Полученные результаты моделирования методов сглаживания смеси полезного сигнала и шума при различных параметрах сигналов и сглаживающих фильтров позволяют сделать следующие выводы.

Для заданного значения уровня σ шума существует оптимальное значение ширины b_{opt} окна сглаживания, при котором достигается максимальное значение коэффициента *knr* подавления шума. Отметим, что оптимальное значение b_{opt}, обеспечивающее максимальное значение коэффициента *knr* подавления шума, нелинейно увеличивается с ростом уровня σ входного шума фильтра.

Максимальные коэффициенты подавления шума, обеспечиваемые при этом фильтрами *ksmooth* и *rsmooth*, близки по величине, но достигаются при различных значениях b_{opt} (у фильтра *rsmooth* оптимальная ширина окна в 1,25 раза больше). Максимальное подавление шума с помощью медианного фильтра требует еще большего значения b_{opt}, но обеспечиваемый при этом коэффициент подавления минимален.

Таким образом, имея оценку уровня шума, искажающего полезный сигнал, можно подобрать оптимальную ширину окна сглаживания фильтра, обеспечивая при этом максимальное подавление мешающего шума (до 5-6 раз) для любого сглаживающего фильтра (из рассмотренных). Из них наибольший коэффициент подавления обеспечивают фильтры *ksmooth* и *rsmooth*. При этом, первый обладает наименьшей оптимальной шириной окна, но требует ее тщательного подбора. Полученный результат позволяет обеспечить адаптивную обработку сигналов телекоммуникационных систем в зависимости от текущей помеховой обстановки и тем самым обеспечить максимальную достоверность приема данных с помощью достаточно простых программно-аппаратных средств.

Литература

1. Апорович А.Ф., Чердынцев В.А. Радиотехнические системы передачи информации. – Минск: Вышэйшая школа, 1985. – 214с.: ил.
2. Былянски П., Ингрем Д. Цифровые системы передачи: Пер. с англ. / Под ред. А.А. Визеля. – М.: Связь, 1980. – 360 с. : ил.
3. Степанов А.В., Матвеев С.А. Методы компьютерной обработки сигналов систем радиосвязи. – М.: Солон-Пресс, 2003. – 208 с. : ил.
4. Васильев В.П. Основы теории и расчета цифровых фильтров / В.П. Васильев, Э.Л. Муро, С.М. Смольский: под. ред. С.М. Смольского. – 2-е изд., стереотип. – М.: ИНФРА-М, 2018. – 272 с. : ил.
5. Денисенко А.Н. Цифровые сигналы и фильтры. – М.: ИД МЕДПРАКТИКА-М, 2008. – 188 с. : ил.
6. Троян В.Н., Киселев Ю.В. Анализ и обработка данных. – СПб.: Изд-во С.-Петерб. Ун-та, 2010. – 580 с. : ил.
7. Кирьянов Д. В. Mathcad 15 / Mathcad Prime 1.0. – СПб.: БХВ-Петербург, 2012. – 432 с. : ил.
8. Воскобойников Ю.Е., Задорожный А.Ф. Основы моделирования и программирования в пакете MathCAD. – 2-е изд., стереотип. – СПб.: Издательство Лань, 2018. – 224 с. : ил.

