по SSDL, и что из этого получилось. URL: https://npo-echelon.ru/common_files/gost/PHD_2016_Barabanov.pdf (дата обращения: 23.03.2021).

6. Отчет АО «ИнфоТеКС». URL: http://new.groteck.ru/images/catalog/46981/40db37ee78e0c6b2ec97593851e6200a.pdsf (дата обращения: 22.06.2021).

7. Разработка безопасного программного обеспечения по ГОСТ Р 56939–2016. URL: https://www.securitylab.ru/blog/personal/crypto-anarchist/312897.php (дата обращения: 23.03.2021).

8. Код безопасности оптимизирует процессы разработки. URL: http://www.mobilecomm.ru/kod-bezopasnosti-optimiziruet-protsessy-razrabotki (дата обращения: 23.04.2021).

9. Барабанов А. В., Марков А. С., Цирлов В. Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5 (13). С. 2–10.

10. Пиков В. А., Басангов М. В., Макрушина Д. А. Комплекс мер по разработке безопасного мобильного банковского приложения по ГОСТ Р 56939–2016 // Цивилизация знаний: российские реалии : тр. XX Междунар. науч. конф. (г. Москва, 19–20 апреля 2019 г.). М. : Российский новый университет, 2019. С. 194–211.

Для цитирования: Постников Н. А. Принципы безопасной разработки программного обеспечения // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 95–104.

УДК 004.056; 004.89; 57.087

О РОЛИ РЕГУЛЯРИЗАЦИИ ВЫЧИСЛЕНИЯ ОТКЛИКОВ КВАДРАТИЧНЫХ ФОРМ НА УСТОЙЧИВОСТЬ БИОМЕТРИКО-НЕЙРОСЕТЕВЫХ РЕШЕНИЙ

Ю. И. Серикова

Пензенский государственный университет, г. Пенза

Аннотация. Устойчивость биометрико-нейросетевых решений может быть многократно увеличена за счет перехода от вычисления общепринятой меры Махаланобиса к специальному подбору одинаково коррелированных данных.

Ключевые слова: регуляризация вычисления, биометрико-нейросетевые решения, мера Махаланобиса

ON THE ROLE OF REGULARIZATION OF CALCULATING THE RESPONSES OF QUADRATIC FORMS TO THE STABILITY OF BIOMETRIC-NEURAL NETWORK SOLUTIONS

Yu. I. Serikova

Penza State University, Penza

Abstract. The stability of biometric-neural network solutions can be increased many times, due to the transition from calculating the generally accepted Mahalonobis measure to a special selection of equally correlated data.

Keywords: regularization of calculating, biometric-neural network solutions, Mahalonobis measure

При выполнении процедур аутентификации личности могут быть использованы искусственные нейронные сети большого размера [1–4], которые предварительно обучаются на биометрических данных личности.

При этом для обучения «глубоких» нейронных сетей [1, 2] требуется, как минимум 100 000 примеров, биометрических образов, размеченных в ручном режиме и много времени на сам процесс обучения.

Для решения задачи аутентификации личности создаются специальные нейронные сети [5], имеющие стандартизованный алгоритм обучения [6] с линейной вычислительной сложностью.

Стандартизованный алгоритм обучения [6] построен на использовании младших одномерных статистических моментов. Используются математические ожидания $E(\nu)$ и стандартные отклонения – $\sigma(\nu)$ биометрических параметров. Как перспектива рассматривается возможность улучшения стандартного алгоритма обучения [7–11] через дополнительное применение коэффициентов корреляции $r(\nu_1, \nu_2)$. При этом основным препятствием является то, что корреляционный функционал двухмерен и накапливает погрешности $\Delta E(\nu_1)$, $\Delta E(\nu_2)$, $\Delta\sigma(\nu_1)$, $\Delta\sigma(\nu_2)$. В конечном итоге на малых выборках коэффициенты корреляции имеют недопустимо большую погрешность.

В нейросетевой биометрии нашла широкое применение мера Махаланобиса [12]. При использовании центрирования и нормирования данных биометрических образов мера Махаланобиса представлена:

$$e^2 = \left(\bar{\nu}\right)^T \cdot \left[r\right]^{=1} \cdot \bar{\nu}. \qquad (1)$$

Основная проблема вычислений данных по (1) является проблема обращения корреляционных матриц. Чем выше размерность корреляционной матрицы, тем хуже их обусловленность.

Для произвольно сформированных корреляционных матриц 4…5 порядков число обусловленности может меняться в пределах от 1 до 200.

Если начать специально подбирать одинаково коррелированные биометрические параметры, то, например, для параметров $r_i \approx 0.0$ число обусловленности будет близко к единице при любой размерности.

Формирование нескольких групп слабо коррелированных параметров является очень эффективным способ регуляризации. Более того, даже в случае не нулевых корреляционных связей $r \neq 0.0$ для симметричных матриц удается однозначно вычислить коэффициент обусловленности:

$$cond\left[r_n\right] = \frac{\max(\lambda_i)}{\min(\lambda_i)} = \frac{\lambda_1}{\lambda_2}, \qquad (2)$$

где λ_i – собственные числа любого типа корреляционной матрицы, только для симметричных корреляционных матриц $\lambda_1 = \max(\lambda_i)$ и $\lambda_2 = \lambda_3 = ,.., = \lambda_n = \min(\lambda_i)$.

При этом число обусловленности симметричных корреляционных матриц всегда меньше чем число обусловленности близких к

ним симметричных матриц с погрешностями вычисления каждого элемента:

$$cond\begin{bmatrix} 1 & r_{1,2} & r_{1,3} \\ r_{2,1} & 1 & r_{2,3} \\ r_{3,1} & r_{3,2} & 1 \end{bmatrix} \geq cond\begin{bmatrix} 1 & E(r) & E(r) \\ E(r) & 1 & E(r) \\ E(r) & E(r) & 1 \end{bmatrix}. \qquad (3).$$

На рис. 1 показаны функции роста минимального значения коэффициента обусловленности в зависимости от показателя равного значения коэффициентов корреляции и размерности матрицы.

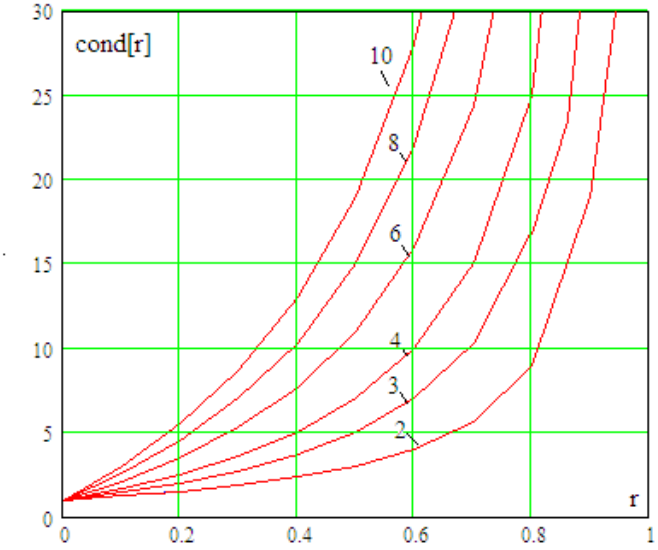


Рис. 1. Функции числа обусловленности симметричных матриц

На рис. 1 даны функции роста числа обусловленности в зависимости от коэффициентов коррелированности симметричных матриц только для малых размерностей n = 2, 3,…, 10.

С ростом размерности функции обусловленности увеличивают свою крутизну, что отражает эффект «проклятия» размерности.

Исходя из соотношения (3) на рис. 1 отображены границы распределений минимально возможных значений коэффициентов обусловленности.

Реальные значения коэффициентов обусловленности всегда выше кривых рис. 1. Для каждой размерности по аналогии с рисунком 1 могут быть построены значения математических ожиданий чисел обусловленности и граница их максимумов. Соотношения этих кривых для выборки в 21 пример показаны на рис. 2.

Из данных рис. 2 видно, что даже относительно небольшие ошибки вычисления коэффициентов корреляции могут приводить

к большим вариациям устойчивости обращения даже трехмерных корреляционных матриц.

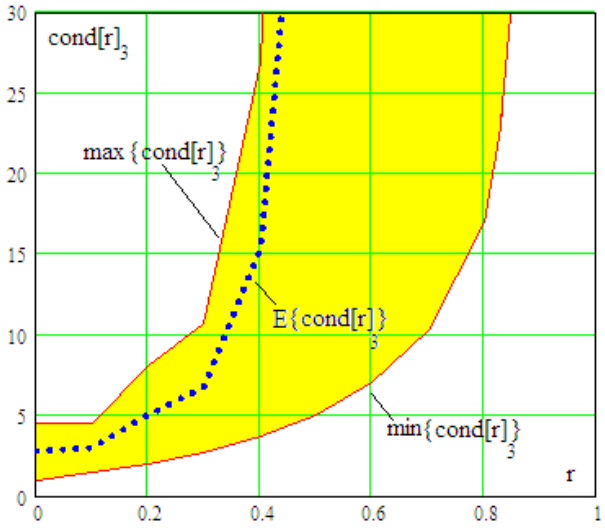


Рис. 2. Разброс чисел обусловленности для почти симметричных корреляционных матриц третьего порядка (более темная заливка) с асимметрией, обусловленной малой выборкой в 21 пример

Замечено, что с ростом размерности обращаемых матриц верхняя и нижняя границы будут расширяться, тем самым увеличивая площадь множества допустимых вариаций чисел обусловленности.

Наоборот, с ростом размеров обучающей выборки, размеры наблюдаемых вариаций числа обусловленности сужаются, приближаясь к правым границам функций изображенных на рисунке2.

Список литературы

1. Гудфеллоу Я., Бенджио И., Курвиль А. Глубокое обучение. М. : ДМК Пресс, 2017. 652 с.

2. Вилзнер Ю. В., Горбацевич В. С., Воронков А. В., Костомаров Н. А. Идентификация лиц в реальном времени с использованием сверточной нейронной сети и хэширующего леса // Компьютерная оптика. 2017. Т. 41, № 2. С. 254–264.

3. Хайкин С. Нейронные сети: полный курс. М. : Вильямс, 2006. 1104 с.

4. Галушкин А. И., Цыпкин Я. З. Нейронные сети: история развития. М. : Радиотехника, 2001. 840 с.

5. Волчихин В. И., Иванов А. И., Фунтиков В. А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации : монография. Пенза : Изд-во ПГУ, 2005. 273 с.

6. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

7. Волчихин В. И., Иванов А. И., Ахметов Б. Б., Серикова Ю. И. Фрактально-корреляционный функционал, используемый при поиске пар слабо зависимых биометрических данных в малых выборках // Известия высших учебных заведений. Поволжский регион. Технические науки. 2016. № 4. С. 25–31.

8. Волчихин В. И., Иванов Н. А., Серикова Ю. И., Банных А. Г. Синтез и тестирование оракула, способного предсказывать асимметричные границы интервала действительного положения математического ожидания малых выборок биометрических данных // Измерение. Мониторинг. Управление. Контроль. 2017. № 2 (20). С. 32–39.

9. Иванов А. И., Ложников П. С., Сулавко А. Е., Серикова Ю. И. Снижение требований к размеру тестовой выборки биометрических данных при переходе к использованию многомерных корреляционных функционалов Байеса // Инфокоммуникационные технологии. 2017. Т. 15, № 2. С. 186–193.

10. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: http://пниэи.рф/activity/science/noc.htm

11. Ахметов Б. Б., Иванов А. И. Многомерные статистики существенно зависимых биометрических данных, порождаемые нейросетевыми эмуляторами квадратичных форм : монография. Алматы, Казахстан : Из-во LEM, 2016. 86 с.

12. Волчихин В. И., Иванов А. И., Малыгина Е. А., Серикова Ю. И. Обучение сетей квадратичных форм на малых выборках биометрических данных с использованием процедуры симметризации корреляционных связей // Измерение. Мониторинг. Управление. Контроль. 2018. № 1 (23). 2018. С. 66–74.