REFERENCES

1. Aporovich A.F., Cherdyntsev V.A. Radiotekhnicheskie sistemy peredachi informatsii. – Minsk: Vysheyshaya shkola, 1985. – 214s.: il.
2. Bylyanski P., Ingrem D. Tsifrovye sistemy peredachi: Per. s angl. / Pod red. A.A. Vizelya. – M.: Svyaz, 1980. – 360s. : il.
3. Stepanov A.V., Matveev S.A. Metody komp'yuternoy obrabotki signalov sistem radiosvyazi. – M: Solon-Press, 2003. – 208 s. : il.
4. Vasil'ev V.P. Osnovy teorii i rascheta tsifrovykh fil'trov / V.P. Vasil'ev, E.L. Muro, S.M. Smol'skiy: pod. red. S.M. Smol'skogo. – 2-e izd., stereotip. – M.: INFRA-M, 2018. – 272s. : il.
5. Denisenko A.N. Tsifrovye signaly i fil'try. – M.: ID MEDPRAKTIKA-M, 2008. – 188s. : il.
6. Troyan V.N., Kiselev Yu.V. Analiz i obrabotka dannykh. – SPb.: Izd-vo S.-Peterb. Un-ta, 2010. – 580s. : il.
7. Kir'yanov D. V. Mathcad 15 / Mathcad Prime 1.0. – SPb.: BKhV-Peterburg, 2012. – 432 s. : il.
8. Voskoboynikov Yu.E., Zadorozhnyy A.F. Osnovy modelirovaniya i programmirovaniya v pakete MathCAD. – 2-e izd., stereotip. – SPb.: Izdatel'stvo Lan', 2018. – 224 s. : il.

УДК 681.3.001:518.5
DOI: 10.34046/aumsuomt100/24

ОЦЕНКИ КАЧЕСТВА МОДИФИЦИРОВАННОГО ШИФРА ФЕЙСТЕЛЯ С ИНВОЛЮТИВНОЙ КВАТЕРНИОННОЙ МАТРИЦЕЙ

Е.И. Духнич, доктор технических наук
Д.А. Демищенко

В данной статье описывается сравнение алгоритмов шифрования, основанных на построении шифра Фейстеля, повышение его эффективности с применением кватернионной инволютивной матрицы. Приведены результаты теста случайностей.

Ключевые слова: криптография, метод Фейстеля, шифрование, дешифрование, кватернионная инволютивная матрица.

QUALITY ASSESSMENT OF THE MODIFIED FEISEL CODE WITH AN INVOLUTIVE QUATERNION MATRIX

E.I. Dukhnich, D.A. Demischenko

This article describes a comparison of encryption algorithms based on the construction of the Feistel cipher, increasing its efficiency using a quaternionic involutive matrix. Bringing the results of the test of chances.
Keywords: cryptography, Feistel method, encryption, decryption, quaternion involutive matrix.

В данной статье мы проведем ценочный анализ алгоритма, предложенного в статье [1], и алгоритма модифицированного инволютивной кватернионной матрицей [2]. Приобретённым достоинством модифицированного алгоритма является ускорения работы алгоритма за счет снижение частоты формирования ключевой матрицы. Размер обрабатываемого блока исходного изображения (сообщения) увеличен до размера 8×8.

В статье [1] был предложен блочный шифр как модификация шифра Фейстеля, в котором открытый текст (P), размером $m \times 2m$, в виде пары матриц P_0 и Q_0, размером $m \times m$, с помощью ключевой матрицы (K) проходит шифрование по алгоритму:

$$P_i = (KQ_{i-1}K^{-1}) mod N Q_i = (P_i + P_{i-1}) \mathrm{mod} N, \quad (1)$$

где i= 1,2,,,n.

Дешифрование выполняется по алгоритму:

$$Q_{i-1} = (K^{-1}P_iK) mod N, P_{i-1} = (Q_i - P_i) \mathrm{mod} N, \quad (2)$$

где i=n, n-1,,, 1.

Приобретенным достоинством этого алгоритма можно считать высокую криптостойкость, однако он отличается высокой сложностью из-за необходимости обращения ключевой матрицы. Причем, если обратной ключевой матрицы не существует, то получатель не сможет расшифровать зашифрованное сообщение.

В статье [3] этот алгоритм был изменен путем использования в качестве ключевой матрицы кватерниона q. При этом первая формула в (1) была заменена на:

$$P_i = (qQ_{i-1}q^{-1}) mod N, \quad (3)$$

а первая формула в (2) была заменена на

$$Q_{i-1} = (q^{-1}P_iq) mod N \quad (4)$$

При этом сложность алгоритма несколько снизилась, но необходимость вычисления обратного кватерниона осталась его недостатком.