Для цитирования: Серикова Ю. И. О роли регуляризации вычисления откликов квадратичных форм на устойчивость биометрико-нейросетевых решений // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 105–109.

УДК 004.056

СРАВНИТЕЛЬНАЯ ОЦЕНКА СТОЙКОСТИ ЗАЩИТЫ К АТАКАМ ИССЛЕДОВАНИЯ КОНТЕЙНЕРА С БИОМЕТРИЧЕСКИМИ ДАННЫМИ «FUZZY EXTRACTORS» И НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД

А. С. Боровский[1], С. Е. Вятчанин[2], Ю. И. Олейник[3]

[1]Оренбургский государственный университет, г. Оренбург
[2]Пензенский государственный университет, г. Пенза
[3]Радиозавод, г. Пенза

Аннотация. Нейросетевые преобразователи биометрия-код всегда оказываются эффективнее «fuzzy extractors», использующих классические самокорректирующиеся коды. Это связано с тем, что искусственные нейронные сети осуществляют обогащение «плохих» биометрических данных с учетом их реального качества. Именно обучение искусственных нейронных сетей позволяет им учитывать вероятности ошибок первого рода по каждому из биометрических параметров.

Ключевые слова: нейросетевые преобразователи биометрия-код, «fuzzy extractors», биометрические данные

COMPARATIVE ASSESSMENT OF DEFENSE RESISTANCE TO ATTACKS OF THE STUDY OF THE CONTAINER WITH BIOMETRIC DATA "FUZZY EXTRACTORS" AND NEURAL NETWORK CONVERTERS BIOMETRICS-CODE

A. S. Borovsky[1], S. E. Vyatchanin[2], Yu. I. Oleynik[3]

[1]Orenburg State University, Orenburg
[2]Penza State University, Penza
[3]Radiozavod, Penza

Abstract. Neuronet converters of biometric code are always more effective than "fuzzy extractors" that use classic self-correcting codes. This is due to the fact that artificial neural networks enrich "bad" biometric data taking into account their real quality. It is the training of artificial neural networks that allows them to take into account the probability of errors of the first kind on each of the biometric parameters.

Keywords: neuronet converters of biometric code, "fuzzy extractors", biometric data

К настоящему времени у западных экспертов сложилось стойкое мнение, что «fuzzy extractors» имеют более сильную защиту чем нейросетевые контейнеры [1–3].

Известно, что «fuzzy extractors» и нейросетевой преобразователь биометрия-код имеют два входа: биометрический вход, принимающий вектор биометрических параметров, и вход, принимающий ключ, защищающий от наблюдения внутренние данные нейросетевого преобразователя биометрия-код [4, 5]. Это представление удобно тем, что позволяет рассматривать их отдельно, и для каждого технического решения независимо оценивать стойкость со стороны биометрического входа и входа ключа. Основанием для подобного разделения компонентов защиты является то, что атаковать средства биометрической аутентификации возможно с указанных выше сторон.

Средство биометрической аутентификации личности может быть атакована со стороны биометрического входа посредством простого перебора с использованием баз биометрических образов «Чужие» достаточных размеров [6, 7]. Применяя биометрические образы из таких баз, можно попытаться найти коллизию биометрических образов «Свой» и «Чужой», при этом вполне очевидно, что вероятность коллизии образов «Свой» и «Чужой» совпадает с вероятностью ошибок второго рода средства биометрической аутентификации. Обозначим вероятность ошибки второго рода при атаке со стороны биометрического входа как $P_{2Б}$. В качестве оценки стойкости к атакам подбора со стороны биометрического входа может быть использована обратная величина вероятности биометрических ошибок второго рода $\{P_{2Б}\}^{-1}$.

Вторым вариантом наиболее вероятной атаки на средство биометрической аутентификации будет являться атака подбора кода ключа защиты внутренних данных нейросетевого преобразователя биометрия-код. В случае положительного исхода данной атаки злоумышленник сможет получить доступ к данным нейросетевого преобразователя биометрия-код, что позволяет восстановить биометрические параметры образа «Свой» или код ключа доступа.

По аналогии с ошибкой второго рода биометрической аутентификации введем показатель вероятности угадывания ключа защиты внутренних данных – $P_{2С}$. Тогда стойкость к атакам подбора криптографической защиты может быть оценена как обратная величина $\{P_{2С}\}^{-1}$.

В итоге получаем систему показателей $\{P_{2Б}\}^{-1}$ и $\{P_{2С}\}^{-1}$, позволяющих сравнивать между собой «fuzzy extractors» и нейросетевые преобразователи биометрия-код.

Если сравнивать эти технологии по эффективности использования биометрической информации (по биометрической защите), то нейросетевые преобразователи всегда оказываются эффективнее [7]. Это связано с тем, что искусственные нейронные сети осуществляют обогащение «плохих» биометрических данных с учетом их реального качества. Именно обучение искусственных нейронных сетей позволяет им учитывать вероятности ошибок первого рода по каждому из биометрических параметров [6].

В этом отношении «fuzzy extractors», использующие классические самокорректирующиеся коды, всегда будут уступать нейросетевым преобразователям биометрия-код [8–11]. Все классические самокорректирующиеся коды строятся в рамках гипотезы равного качества биометрических данных, которая работает некорректно и дает большие ошибки. К сожалению, в биометрии наблюдается значительный разброс показателей качества биометрических параметров [12]. В итоге избыточность нейросетевых обогатителей (отношение числа входов нейронной сети к числу ее выходов) будет всегда меньше, чем избыточность классических кодов с обнаружением и исправлением ошибок [11].

Для сокращения избыточности можно использовать самокорректирующие коды [8–10], безопасно хранящие информацию о синдромах ошибок, в виде внешне хранимых эталонов, сформированных из усеченных хэш-функций. В связи с этим объединение самокорректирующихся неизбыточных кодов с нейросетевыми преобразователями биометрия-код дает гораздо более эффективные технические решения по сравнению с «fuzzy extractors».

Например, в случае с биометрическими параметрами низкого качества, например, для рукописного почерка, с 20 % ошибок (из 256 анализируемых параметров), приходится использовать самокорректирующийся код с 800 % избыточности. Информационная часть самокорректирующегося кода составит 256/9 = 28 бит. Защиты биометрических данных кодом ключа длиной 28 бит будет явно недостаточно. Ухудшение биометрических данных (снижение их числа и их качества) приводят к катастрофическому снижению защиты биометрических данных, расположенных в «нечетких контейнерах» «fuzzy extractors».

Сложившаяся практика парольной защиты сводится к защите пароля с 2^{20} возможными состояниями хэш-функцией MD5 [13] имеющей 2^{128} возможных состояний. Другими словами, применяемая криптографическая защита парольной аутентификации намного сильнее самого пароля. Степенной показатель защиты должен быть примерно в 3–5 раз выше, чем показатель парольной защиты.

Имеет смысл требовать то же самое и при защите биометрии. Степенной показатель (длина ключа) защиты должен быть в 3–5 раз больше, чем соответствующий показатель стойкости биометрической защиты. Нейросетевые преобразователи биометрии в код в сочетании с самокорректирующимися кодами должны быть намного эффективнее, чем «fuzzy extractors» [11, 12]. При этом использование требований «Технической спецификации»[14] позволит надежно защитить от изучения и извлечения данные нейросетевого контейнера.

Список литературы

1. Dodis Y., Reyzin L., Smith A. Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. 2004. April 13. URL: www.cs.bu.edu/~reyzin/fuzzy.html

2. Juels A., Wattenberg M. A fuzzy commitment scheme. In Sixth ACM Conference on Computer and Communications Security. New York : ACM Press, 1999. P. 28–36.

3. Jain A. K., Ross A., Pankanti S. Biometrics: A Tool for Information Security // IEEE transactions on information forensics and security. 2006. Vol. 1, № 2. P. 125–143.

4. Иванов А. И. Нечеткие экстракторы: проблема использования в биометрии и криптографии // Первая миля. 2015. № 1. С. 54–57.

5. Вятчанин С. Е., Малыгин А. Ю., Сериков А. В. Анализ эффективности систем аутентификации с нечеткими экстракторами и преобразователями биометрия-код // Проблемы автоматизации и управления в технических системах : сб. докл. XXXII Междунар. науч.-техн. конф. 2017. Т. 1. С. 104–105.

6. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

7. Язов Ю. К., Волчихин В. И., Иванов А. И. [и др.]. Нейросетевая защита персональных биометрических данных / под ред. Ю. К. Язова. М. : Радиотехника, 2012. 157 с.

8. Блейхут Р. Теория и практика кодов, контролирующих ошибки (Theory and Practice of Error Control Codes). М. : Мир, 1986. 576 с.

9. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М. : Мир, 1976. С. 596.

10. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М. : Техносфера, 2005. 320 с.

11. Иванов А. И., Сомкин С. А., Андреев Д. Ю., Малыгина Е. А. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы // Вестник УрФО. Безопасность в информационной сфере. 2014. № 2 (12). С. 16–23.

12. Язов Ю. К., Волчихин В. И., Иванов А. И. [и др.]. Нейросетевая защита персональных биометрических данных. М. : Радиотехника, 2012. 157 с.

13. Хэш-функция MD5. URL://tools.ietf.org/html/rfc1321

14. Техническая спецификация (проект) «Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов» (026 ТК). М. : РОССТАНДАРТ, 2019.

Для цитирования: Боровский А. С., Вятчанин С. Е., Олейник Ю. И. Сравнительная оценка стойкости защиты к атакам исследования контейнера с биометрическими данными «fuzzy extractors» и нейросетевых преобразователей биометрия-код // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 110–114.

УДК 004.056

ВЫСОКОНАДЕЖНАЯ БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ОТКРЫТЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

С. В. Качалин[1], Ю. И. Олейник[2], В. А. Цимбал[3]

[1]Научно-производственное предприятие «Рубин», г. Пенза

[2]Радиозавод, г. Пенза

[3]филиал Военной академии Ракетных войск стратегического назначения имени Петра Великого, г. Серпухов Московской области

Аннотация. Рассмотрены перспективы использования биометрико-нейросетевой аутентификации личности в сети Интернет.

Ключевые слова: биометрическая аутентификация, инфокоммуникационные сети, аутентификация личности

HIGHLY RELIABLE BIOMETRIC AUTHENTICATION OF USERS OF OPEN INFORMATION AND COMMUNICATION NETWORKS

S. V. Kachalin[1], Yu. I. Oleinik[2], V. A. Tsymbal[3]

[1]Research and Production Enterprise "Rubin", Penza

[2]Radiozavod, Penza

[3]Branch of Military Academy of Strategic Rocket Troops after Peter the Great, Serpukhov, Moscow region

Abstract. The prospects of using biometric-neural network identity authentication on the Internet are considered.

Keywords: biometric authentication, communication networks, identity authentication

В настоящее время интернет стал общемировой сетью передачи и хранения данных. При этом, несмотря на все те преимущества, которые предоставляет интернет, очевидна, прямая угроза информационной безопасности для конфиденциальной информации пользователей (данные учетных записей, кредитных карт, личная информация и т.п.). При этом ничто не мешает злоумышленнику при желании выдавать себя за другого пользователя и проводить операции от его имени [1].

В настоящее время наиболее популярным методом защиты передаваемой по сети Интернет конфиденциальной информации, является применение защищенных сеансов между клиентом и сервером, организованных при помощи протоколов SSL/TLS. Стандарт протокола SSL описан в [2]. Стандарт IETF протокола TLS описан в RFC 2246 [3]; в RFC 4346 [4].

Применяемая в SSL/TLS криптографическая защита пересылаемых пакетов данных и механизмы взаимной аутентификации клиента и сервера позволяют предотвратить пассивный перехват, обнаружить искажение и фальсификацию конфиденциальной информации. В существующих реализациях определено использование следующих криптографических систем на открытом ключе – RSA, Diffie-Hellman, DSA, Fortezza; алгоритмов симметричной криптографии – RC2, RC4, IDEA, DES, AES, Camellia; однонаправленных функции хеширования – MD2, MD4, MD5, SHA [1].

Кроме того, возможно расширение реализаций алгоритмами, соответствующих российским криптографическим стандартам ГОСТ 28147–89, ГОСТ Р 34.10–94 и ГОСТ Р 34.11–94, что делает возможным выполнение модификации протокола с учетом национальных требований к безопасности передаваемой информации [1].

Согласно спецификации протоколов TLS/SSL, аутентификация клиента является необязательной, и может быть проведена сервером с использованием любой информации, хранимой пользователем в тайне: учетной записи пользователя; почтового адреса и пароля; информации данных кредитных карт; ответов на контрольные вопросы; одноразовых паролей.

Требования к высоконадежным средствам биометрической аутентификации определены в ГОСТ Р 52633–2006 [5]. Нейросетевой преобразователь биометрия-код способен обеспечить надежную локальную и дистанционную аутентификацию личности по его уникальным биометрическим данным. Вводимый пользователем личный тайный биометрический образ преобразуется в длинный код аутентификации. Сравнение значения хеш-функции длинного кода аутентификации с ее эталонным значением позволяет выполнить однозначную идентификацию [1].

При этом возможно реализовать два варианта протокола дистанционной биометрической аутентификации личности пользователя [1].

В первом варианте обучаемая сеть и процедуры извлечения из нее длинного кода аутентификации хранятся и исполняются на сер-

вере, а пользователь передает для аутентификации свой личный биометрический образ [6].

Во втором варианте алгоритмы и данные для преобразователя хранятся на сервере, но высылаются пользователю в начале процедуры аутентификации [6]. Преобразование биометрия-код, т.е. выделение длинного кода аутентификации, проводится на стороне «Клиента». После этого вычисляется хеш-функция от кода и ее значение отправляется серверу для завершения процедуры аутентификации.

В связи с тем, что при применении первого варианта организации процедуры биометрической аутентификации может быть обеспечена более простая защита от атак подбора биометрических образов и разработаны надежные механизмы биометрического аудита на стороне сервера, рассмотрим его более подробно.

На первом этапе, в соответствии с процедурами протоколов SSL/TLS, устанавливается соединение между машиной «Клиента» (пользователя) и сервера, согласуются криптографические алгоритмы на открытом ключе, на симметричных ключах, алгоритмы хеширования. Клиент и сервер обмениваются «приветствиями» и ключами. Сервер отправляет клиенту сертификат для подтверждения своей подлинности; клиентом производится аутентификация сервера. После все передаваемые между машиной «Клиента» и сервера пакеты шифруются на симметричном ключе, т.е. дальнейший обмен данными проводится по защищенному каналу.

На втором этапе проводится биометрическая аутентификация Клиента. Клиент вводит личный тайный биометрический образ и имя. Биометрический образ и имя передается по защищенному каналу серверу, который выполняет процедуру аутентификации. На шаге 2 личный биометрический образ «Клиента», с указанным именем, при помощи нейросетевого преобразователя биометрия-код конвертируется в длинный код аутентификации «Клиента». На 3-м шаге выполняется сличение полученного хеш-функции длинного кода с ее эталоном, хранимый сервером в тайне. В случае совпадения кодов, аутентификация считается выполненной успешно, и сервер отправляет «Клиенту» подтверждение успешной аутентификации. Обмен данными продолжается в авторизованном режиме. В случае несовпадения хеш-функции длинного кода аутентификации и ее эталона, аутентификация считается не пройденной и, в зависимости от решения, принимаемого биометрическим аудитором могут рассмотрены следующие варианты: «Клиенту» предлагается

ввести личный образ еще раз; в случае обнаружения атаки, происходит разрыв соединения.

Биометрический аудит является неотъемлемой частью механизма аутентификации «Клиента» и предполагает обнаружение и предотвращение атак сервера через биометрию. Разные типы атак биометрической информации описаны в [1]. Подобные атаки могут быть легко обнаружены и отражены, если сервер оснащен соответствующими средствами защиты и обнаружения атак.

В ГОСТ Р ИСО/МЕК 19784–1 [7] дается спецификация биометрического программного интерфейса (BioAPI), определяющего общую высокоуровневую модель биометрического распознавания, пригодную для любой биометрической технологии. Вопросы связанные с надежным хранением биометрических шаблонов, используемых для верификации и идентификации пользователя в нем не определены. Однако, в связи с существующими реальными внешними и внутренними угрозами компрометации личных шаблонов пользователя, важным становится вопрос их надежного хранения на сервере. Очевидно, что системы, использующие биометрическую аутентификацию пользователя должны поддерживать и механизмы надежного хранения биометрических шаблонов пользователя даже в доверенной среде обработки и хранения информации на сервере.

В этой связи личная биометрия пользователя должна храниться на сервере в нейросетевом контейнере и не может быть извлечена из него злоумышленником [1]. Кроме того, злоумышленник не может установить связь нейросетевого контейнера с конкретным пользователем (должна быть обеспечена анонимность биометрической записи). При смене кода аутентификации полностью меняется содержание нейросетевого контейнера даже для одного и того же биометрического образа [1]. Сильная биометрическая защита в соответствии с идеологией ГОСТ Р 52633–2006 [5] может быть обеспечена только при сохранении в тайне самого биометрического образа и длинного кода аутентификации. Обеспечивать сохранение тайны параметров биометрической аутентификации необходимо не только самому пользователю, но и системе в целом. В этом плане спецификация BioAPI (ГОСТ Р ИСО/МЕК 19784-1) [7] является ущербной.

Использование ГОСТ Р ИСО/МЕК 19784-1 [7]без учета требований ГОСТ Р 52633–2006 [5] допустимо только в слабозащищенных системах полицейского контроля, не предъявляющих особых требований к обеспечению анонимности проверяемого и сохранении в тайне его биометрических данных.

Список литературы

1. Иванов А. И. Нейросетевая биометрия и защита информации : учеб. пособие. Пенза : Изд-во ПГУ, 2019. 141 с.

2. SSL 3.0 specification. URL: http://wp.netscape.com/eng/ssl3/draft 302.txt

3. RFC 2246: "The TLS Protocol Version 1.0". URL: http://tools.ietf. org/html/rfc2246

4. RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1". URL: http://tools.ietf.org/html/rfc4346

5. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. М. : Стандартинформ, 2007. 24 с.

6. Патент RU 2273877. Способ распределения ключей в большой территориально разнесенной системе / Ефимов О. В., Иванов А. И., Фунтиков В. А. ; приоритет 16.08.2004 ; патентообладатель ФГУП «ПНИЭИ» (RU).

7. ГОСТ Р ИСО/МЕК 19784-1. Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Спецификация биометрического программного интерфейса.

Для цитирования: Качалин С. В., Олейник Ю. И., Цимбал В. А. Высоконадежная биометрическая аутентификация пользователей открытых инфокоммуникационных сетей // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 115–119.

УДК 004.056.53

РЕАЛИЗАЦИЯ ВЫСОКОИНТЕРАКТИВНОЙ HONEYPOT-СИСТЕМЫ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

А. С. Дёмочкин, А. П. Иванов

Пензенский государственный университет, г. Пенза

Аннотация. Приводится описание реализации высокоинтерактивной honeypot-системы, в том числе каждого модуля системы. Приводится проверка работоспособности системы на примере проведения атаки «Brute-forceSSH».

Ключевые слова: сетевые атаки, honeypot-система, атака «Brute-forceSSH»

IMPLEMENTATION OF A HIGH INTERACTIVE HONEYPOT SYSTEM FOR DETECTING NETWORK ATTACKS

A. S. Demochkin, A. P. Ivanov

Penza State University, Penza

Abstract. A description of the implementation of a highly interactive honeypot system is given, including each module of the system. The system performance check is given on the example of "Brute-force SSH" attack.

Keywords: honeypot system, network attacks, "Brute-force SSH" attack

По определению, которое было сформулировано Лансом Шпицнером, основателем Honeypot Technology [1], honeypot – это ресурс информационной системы, ценность которого заключается в его несанкционированном или незаконном использовании. Данный вид технологий позволяет обнаруживать атаки, проводимые на систему, собирать информацию о злоумышленнике и методах проведения им атак, а также реагировать на все действия злоумышленника в режиме реального времени.

В [2, 3] было определено, что в настоящее время общедоступные программные реализации высокоинтерактивных honeypot-систем имеют ряд недостатков. Поэтому была разработана собственная высокоинтерактивная honeypot-система, позволяющая обнаруживать в режиме реального времени сетевые атаки, в том числе

на этапе получения доступа в honeypot-систему, то есть когда система может быть скомпрометирована.

Архитектура созданной высокоинтерактивной honeypot-системы представлена на рис. 1.

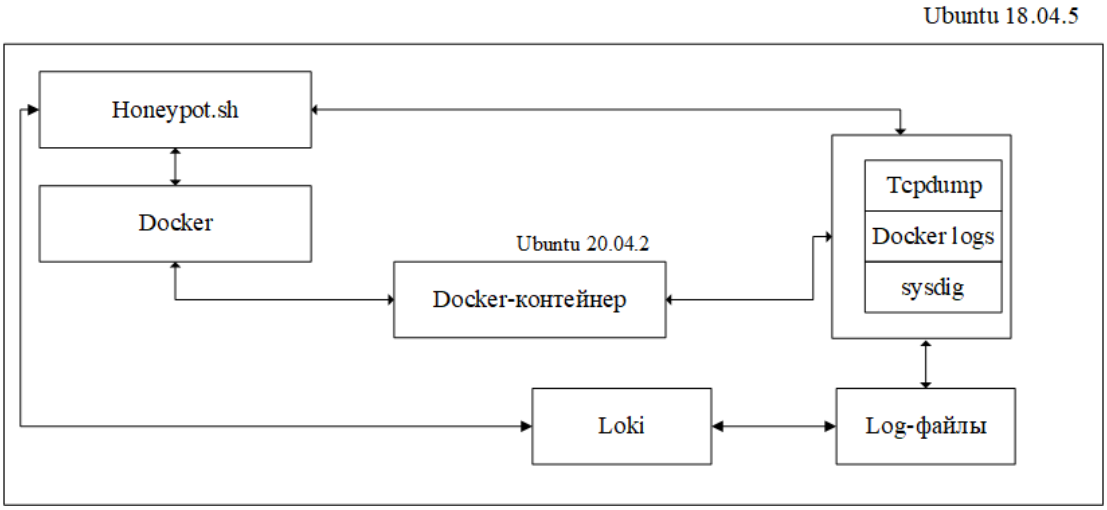


Рис. 1. Архитектура созданной высокоинтерактивной honeypot-системы

Высокоинтерактивная honeypot-система состит из следующих модулей:

– модуль, реализующий механизм «обмана» злоумышленника;

– модуль обнаружения факта атаки на honeypot-систему;

– модуль сбора и визуализации данных о действиях злоумышленника;

– модуль управления honeypot-системой.

В качестве хостовой системы, на которой была развернута реализованная honeypot-система была выбрана ОС Linux–Ubuntu 18.04.5.

Модуль, реализующий механизм «обмана» злоумышленника, представлял из себя docker-контейнер. Функция данного модуля состояла в том, чтобы привлечь внимание злоумышленника для проведения атак. Для этого разработанный docker-контейнер имитировал работу реального хоста под управлением ОС Ubuntu 20.04.2. Также в docker-контейнере были установлены необходимые пакеты, позволяющие собрать информацию о системе, был развернут ssh-сервер, web-сервер «Apache», а также сервер «Apache Tomcat», который имел уязвимую версию пакета 9.0.27 для того, чтобы привлечь внимание злоумышленника. Кроме этого, в docker-контейнер была создана учетная запись пользователя без прав «sudo», но с «простыми» аутентификационными данными. Такое решение

было принято для того, чтобы исследовать действия злоумышленника при вероятности компрометации системы.