В статье [2] для модификации шифра Хилла было предложено использовать инволютивную (обратную самой себе) форму ключевой матрицы, что упрощает процесс дешифрования. Для ее формирования используется кватернион:

$$q = w + xi + yj + zk. \quad (5)$$

Данному кватерниону соответствует матрица K_{11} следующего вида:

$$K_{11} = \begin{bmatrix} w_{11} & x_{12} & y_{21} & z_{22} \\ -x_{12} & w_{11} & -z_{22} & y_{21} \\ -y_{21} & z_{22} & w_{11} & -x_{12} \\ -z_{22} & -y_{21} & x_{12} & w_{11} \end{bmatrix} \quad (6)$$

Далее формируется кватернионная инволютивная ключевая матрица:

$$K_m = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}, \quad (7)$$

где $K_{12} = I - K_{11}$, $K_{21} = I + K_{11}$ и $K_{22} = -K_{11}$, I – единичная матрица.

Блок-схема предлагаемого алгоритма шифрования представлена на рис. 1, где ||– операция конкатенации.

Оба алгоритма были реализованы, их результаты шифрования и дешифрования представлены на рисунках (рис. 2-3) соответственно.

Из сравнения рис. 2 и 3 визуально видно, что пиксели на зашифрованном модифицированным алгоритмом изображении более равномерно распределены. Для количественного сравнения качества шифров можно использовать статистические тесты diehard [4], которые оценивают качество набора случайных чисел. Вместе они рассматриваются как один из наиболее строгих существующих наборов тестов (отсюда и название — англ. «die-hard» в качестве прилагательного означает приблизительно «трудноубиваемый» и обычно переводится на русский фразеологизмом «крепкий орешек»).

Описание тестов:

1. Дни рождения (BirthdaySpacings) — выбираются случайные точки на большом интервале. Расстояния между точками должны быть асимптотически распределены по Пуассону. Название этот тест получил на основе парадокса дней рождения.

2. Ранги матриц (Ranksofmatrices) — выбираются некоторое количество бит из некоторого количества случайных чисел для формирования матрицы над {0,1}, затем определяется ранг матрицы. Считаются ранги.

3. Тест на парковку (ParkingLot Test) — единичные окружности случайно размещаются в квадрате 100×100. Если окружность пересекает уже существующую, попытаться ещё. После 12

000 попыток, количество успешно «припаркованных» окружностей должно быть нормально распределено.

4. Тест случайных сфер (RandomSpheres Test) — случайно выбираются 4000 точек в кубе с ребром 1000. В каждой точке помещается сфера, чей радиус является минимальным расстоянием до другой точки. Минимальный объём сферы должен быть экспоненциально распределён с некоторой медианой.

5. Пересекающиеся перестановки (OverlappingPermutations) — анализируются последовательности пяти последовательных случайных чисел. 120 возможных перестановок должны получаться со статистически эквивалентной вероятностью

6. Тест игры в кости (The Craps Test) — играется 200 000 игр в кости, подсчитываются победы и количество бросков в каждой игре. Каждое число должно удовлетворять некоторому распределению.

7. Тест сжатия (The Squeeze Test) — 231 умножается на случайные вещественные числа в диапазоне [0,1) до тех пор, пока не получится 1. Повторяется 100 000 раз. Количество вещественных чисел, необходимых для достижения 1, должно быть распределено определённым образом.

8. Тест пересекающихся сумм (OverlappingSums Test) — генерируется длинная последовательность вещественных чисел из интервала [0,1). В ней суммируются каждые 100 последовательных чисел. Суммы должны быть нормально распределены с характерными средним и дисперсией.