Модуль обнаружения факта атаки на высокоинтерактивную honeypot-систему состоял из совокупности утилит tcpdump, dockerlogs и sysdig. Утилита tcpdump позволяла регистрировать весь входящий сетевой трафик, связанный с honeypot-системой (ip-адреса, номера портов, с которых отправлялись пакеты, версии протоколов). Утилита dockerlogs регистрировала события, связанные с сетевыми соединениями к honeypot-системе, а также попытками авторизации в honeypot-систему. Для регистрации событий, связанных с чтением, записью и изменением прав доступа к файлам и директориям, а также для отслеживания команд, которые выполнялись в интерактивном режиме внутри honeypot-системы, использовался инструмент для отслеживания системной активности – sysdig [4].

Для сбора данных о действиях злоумышленника использовались специально-созданные log-файлы, куда сохранялась вся зарегистрированная информация с помощью утилит tcpdump, dockerlogs и sysdig. Данные файлы располагались в специально-созданной директории на хостовой машине /var/log/honeypot. Для централизованного сбора всех данных, которые хранились в log-файлах, использовался стек «Loki» [5]. Данный стек является общедоступным и представлял из себя совокупность средства хранения собранных данных из log-файлов (Loki), элемента обработки данных, отправляющий входящие данные (информация из log-файлов) в Loki (Promtail), а также web-интерфейса для визуализации и анализа собранных данных (Grafana).

Модуль управления honeypot-системой представлял из себя разработанный скрипт на языке bash, который выполнял запуск и остановку всех модулей honeypot-системы. Также данный скрипт выполнял межсетевое экранирование и перенаправление всего сетевого трафика, идущего на хостовую систему, в docker-контейнер, представляющий из себя модуль, реализующий механизм «обмана» злоумышленника. Перенаправление было реализованы с помощью правил «iptables». Кроме этого, разработанный bash-скрипт реализовывал подсистему очистки, которая производилась при завершении работы honeypot-системы.

Для проверки работоспособности разработанной высокоинтерактивной honeypot-системы была проведена имитация атаки «BruteforceSSH». Данная атака состояла из этапа сетевой разведки, этапа перебора учетных данных пользователей для получения доступа

к системе, а также этапа сбора информации о скомпрометированный системе при успешном получении доступа к ней. Для проведения этапа сетевой разведки использовалась утилита «nmap» [6]. Для проведения этапа перебора учетных данных пользователей использовалась утилита «hydra» [7], а также подготовленные словари для перебора логинов пользователей и паролей пользователей.

Результаты работы honeypot-системы представлены на рис. 2–7. Все данные, собранные honeypot-системой, были просмотрены в web-интерфейсе «Grafana».

```
2021-05-22 12:33:18  IP 192.168.110.150.60448 > 192.168.0.129.80: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.48540 > 192.168.0.129.22: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.46136 > 192.168.0.129.5432: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.60432 > 192.168.0.129.80: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.48524 > 192.168.0.129.22: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.59732 > 192.168.0.129.8080: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.55986 > 192.168.0.129.5910: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.57252 > 192.168.0.129.389: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.54474 > 192.168.0.129.53: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.56034 > 192.168.0.129.23: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.60432 > 192.168.0.129.80: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.48524 > 192.168.0.129.22: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.59732 > 192.168.0.129.8080: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.57858 > 192.168.0.129.3306: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.60432 > 192.168.0.129.80: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.48524 > 192.168.0.129.22: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.44662 > 192.168.0.129.21: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.59732 > 192.168.0.129.8080: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.47698 > 192.168.0.129.443: tcp 0
2021-05-22 12:33:18  ARP, Reply 192.168.0.150 is-at 02:42:38:db:1a:6e, length 28
2021-05-22 12:33:18  IP 192.168.110.150.60420 > 192.168.0.129.80: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.60420 > 192.168.0.129.80: tcp 0
2021-05-22 12:33:18  IP 192.168.110.150.47696 > 192.168.0.129.443: tcp 0
```

Рис. 2. Результаты обнаружения сетевой атаки honeypot-системой

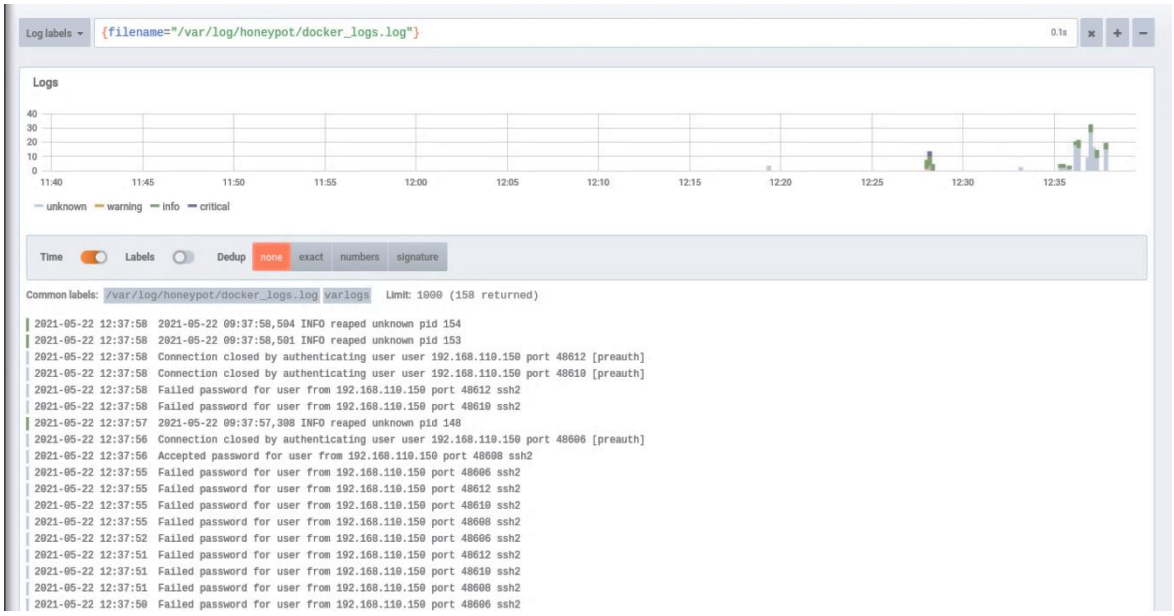


Рис. 3. Результаты обнаружения сетевой атаки honeypot-системой

```
2021-05-22 12:37:03  Disconnected from authenticating user root 192.168.110.150 port 48596 [preauth]
2021-05-22 12:37:03  Received disconnect from 192.168.110.150 port 48596:11: Bye Bye [preauth]
2021-05-22 12:37:02  Failed password for root from 192.168.110.150 port 48596 ssh2
2021-05-22 12:37:02  Failed password for root from 192.168.110.150 port 48594 ssh2
2021-05-22 12:37:02  Failed password for root from 192.168.110.150 port 48592 ssh2
2021-05-22 12:37:02  Failed password for root from 192.168.110.150 port 48590 ssh2
2021-05-22 12:37:00  Failed password for root from 192.168.110.150 port 48596 ssh2
2021-05-22 12:37:00  Failed password for root from 192.168.110.150 port 48594 ssh2
2021-05-22 12:37:00  Failed password for root from 192.168.110.150 port 48592 ssh2
2021-05-22 12:37:00  Failed password for root from 192.168.110.150 port 48590 ssh2
2021-05-22 12:36:57  Failed password for root from 192.168.110.150 port 48596 ssh2
2021-05-22 12:36:57  Failed password for root from 192.168.110.150 port 48594 ssh2
2021-05-22 12:36:57  Failed password for root from 192.168.110.150 port 48592 ssh2
2021-05-22 12:36:57  Failed password for root from 192.168.110.150 port 48590 ssh2
2021-05-22 12:36:56  Failed password for root from 192.168.110.150 port 48592 ssh2
2021-05-22 12:36:56  Failed password for root from 192.168.110.150 port 48590 ssh2
2021-05-22 12:36:56  Failed password for root from 192.168.110.150 port 48596 ssh2
2021-05-22 12:36:56  Failed password for root from 192.168.110.150 port 48594 ssh2
```

Рис. 4. Результаты обнаружения сетевой атаки honeypot-системой

Рис. 5. Результаты обнаружения сетевой атаки honeypot-системой

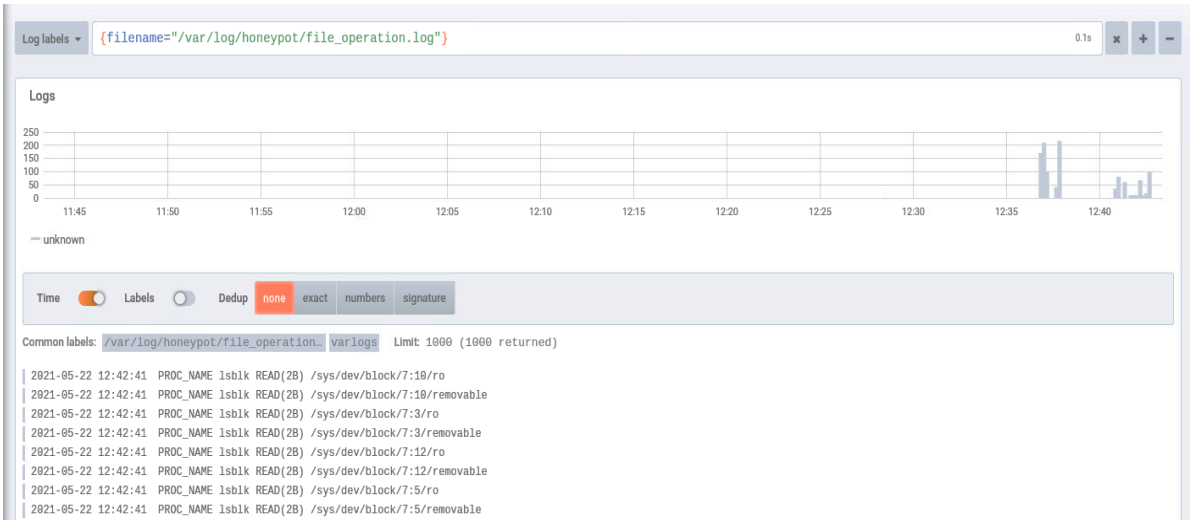


Рис. 6. Результаты обнаружения сетевой атаки honeypot-системой

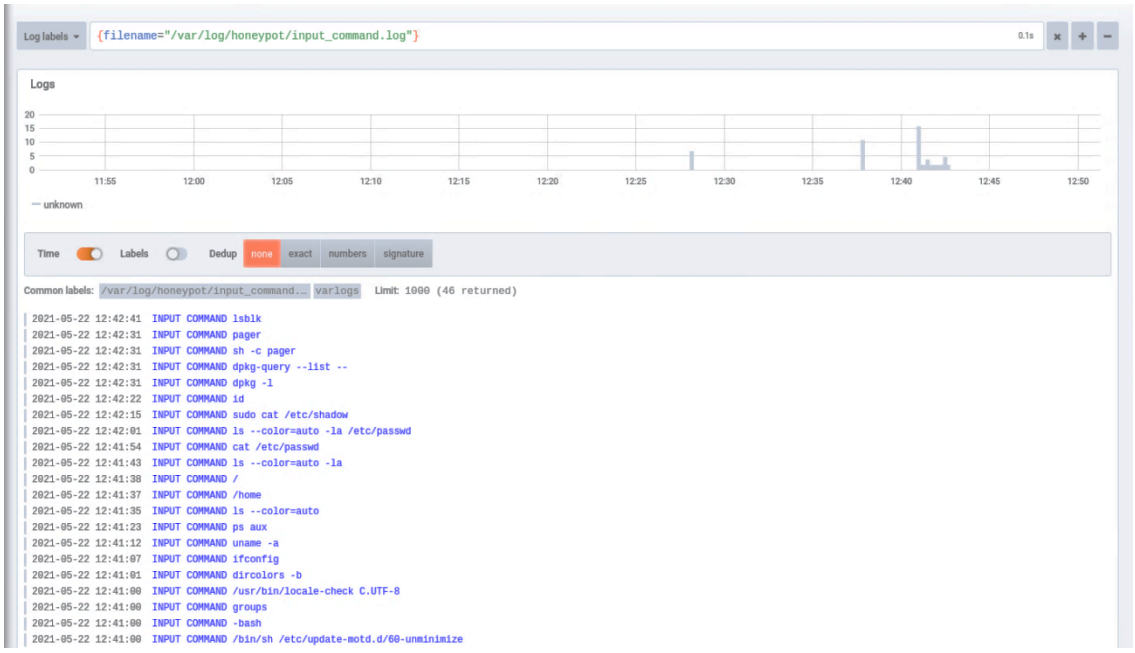


Рис. 7. Результаты обнаружения сетевой атаки honeypot-системой

На рис. 2 можно заметить, что honeypot-система зафиксировала весь входящий трафик, идущий от ip-адреса 192.168.110.150. Кроме этого, система зафиксировала время отправки пакетов, порты, на которые выполнялась отправка пакетов, а также используемый сетевой протокол.

На рис. 3–4 можно увидеть, что honeypot-система зафиксировала многочисленные неуспешные попытки авторизации пользователей с логинами «user» и «root» через ssh-соединение. В тоже время на рис. 5 можно заметить, что пользователь «user» смог авторизоваться в honeypot-системе. Это показывает, что кто-то смог получить доступ во внутрь honeypot-системы. Рисунок 6 демонстрирует часть зарегистрированной информации, связанной с обращением к разным процессам в honeypot-системе, в частности зафиксированы события по работе с процессами в директории «sys/dev/block». Рисунок 7 же наглядно показывает, какие команды были выполнены пользователь «user» в модуле «обмана» злоумышленника (docker-контейнере). Так, выполнялись команды по получению информации о сетевых интерфейсах системы, информации из файлов, содержащих данные о других пользователей системы, информации о установленных пакетах в системе и т.д.

В результате можно сделать вывод, что разработанная высокоинтерактивная honeypot-система смогла зафиксировать атаку, проводимую на нее. Таким образом можно утверждать, что система

работает исправно и с помощью нее в дальнейшем можно обнаруживать и анализировать различные виды сетевых атак.

Список литературы

1. Taxonomy of Honeynet Solutions. URL: https://www.researchgate.net/publication/283939692_Taxonomy_of_Honeynet_Solutions (дата обращения: 28.05.2021).
2. Дёмочкин А. С., Иванов А. П. Анализ программных реализаций Honeypot-технологий с высоким уровнем взаимодействия // Инжиниринг и технологии. 2021. URL: http://engineering-pnzgu.ru/6121 (дата обращения: 28.05.2021).
3. Дёмочкин А. С., Иванов А. П. Классификация honeypot-технологий. Обзор программных реализаций honeypot с низким уровнем взаимодействия // Информационные технологии в науке и образовании. Проблемы и перспективы : сб. ст. по материалам VIII Всерос. межвуз. науч.-прак. конф. / под ред. Л. Р. Фионовой. Пенза : Изд-во ПГУ, 2021. С. 381–386.
4. Sysdig. URL: https://github.com/draios/sysdig (дата обращения: 28.05.2021).
5. Grafana Loki. URL: https://grafana.com/oss/loki/ (дата обращения: 28.05.2021).
6. Nmap: the Network Mapper – Free Security Scanner. URL: https://nmap.org/ (дата обращения: 28.05.2021).
7. THC-hydra. URL: https://github.com/vanhauser-thc/thc-hydra (дата обращения: 28.05.2021).

Для цитирования: Дёмочкин А. С., Иванов А. П. Реализация высокоинтерактивной honeypot-системы для обнаружения сетевых атак // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 120–126.

СВЕДЕНИЯ ОБ АВТОРАХ

Банных Андрей Григорьевич, аспирант кафедры технических средств информационной безопасности, Пензенский государственный университет, г. Пенза.

Безяев Александр Викторович, к.т.н., ведущий научный сотрудник, Пензенский филиал АО «НТЦ "Атлас"», г. Пенза.

Боровский Александр Сергеевич, д.т.н., доцент, заведующий кафедрой управления и информатики в технических системах, Оренбургский государственный университет, г. Оренбург.

Волчихин Владимир Иванович, д.т.н., профессор, президент Пензенского государственного университета, заслуженный деятель науки РФ, г. Пенза.

Вятчанин Сергей Евгеньевич, доцент, начальник кафедры военного учебного центра, Пензенский государственный университет, г. Пенза.

Геращенко Михаил Сергеевич, ассистент кафедры медицинской кибернетики и информатики, Пензенский государственный университет, г. Пенза.

Горбунов Кирилл Андреевич, студент кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Дёмочкин Александр Сергеевич, студент кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Дорошкевич Виктор Вениаминович, ассистент кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Ерёменко Роман Викторович, старший преподаватель военного учебного центра, Пензенский государственный университет, г. Пенза.

Зефиров Сергей Львович, к.т.н., доцент, заведующий кафедрой информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Золотарева Татьяна Александровна, старший преподаватель кафедры информатики, информационных технологий и защиты информации, Липецкий государственный педагогический университет имени П. П. Семенова-Тян-Шанского, г. Липецк.

Иванов Александр Иванович, д.т.н., доцент, научный консультант АО «ПНИЭИ», г. Пенза.

Иванов Алексей Петрович, к.т.н., доцент, заведующий кафедрой технических средств информационной безопасности, Пензенский государственный университет, г. Пенза.

Иванова Надежда Александровна, специалист Российского отделения компании «ABBYY», г. Москва.

Качалин Сергей Викторович, к.т.н., заместитель начальника отдела АО «НПП "Рубин"», г. Пенза.

Князьков Владимир Сергеевич, д.т.н., профессор, главный научный сотрудник Научно-исследовательского института фундаментальных и прикладных исследований, Пензенский государственный университет, г. Пенза.

Куликов Сергей Владимирович, специалист ООО «Лаборатория умных технологий», г. Пенза.

Ложников Павел Сергеевич, д.т.н., доцент, заведующий кафедрой комплексная защита информации, Омский государственный технический университет, г. Омск.

Лукин Виталий Сергеевич, младший научный сотрудник регионального учебно-научного центра «Информационная безопасность», Пензенский государственный университет, г. Пенза.

Малыгина Елена Александровна, к.т.н., докторант кафедры технических средств информационной безопасности, Пензенский государственный университет, г. Пенза.

Маркулева Марина Владимировна, старший преподаватель кафедры медицинской кибернетики и информатики, Пензенский государственный университет, г. Пенза.

Никитин Владислав Валерьевич, инженер АО «Радиозавод», г. Пенза.

Олейник Юрий Иванович, к.т.н., главный специалист НО НТЦ АО «Радиозавод», г. Пенза.

Персиков Егор Андреевич, студент кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Пирогов Алексей Андреевич, студент кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Полковникова Светлана Андреевна, аспирант кафедры вычислительной техники, Пензенский государственный университет, г. Пенза.

Постников Николай Андреевич, инженер АО «ПНИЭИ», г. Пенза.

Птицын Никита Юрьевич, курсант военного учебного центра, Пензенский государственный университет, г. Пенза.

Ратников Кирилл Андреевич, аспирант кафедры технических средств информационной безопасности, Пензенский государственный университет, г. Пенза.

Серикова Юлия Игоревна, аспирант кафедры вычислительной техники, Пензенский государственный университет, г. Пенза.

Сомкин Сергей Александрович, заместитель генерального директора АО «ПНИЭИ», г. Пенза.

Строков Алексей Валерьевич, специалист компании «Организационно-технические решения», г. Москва.

Сулавко Алексей Евгеньевич, к.т.н., доцент кафедры комплексной защиты информации, Сибирский государственный автомобильно-дорожный университет, г. Омск.

Султанов Борис Владимирович, д.т.н., профессор кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Урнев Иван Васильевич, д.т.н., старший научный сотрудник Научно-исследовательского института фундаментальных и прикладных исследований, Пензенский государственный университет, г. Пенза.

Цимбал Владимир Анатольевич, заслуженный деятель науки РФ, д.т.н., профессор кафедры автоматизированных систем управления филиала Военной академии Ракетных войск стратегического назначения имени Петра Великого, г. Серпухов Московской области.

Щербакова Анастасия Юрьевна, старший преподаватель кафедры информационной безопасности систем и технологий, Пензенский государственный университет, г. Пенза.

Юнин Алексей Петрович, ведущий специалист АО «ПНИЭИ», г. Пенза.

СОДЕРЖАНИЕ

АО «Пензенский научно-исследовательский электротехнический институт» (АО «ПНИЭИ»)

В АО»ПНИЭИ» в настоящее время разрабатываются и серийно выпускаются комплексы и технические средства криптографической защиты информации, средства специальной связи, обеспечивающие конфиденциальность, достоверность, целостность информации при передаче ее по различным каналам связи. Активно развиваются такие направления как

– создание средств управления защищенными информационно-телекоммуникационными сетями;

– создание специальных систем передачи данных;

– создание средств электронного документооборота;

– развитие и внедрение биометрико-нейросетевых технологий.

Учеными и специалистами ПНИЭИ создаются и внедряются новые поколения аппаратуры и комплексов технических средств для обработки и защиты мультимедийной информации, передаваемой по разнородным каналам и информационно-телекоммуникационным системам связи, созданным на базе современных международных протоколов.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Комплекс технических средств ПОРТАЛ

КТС ПОРТАЛ предназначен для организации защищенного корпоративного (ведомственного) портала с мультимедийными сервисами, имеющего собственную логическую инфраструктуру управления, не зависящую от зарубежных ресурсов логического управления публичной сетью Интернет, и комплексно реализующего современные технологии безопасности доверенных вычислений на основе отечественной элементной базы.

В основе системных решений лежит разработка собственной облачной криптографически защищенной среды, реализующей идеологию «интернет в интернете», и предоставляющей набор как стандартных, так и узкоспециализированных веб-сервисов.

Комплекс разворачивается на базе существующих ведомственных локальных сетей и не требует установки и настройки программного обеспечения на рабочих станциях. Работа пользователей осуществляется также, как если бы они работали через Интернет, но реальный выход в глобальную сеть пользователям будет недоступен, и наоборот, доступ в ведомственную сеть со стороны открытой сети Интернет также невозможен.

КТС включает в себя серверную составляющую, аппаратные средства криптографической защиты информации, мобильное приложение для доступа с Android-устройств и программное обеспечение взаимосвязанных и объединенных между собой прикладных сервисов.

Пользователь получает доступ к защищенной электронной почте, защищенному мессенджеру мгновенных сообщений с различный устройств (смартфон, планшет, ноутбук и т.д.), организует защищенные аудио и видеоконференции между разнородными техническими средствами, ведет защищенные переговоры с помощью сервиса виртуальной АТС, получает доступ к защищенному облачному хранилищу файлов и защищенному сервису справочной информации. При этом действия пользователя мало отличаются от привычных ему действий при работе в интернете через стандартный браузер.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

ПОРТАЛ-СЕРВЕР

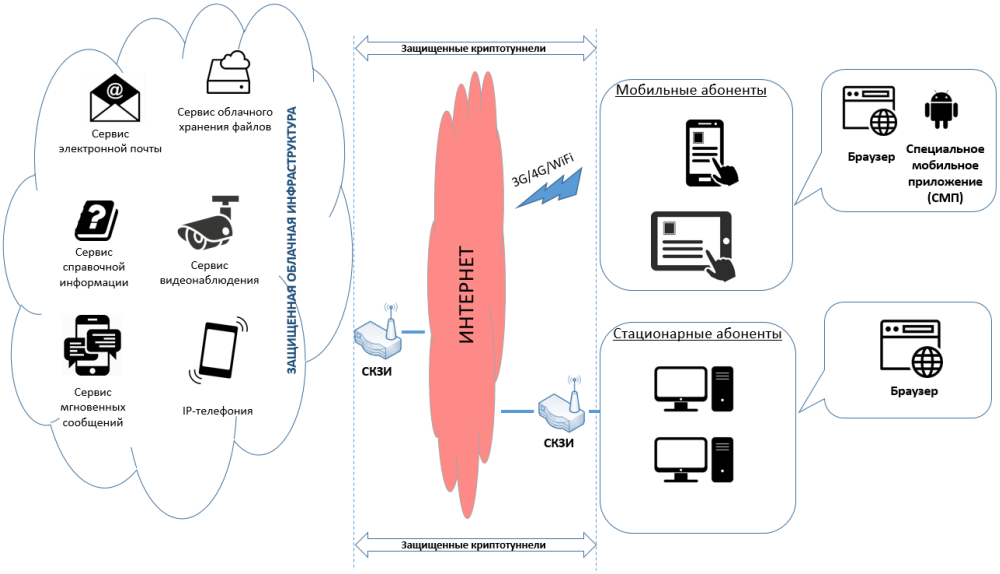
Продукт Портал-сервер представляет собой облачную криптографически замкнутую среду информационного взаимодействия и входит в линейку изделий комплекса "Портал".