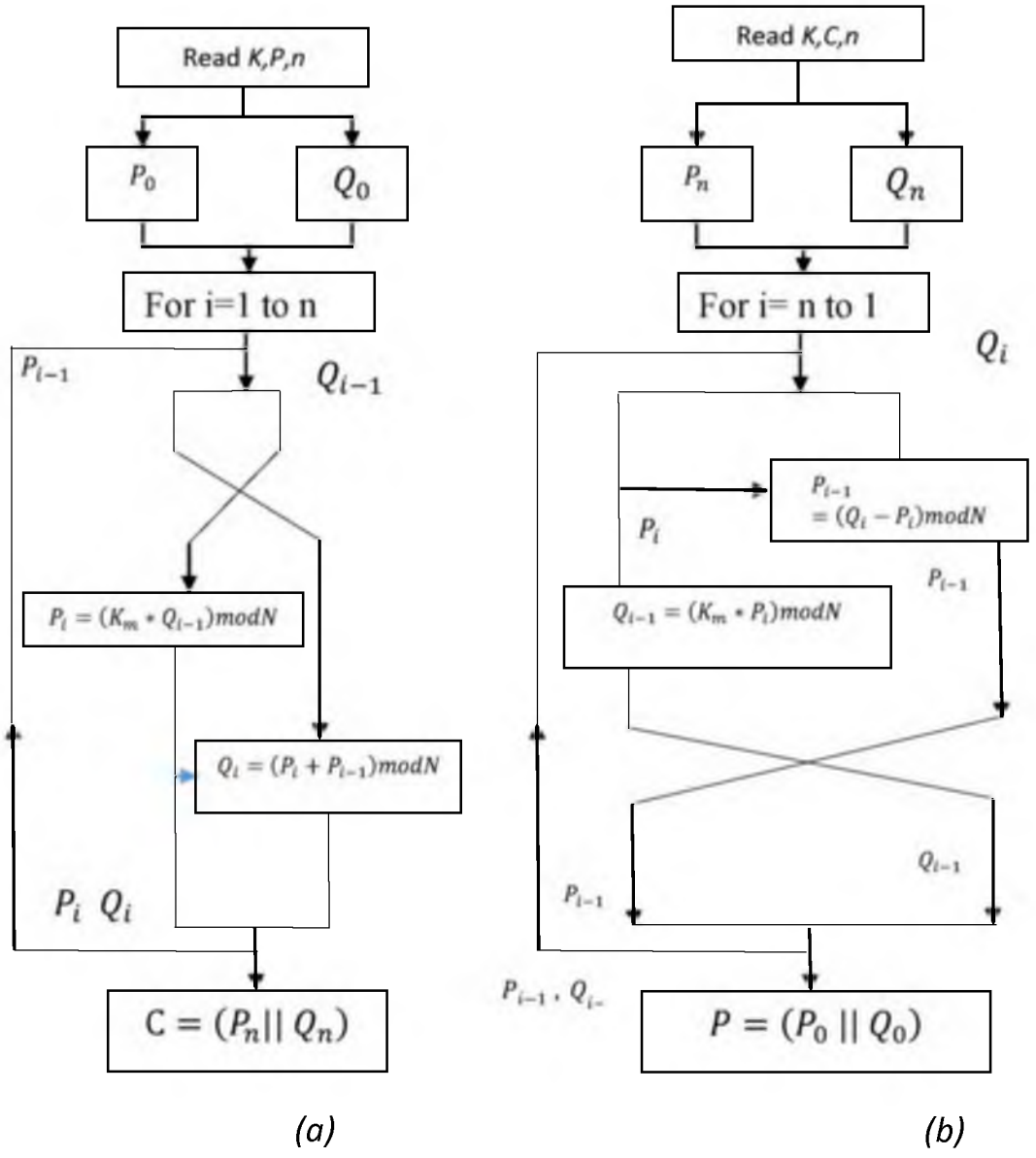

Рисунок 1 – a) Блок-схема алгоритма шифрования, b) Блок-схема алгоритма дешифрования