Состав системных служб

- DNS-служба
- служба синхронизации времени (NTP)
- сетевая служба
- служба маршрутизации

Состав защищенных прикладных сервисов

- сервис электронной почты
- сервис обмена мгновенными сообщениями
- сервис видеоконференций
- сервис справочной информации (Вики-страницы)
- сервис облачного хранения файлов (Диск)
- видеонаблюдение
- голосовая и ведеосвязь



Логическая организация защищенной облачной системы реализована так как это делается в глобальной сети Интернет – т.е. с собственной внутренней структурой доменных имен для доступа к ресурсам. По аналогии с сетью Интернет, пользователи могут использовать облачные сервисы через привычные для них браузеры без каких-либо дополнительных условностей.

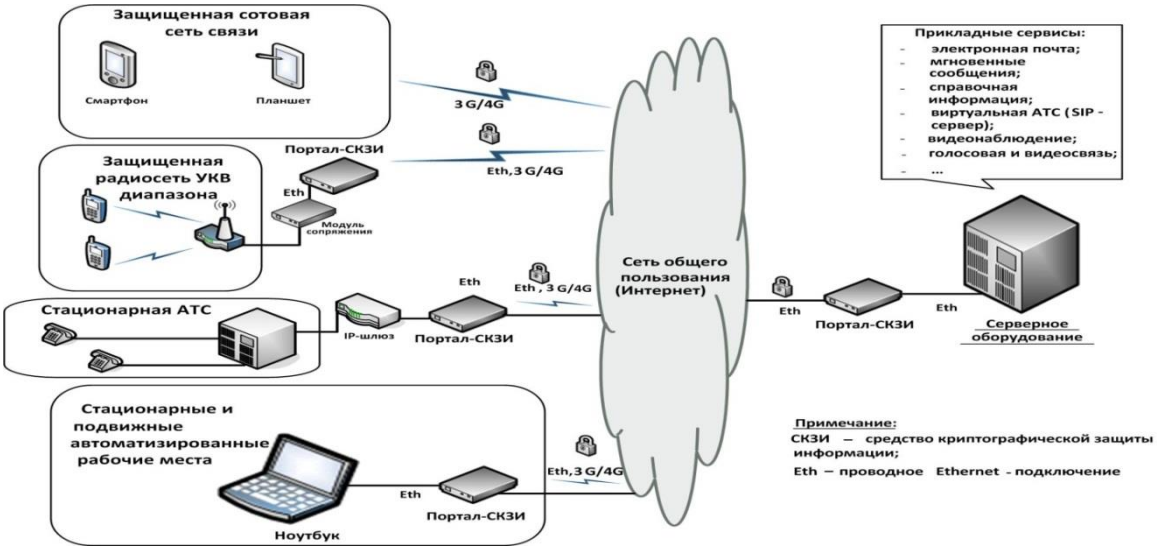
Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Доступ к информационным ресурсам может осуществляться с любого клиентского устройства сети, находящегося за СКЗИ. Разграничение доступа осуществляется с помощью механизмов аутентификации.

Также возможна организация следующей схемы связи разнородных информационных систем и отдельных технических средств в единой криптографически защищенной сервис-ориентированной среде:



Доступна организация системным администратором с помощью виртуальной АТС аудиоконференции между разнородными техническими средствами (смартфон, планшет, радиостанция, стационарный телефон, стационарное и подвижное рабочее место).

Средства криптографической защиты (Портал-СКЗИ)

Криптографическую защиту передаваемых данных в этих средах возможно осуществлять на различных уровнях стека телекоммуникационных протоколов:

- на канальном уровне (в проработке)
- на прикладном уровне (Портал-ПО, Портал-1-SD)
- на сетевом уровне (Портал-10, М-687, Швейцар-М, Портал-1000)

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Таблица 1 – Возможные типы СКЗИ для использования в предлагаемой архитектуре

Наимено-вание	**Класс защиты**	**Скорость**	**Габариты, мм**	**Примечание**
Портал-ПО	длина ключа до 56 бит	Ограничена производи-тельностью устройства	–	Реализуется на прикладном уровне
Портал-1-SIM	длина ключа до 56 бит, для класса КС1 – в разработке	1 Мбит/с	форм-фактор SIM-карты	Совместная работа с программным СКЗИ
Портал-1-SD	длина ключа до 56 бит, для класса КС1 – в разработке		форм-фактор SD-карты, microSD-карты	Совместная работа с Портал-10, Портал-1000
Портал-10	длина ключа до 56 бит, для класса КС1 – в разработке	10 Мбит/с	165×115×25	Поддержка Wi-Fi, работа в динамических IP- адресах Совместная работа с Портал-1-SD, Портал-1000
Портал-1000	длина ключа до 56 бит, для класса КС1, КА – в разработке	600 Мбит/с	440×380×58	Совместная работа с Портал-1-SD, Портал-10, М-687А, Швейцар-М
Швейцар-М	КА, КВ	35 Мбит/с	230×165×55	Совместная работа с М-687, Портал-1000, Швейцар-М
М-687 (М-687А, М-687В)	КА, КВ, гостайна	95 Мбит/с	392x316x53	Совместная работа с Швейцар-М, Портал-1000

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ
440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф
(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Изделие ПОРТАЛ-1-SD

Изделие является составной частью комплекса ПОРТАЛ и обеспечивает шифрование информации с длиной ключа 56 бит.

Обеспечивает

- **обмен с изделиями КТС *ПОРТАЛ***
- чтение ключевой, служебной и пользовательской информации из встроенной FLASH-памяти
- криптографическую обработку информации в соответствии с заданным алгоритмом специального преобразования

Основные технические характеристики

- максимальная тактовая частота – 20 МГц
- ряд напряжений питания – 1,8 В ± 10%; 3,0 В ± 10%; 5,0 В ± 10 %
- интерфейс ввода-вывода информации – последовательный в соответствии со стандартом SD и микроSD (SPI)
- объем встроенной FLASH-памяти – 16 Гбайт
- количество циклов стирания/записи FLASH-памяти – не менее 100 000
- время сохранности информации во FLASH-памяти – не менее 10 лет
- встроенный аппаратный ускоритель операций для криптографических алгоритмов DES
- диапазон рабочих температур: от минус 25 °С до плюс 85 °С.

Производится на базе отечественного микроконтроллера «Курган» с доверенным загрузчиком нулевого уровня.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Изделие ПОРТАЛ-1-SIM

Изделие является составной частью комплекса ПОРТАЛ и обеспечивает шифрование информации с длиной ключа 56 бит по интерфейсу стандарта ISO/IEC 7816-3.

Обеспечивает

- обмен с изделиями КТС *ПОРТАЛ*
- запись, хранение ключевой, служебной и пользовательской информации во встроенной FLASH-памяти
- чтение ключевой, служебной и пользовательской информации из встроенной FLASH-памяти
- криптографическую обработку информации в соответствии с заданным алгоритмом специального преобразования

Основные технические характеристики

- максимальная тактовая частота – 20 МГц
- ряд напряжений питания – 1,8 В ± 10 %; 3,0 В ± 10 %; 5,0 В ± 10 %
- интерфейс ввода-вывода информации – последовательный в соответствии со стандартом ISO/IEC 7816-3
- протокол информационно-логического взаимодействия – оригинальный на основе протокола T0 стандарта ISO/IEC 7816-3
- объем встроенной FLASH-памяти – 384 Кбайт
- количество циклов стирания/записи FLASH-памяти не менее 100 000
- время сохранности информации во FLASH-памяти не менее 10 лет
- встроенный аппаратный ускоритель операций для криптографических алгоритмов – ГОСТ 28147–89 и DES
- встроенный сопроцессор модульной арифметики
- форм-фактор – SIM
- диапазон рабочих температур: от минус 25 до плюс 85 °С

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Изделие ПОРТАЛ-10

Изделие является составной частью комплекса ПОРТАЛ и обеспечивает шифрование и имитозащиту конфиденциальной информации с длиной ключа 56 бит

Обеспечивает

- встречную работу с аналогичным изделием ПОРТАЛ-10, а так же с изделием ПОРТАЛ-1000
- криптографическую защиту IP-пакетов методом полной инкапсуляции
- прозрачное автоматическое шифрование/расшифрование информации с заданной стойкостью по алгоритму шифрования – ГОСТ 28147-89
- контроль целостности пакетов данных – имитозащиту по ГОСТ 28147–89
- аутентификацию источника данных
- ключевую систему – полносвязную ключевую матрицу с индивидуальными ключами на каждом направлении обмена, ключевая структура предусматривает работу с 5000 абонентами
- гибкую полнофункциональную настройку изделия (с ПЭВМ)
- возможность встречной работы через NATP преобразователи (через маршрутизаторы, межсетевые экраны) в сетях с «серой IP адресацией»
- возможность встречной работы через сети операторов сотовой связи 3G (HSDPA, HSUPA,UMTS), EDGE, GPRS, LTE при наличии сервера маршрутизации мобильного трафика;
- возможность подключения USB-модема непосредственно к изделию
- возможность встречной работы по каналам Ethernet (100BASE-T), Wi-Fi
- возможность работы в режиме сервера маршрутизации мобильного трафика
- контроль технического состояния готовности к работе
- контроль наличия действующих и очередных ключей
- контроль целостности программного обеспечения
- контроль меток точного времени
- функцию дистанционного конфигурирования (реконфигурирования)
- дистанционное управление ключами (ввод ключевой информации, переход с действующего ключа на очередной, полное и выборочное стирание ключевой информации)
- круглосуточную необслуживаемую работу

Электропитание изделия ПОРТАЛ-10 осуществляется от:

- сети переменного тока напряжением 220 В (+ 22 В; – 33 В) с частотой 50 Гц
- сети постоянного тока напряжением 5 В (стандартный USB интерфейс)

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Изделие подключается к локальной сети, а также к оборудованию транспортной сети по интерфейсу Ethernet (100BASE-T на скорости 100 Мбит/с), Wi-Fi или к сети операторов сотовой связи 3G (HSDPA, HSUPA,UMTS), EDGE, GPRS, LTE через модемное оборудование и поддерживает протокол Ethernet 802.3 на портах, не внося ограничений в работу протоколов верхних уровней.

Габаритные размеры изделия: 165x110x30 мм; масса 0,7 кг.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Комплекс «Швейцар»

В АО «ПНИЭИ» создан комплекс технических средств, позволяющий решить задачу по защите информации, передаваемой по протоколам IP. Комплекс предназначен для организации защищенной связи и обмена информацией между сегментами телекоммуникационных систем ведомств, а также для решения задач автоматизации управления безопасностью, включая функции дистанционного управления средствами криптографической защиты.

На базе комплекса предусматривается построение подсистем имеющих в составе до 5000 объектов (объект – локальная сеть или отдельный пользователь): архитектура комплекса позволяет строить подсистему криптографической защиты с единым центром управления безопасностью либо с иерархической структурой управления и контроля, содержащей до 200 подсетей.

Разработка велась с учетом потребности средств защиты как в сегменте защиты информации, содержащей сведения, составляющие государственную тайну со степенью секретности «секретно», так и защиты конфиденциальной информации:

– изделия М-687 (гос. тайна), М-687А и М-687В (конфиденциальный контур) с пропускной способность до 100 Мбит/с со стыками Ethernet, обеспечивающие шифрование и имитозащиту информации и режим ввода ключевой информации по каналам связи и удаленного мониторинга, обеспечивают взаимодействие с изделием Швейцар-М (при защите конфиденциальной информации);

– изделие Швейцар-М (конфиденциальный контур) с пропускной способность до 40 Мбит/с, обеспечивающее шифрование и имитозащиту информации и режим ввода ключевой информации по каналам связи и удаленного мониторинга, обеспечивает взаимодействие с изделиями М-684А и М-687В;

– аппаратура М-684 (гос. тайна), М-684А и М-687В (конфиденциальный контур)- станции децентрализованного изготовления ключей и их распределения по каналам связи, с функциями удаленного мониторинга состояния технических средств комплекса, автоматизированного сбора и учета сведений о событиях безопасности в подсистеме криптографической защиты. Обеспечивают возможность организации многоуровневой иерархической подсистемы управления безопасностью в сетях IP, реализованных на базе изделий М-687 (М-687А, М-687В) и Швейцар-М.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

– Все изделия комплекса удобны в эксплуатации, не требуют длительной специальной подготовки персонала, обеспечивают круглосуточную необслуживаемую работу, имеют относительно низкую стоимость по сравнению с аналогами.

– Комплекс является самостоятельной разработкой в полном объеме схемных решений и программного обеспечения, в нем отсутствует системное программное обеспечение сторонних разработчиков и не предъявляются требования к смежной аппаратуре.

Продукт прошел сертификацию на соответствие требованиям ФСБ по защите информации, содержащей сведения, составляющие государственную тайну, и на соответствие по защите информации, не содержащей сведений, составляющих государственную тайну.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Изделие М-687 (М-687А, М-687В)

ИЗДЕЛИЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ В IP-СЕТЯХ

Изделие обеспечивает работу

- М-687 в режиме шифрования и имитозащиты информации, содержащей сведения, составляющие государственную тайну с грифом не выше «секретно» (встречная работа с аналогичным изделием и изделием М-641)
- М-687А в режиме шифрования и имитозащиты конфиденциальной информации, класс КА (встречная работа с аналогичным изделием и изделиями М-641К
- М-687В в режиме шифрования и имитозащиты конфиденциальной информации, класс КВ (изделие работает встречно с аппаратурой Швейцар-Я)

Примечание – изделия изготавливаются по единой документации, различие – ключевые документы, вводимые на объектах эксплуатации.

Изделие имеет два исполнения

- аппаратура М-687 (М-687А, М-687В) РИВУ.465644.01 – с пультом управления ПБ090 РИВУ.468381.010
- аппаратура М-687 (М-687А, М-687В) РИВУ.465644.031-01 – без пульта управления ПБ090 РИВУ.468381.010

Изделие обеспечивает

- криптографическую защиту IP-пакетов методом полной инкапсуляции
- прозрачное автоматическое шифрование/расшифрование информации с заданной стойкостью по алгоритму шифрования – ГОСТ 28147–89
- контроль целостности пакетов данных – имитозащиту по ГОСТ 28147–89
- аутентификацию источника данных
- поддержку фрагментации пакетов
- возможность генерации «ложного трафика» и выравнивание размеров передаваемых пакетов (нормализацию трафика). Режим аналогичный режиму работы изделия «Сито»
- ключевую систему – полносвязную ключевую матрицу с индивидуальными ключами на каждом направлении обмена, ключевая структура предусматривает работу с 5000 абонентов
- гибкую полнофункциональную настройку изделия (с ПЭВМ)
- межсетевое экранирование информационных потоков с выполнением следующих требований:

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

- возможность задания правил фильтрации IP-пакетов для обоих направлений передачи (LAN-WAN, WAN-LAN), с не менее чем 100 правил для каждого направления передачи
- возможность протоколирования событий межсетевого экранирования
- поддержку классификации трафика на основе IP-адресов, номеров протоколов, номеров портов транспортных протоколов TCP и UDP, полей ToS или DiffServ и поддерживает маркировку и перемаркировку трафика по полям ToS или DiffServ в соответствии с заданными правилами.
- возможность назначения IP-адреса «вручную» (статическая адресация) и динамически по протоколу DHCP. Аппаратура с динамически назначенным IP-адресом WAN обеспечивает возможность встречной работы только с аппаратурой с «вручную» назначенным IP-адресом WAN
- возможность дистанционного мониторинга и управления ключевой информациимот аппаратуры децентрализованного изготовления ключей (М-684):
  - контроль технического состояния готовности к работе
  - контроль наличия действующих и очередных ключей
  - контроль целостности программного обеспечения
  - контроль меток точного времени
  - функцию дистанционного конфигурирования (реконфигурирования)
  - дистанционное управления ключами (ввод ключевой информации, переход с действующего ключа на очередные, полное и выборочное стирание ключевой информации)
- защиту от НСД при вскрытии корпуса
- круглосуточную необслуживаемую работу
- пропускную способность 94 Мбит/с при длине передаваемых пакетов 1400 байт

М-687 имеет оригинальный, разработанный специалистами АО «ПНИЭИ» конструктив, выполняющий функции экранирования и теплоотвода с возможностью установки в 19” стойку (высота-1U).

Электропитание изделия осуществляется от сети переменного тока напряжением 220 В (+ 22 В; – 33 В) с частотой 50 Гц ± 2,5 Гц. Мощность, потребляемая изделием от сети переменного тока, не превышает 15 В·А.

Изделие подключается к локальной сети (или отдельной станции), а также к оборудованию транспортной сети по интерфейсам Ethernet (10BASE-T, 100BASE-TX, RJ-45 на скоростях 10 и 100 Мбит/с) и поддерживает протокол Ethernet 802.3 на портах, не внося ограничений в работу протоколов верхних уровней.

Габаритные размеры изделия: 392x316x52,5 мм, масса-5,3 кг.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Швейцар-М

ИЗДЕЛИЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Предназначено для обеспечения безопасности конфиденциальной информации в IP-сетях стандарта IEEE 802.3/802.3u

Обеспечивает

- встречную работу с изделиями Швейцар-Я, Швейцар-М, М-687А, М-687В
- криптографическую аутентификацию изделий встречной работы
- криптографическую защиту IP-пакетов методом полной инкапсуляции
- прозрачное шифрование информации в режиме гаммирования с обратной связью по ГОСТ 28147-89
- контроль целостности пакетов данных – имитозащиту по ГОСТ 28147–89
- создание не менее 50 криптографически защищенных туннелей
- создание 10 новых криптографически защищенных туннелей в секунду
- защиту от кодирования открытой информации (выравнивание трафика, генерация ложного трафика, маркировка поля ToS)
- межсетевое экранирование сетевого трафика на основе пакетной фильтрации
- наличие механизма QoS на сетевом уровне
- наличие ключевой системы – полносвязной ключевой матрицы с индивидуальными ключами на каждом направлении обмена
- возможность встречной работы с 5000 изделий в сети
- ввод ключевой информации с использованием пульта ПБ090
- взаимодействие со станцией генерации и распределения ключей
- функциональную настройку с использованием пульта ПБ090, USB-flash накопителей и ПЭВМ, а также со стороны станции генерации и распределения ключей
- мониторинг работы изделия на ПЭВМ, подключаемой к управляющему порту изделия
- регистрация событий безопасности
- ведение статистики межсетевого экранирования
- контроль целостности программного обеспечения
- защиту от НСД при вскрытии корпуса
- круглосуточную необслуживаемую работу

По условиям эксплуатации изделие удовлетворяет требованиям групп 1.1, 1.3. Диапазон рабочих температур: от – 10 до +50 °С.

Изделие имеет специально разработанный малогабаритный экранированный, теплоотводящий корпус.

Габаритные размеры изделия: 230×165×30 мм.

Вес: ~1кг.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

М-684

АППАРАТУРА ДЕЦЕНТРАЛИЗОВАННОГО ИЗГОТОВЛЕНИЯ, РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ И ОРГАНИЗАЦИИ МНОГОУРОВНЕВОЙ СИСТЕМЫ ДИСТАНЦИОННОГО МОНИТОРИНГА В IP-СЕТЯХ

Предназначена для децентрализованного изготовления и распределения шифрключей по каналам связи и организации многоуровневой системы дистанционного мониторинга в сетях передачи данных IP.

Обеспечивает

- децентрализованное изготовление ключевых документов
- распределение и доведение ключей до изделий Швейцар-М, М-687 (М-687А, М-687В) по каналам связи согласно заданной схемы распределения, а также до М-684, находящейся на нижележащих уровнях управления
- дистанционное управление ключами в изделиях Швейцар-М, М-687 (М-687А, М-687В) и М-684, находящихся на нижележащих уровнях управления, по каналам связи, включая управление сменой, стиранием (сбросом) ключей, контроль их наличия и состояния
- запись ключевой и служебной информации, в том числе и контроль правильности осуществленной записи на носители ДК-6 в целях доставки ключевой информации и ее непосредственного ввода в изделия Швейцар-М, М-687 (М-687А, М-687В), Швейцар-Я согласно заданной схемы распределения
- запись больших массивов ключевой и служебной информации, в том числе и контроль правильности осуществления записи на ВНИ в целях доставки до М-684, находящейся на нижележащих уровнях управления, при отсутствии канала связи
- поэкземплярный учет ключей, сроков их действия, стирания, а также отображение сведений о наличии действующих и очередных ключей в обслуживаемых изделиях Швейцар-М, М-687 (М-687А, М-687В), Швейцар-Я, а также в М-684, находящихся на нижележащих уровнях управления
- своевременную доставку очередных ключей для обслуживаемых изделий Швейцар-М, М-687 (М-687А, М-687В), а также для М-684, находящихся на нижележащих уровнях управления, с использованием каналов связи

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

- выполнение режима удаленного конфигурирования (реконфигурирования) и мониторинга изделий Швейцар-М, М-687 (М-687А, М-687В) в зашифрованном и имитозащищенном виде по каналам связи и отображение его результатов на мониторе:
  - контроль технического состояния готовности к работе
  - контроль наличия действующих и очередных ключей
  - контроль целостности программного обеспечения
  - контроль меток точного времени
  - функцию дистанционного конфигурирования (реконфигурирования)
  - дистанционное управления ключами (ввод ключевой информации, переход с действующего ключа на очередные, полное и выборочное стирание ключевой информации)
- выполнение следующих функций по управлению безопасностью:
  - ведение баз данных, обеспечивающих ввод, хранение и редактирование сведений о криптографической связанности абонентов, а также служебной информации об абонентах
  - ввод сведений о произошедших компрометациях, рассылка и доведение команд восстановления связи в целях исключения скомпрометированных абонентов из сети связи
- круглосуточную работу

Габаритные размеры: 370 х 313 х 70 мм

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Изделие БиоЗамок

БиоЗамок-БВ

БиоЗамок-К

Изделие БиоЗамок предназначено для управления электромеханическим замком или защелкой входной двери с помощью смартфона. Электронное управление замком удобно, тем что позволяет отказаться от использования связки ключей. Это экономит время так как смартфон всегда под рукой.

Модификация БиоЗамок-БВ позволяет дополнительно проверить пользователя посредством биометрической аутентификации. В качестве биометрических характеристик могут использоваться изображение лица или отпечаток пальца. Изделие БиоЗамок поддерживает считывание бесконтактных карт и брелоков RFID, обеспечивает удаленный доступ к встроенной видеокамере.

Управление и конфигурирование изделия БиоЗамок может осуществляться через Web-интерфейс, как на ПК, так и с помощью смартфона.

Монтаж изделия БиоЗамок может производиться:

– на внешнюю сторону двери (БиоЗамок-БВ);

– в полость внутри каркаса двери (БиоЗамок-К);

– в стену (БиоЗамок-БВ).

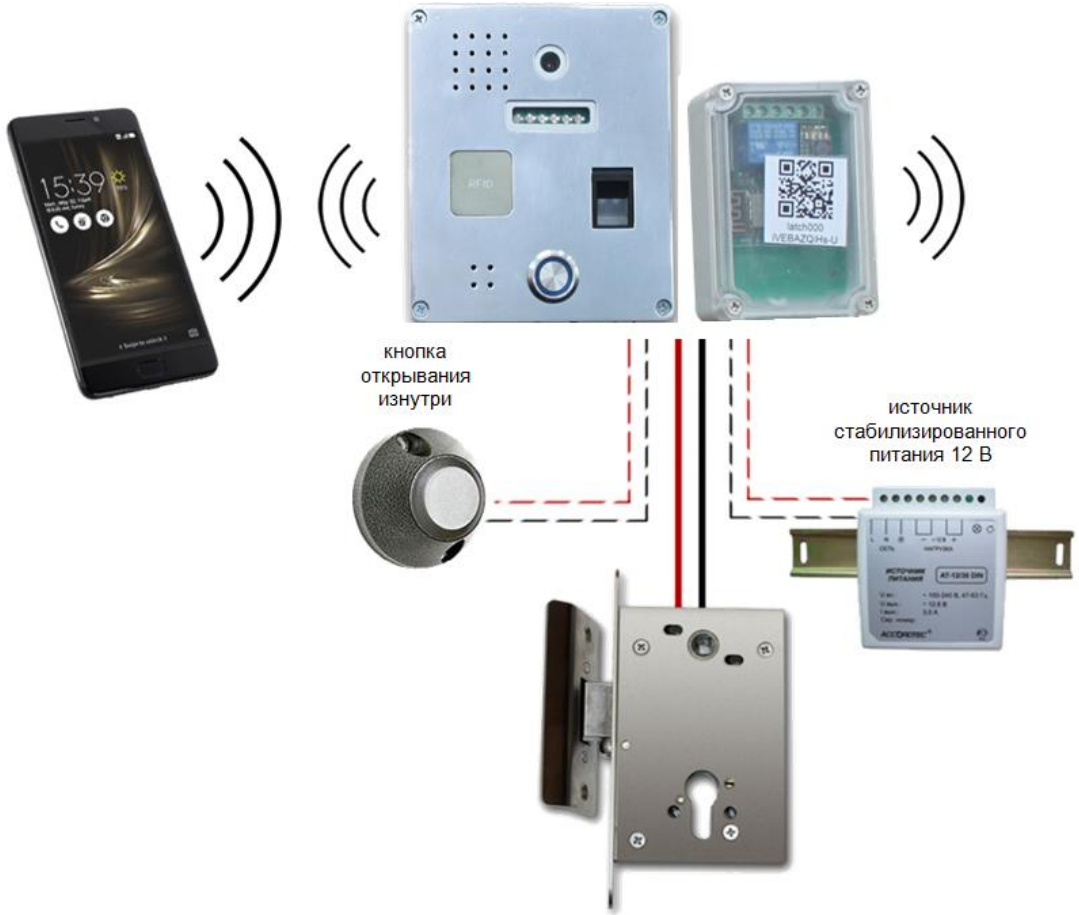
Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Технические характеристики изделия БиоЗамок

Напряжение питания	+12 В
Мощность потребления	6 Вт
Температура эксплуатации	от 0 до +50 °С
Допустимая влажность воздуха	не более 80 %
Вес (нетто)	0,5 кг
Габаритные размеры (ШхВхГ)	130x150x40 мм
Формат бесконтактных карт и брелоков	EM4100
Интерфейс беспроводной сети Wi-Fi	IEEE 802.11 b/g/n
Поддержка браузеров	Firefox, Chrome, Internet Explorer
Разрешение изображения	не менее 320 x 480 пикселей
Вероятность ошибочного предоставления доступа	менее 0,001 %
Вероятность ошибочного отказа в доступе	менее 1%



Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

БиоТокен

ПРОГРАММНО-АППАРАТНОЕ СРЕДСТВО ДЛЯ ПРОВЕРКИ И ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ С БИОМЕТРИЧЕСКИМ ПОДТВЕРЖДЕНИЕМ ЛИЧНОСТИ

Область применения

– системы обезличивания персональных данных медицинских учреждений (в составе изделия БиоГарант)
– системы электронного документооборота, торговли и услуг

и

– системы контроля и управления доступом с аппаратно-программным модулем доверенных вычислений, как отдельный фактор идентификации или для связывания биометрии с паролем доступа
– серверы децентрализованной идентификации пользователей

Функциональные возможности

– получение биометрических данных с графического планшета или сканера отпечатков пальцев
– создание и/или загрузка пары ключей формирования ЭП
– генерация псевдослучайных чисел с использованием естественной нестабильности биометрических образов
– формирование ЭП под электронными документами после биометрической авторизации пользователя
– связывание биометрии с личным ключом в процессе настройки БиоТокен с учетом требований пакета стандартов ГОСТ Р 52633 без выхода введенной биометрии и ключа пользователя из доверенной вычислительной среды БиоТокен
– обучение преобразователя биометрия-код (ГОСТ Р 52633.0–2006) на числе примеров биометрических образов «Свой» от 8 до 32 «Свой»
– хранение параметров связывания в защищенном биометрическом контейнере (ГОСТ Р 52633.4–2011)
– подтверждение критических операций загрузки данных в БиоТокен авторизованным пользователем

Электропитание устройства осуществляется от USB порта ПЭВМ. Устройство потребляет не более 150 мА.

Средство выполнено в форм-факторе USB, по условиям эксплуатации удовлетворяет требованиям климатического исполнения УХЛ4.2 ГОСТ 15150 с ограничением предельной пониженной температуры окружающей среды до минус 10°С.

Средний срок службы – не менее 5 лет.

Средняя наработка на отказ – не менее 10 000 ч.

Габаритные размеры – 72х40х17 мм.

Масса – не более 50 г.

Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

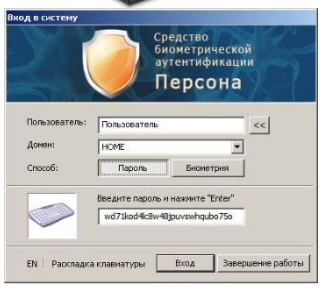
(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Персона

ПРОГРАММНОЕ СРЕДСТВО БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Обеспечивает выполнение функций:

- защищённую биометрическую идентификацию субъектов доступа, проводимую путём создания нейросетевых биометрических контейнеров (НБК)
- простую защищённую и строгую биометрическую аутентификацию субъектов доступа с использованием НБК
- доступ к авторизованному запуску операционной системы Windows XP и контроль доступа к ее ресурсам с помощью средств криптографической защиты информации (СКЗИ)
- защиту файлов данных и контейнеров СКЗИ произвольного размера с помощью биометрических образов

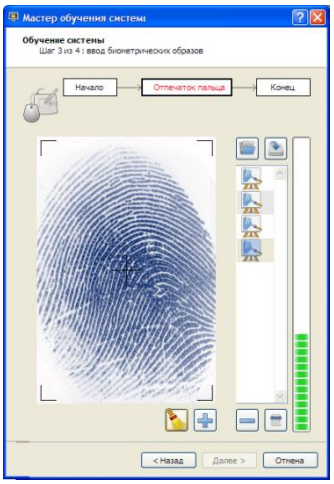


Программное средство осуществляет преобразование легкозапоминаемого рукописного слова-пароля или отпечатка пальца в произвольный длинный пароль или ключ до 256 бит. Таким образом, пользователь избавлен от необходимости хранить надлежащим образом ключ или запоминать длинный случайный пароль. При подключении дополнительных модулей возможно связывание пароля (ключа) с голосовой фразой и другими биометрическими технологиями.

В программном средстве используются алгоритмы быстрого автоматического обучения искусственных нейронных сетей, параметры которых хранятся в нейросетевых биометрических контейнерах.

Преимуществом НБК является то, что сам ключ в них не хранится, не хранятся также биометрические образы пользователя.

Программное средство биометрической идентификации и аутентификации пользователей устанавливается на персональный компьютер с операционной системой семейства Windows, выполнено в соответствии с требованиями пакета стандартов ГОСТ Р 52633 и Федерального закона «О персональных данных».



Акционерное общество
ПЕНЗЕНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ ИНСТИТУТ

440000, г. Пенза, ул. Советская, 9
info@pniei.penza.ru
сайт: пниэи.рф

(841-2) 59-33-50
приемная (841-2) 59-33-35
служба маркетинга (841-2) 59-33-43

Научное издание

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сборник научных статей по материалам
III Всероссийской научно-технической конференции
(г. Пенза, 4 июня 2021 г.)

Том 1

Статьи печатаются в авторской редакции.

Корректор *В. В. Устинская*
Компьютерная верстка *Р. Б. Бердниковой*
Дизайн обложки *А. А. Стаценко*

Подписано в печать 21.09.2021.
Формат $60\times84^{1}/_{16}$. Усл. печ. л. 8,95.
Заказ № 451. Тираж 30.

Издательство ПГУ
440026, Пенза, Красная, 40
Тел./факс: (8412) 666-049, 666-777; e-mail: iic@pnzgu.ru

Вниманию авторов!

Издательство ПГУ выпускает учебную, научную и художественную литературу, презентационную и акцидентную продукцию, а также полноцветные юбилейные и мемориальные издания в соответствии с ГОСТ 7.60–2003.

Издательство ПГУ принимает к изданию рукописи, подготовленные с использованием текстового редактора Microsoft Word for Windows версий **2003 и выше**. Формат – А4, основной шрифт – Times New Roman, 14–16 pt через одинарный интервал (минимальный размер шрифта в таблицах и сносках – 12,5 pt). Тип файла в электронном виде – doc, docx.

Работа должна содержать индекс УДК, аннотацию.

Аннотация (ГОСТ 7.86–2003, ГОСТ 7.9–1995) включает характеристику основной темы, проблемы объекта, цели работы и ее результаты. В аннотации указывают, что нового несет в себе данный документ в сравнении с другими, родственными по тематике и целевому назначению. Аннотация может включать сведения о достоинствах произведения. Текст аннотации начинают фразой, в которой сформулирована главная тема документа. Заканчивается аннотация читательским адресом.

Рисунки и таблицы должны быть размещены в тексте после ссылки на них (растровые рисунки предоставляются в виде отдельных файлов в формате jpg, BMP с разрешением 300 dpi, векторные рисунки в формате Corel Draw с минимальной толщиной линии 0,75 pt. Рисунки должны быть доступны для правки!). Рисунки должны сопровождаться подрисуночными подписями, на все рисунки и таблицы в тексте должны быть ссылки.

Формулы в тексте выполняются только в редакторе формул **MathType версия 5.0** и выше. Символы греческого и русского алфавита должны быть набраны прямо, нежирно; латинского – курсивом, нежирно; обозначения векторов и матриц – прямо, жирно; цифры – прямо, нежирно. Наименования химических элементов набираются прямо, нежирно. Эти же требования необходимо соблюдать и в рисунках.

В списке литературы **нумерация источников** должна соответствовать очередности ссылок на них в тексте ([1], [2], …). Номер источника указывается в квадратных скобках. Требования к оформлению списка литературы на русские и иностранные источники (ГОСТ Р 7.0.5–2008): для книг – фамилия и инициалы автора, название, город, издательство, год издания, том, количество страниц; для журнальных статей, сборников трудов – фамилия и инициалы автора, название статьи, полное название журнала или сборника, серия, год, том, номер, страницы; для материалов конференций – фамилия и инициалы автора, название статьи, название конференции, город, издательство, год, страницы.

К материалам **должна** прилагаться следующая информация: фамилия, имя, отчество, контактные телефоны.

Контакты Издательства ПГУ: т.: (8412) 66-60-49, 66-67-77, e-mail: iic@pnzgu.ru