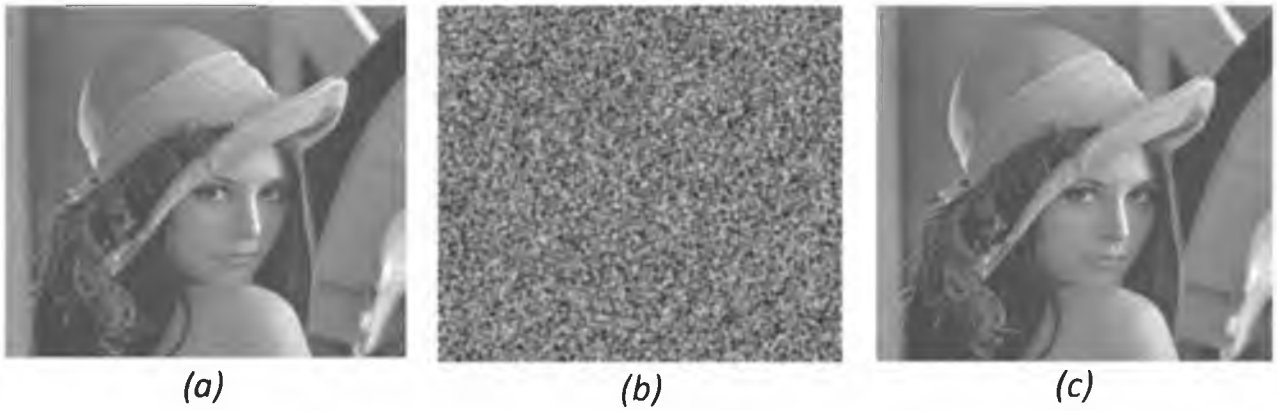

Рисунок 2 – a) оригинальное изображение, b) зашифрованное оригинальным шифром изображение, c) результат дешифрования изображения

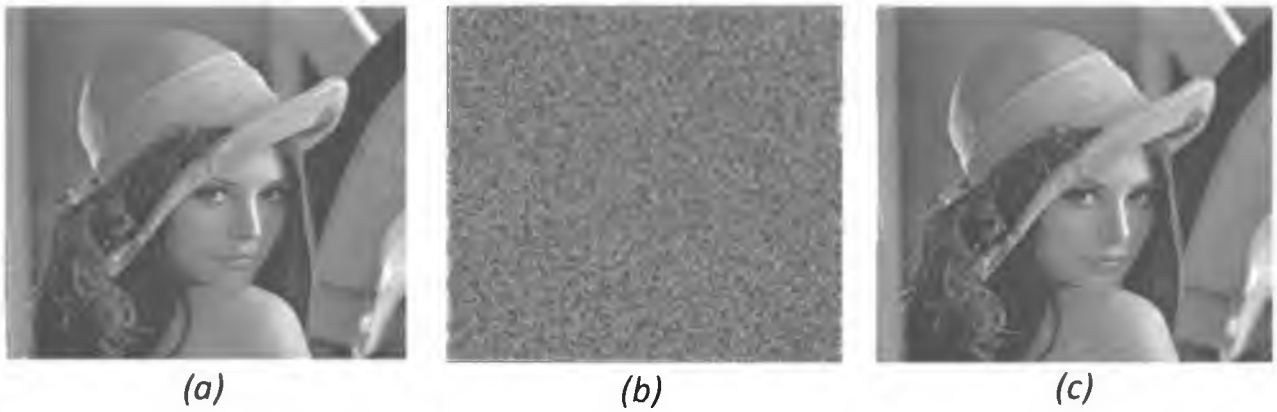

Рисунок 3 – a) оригинальное изображение, b) зашифрованное модифицированным шифром изображение, c) результат дешифрования изображения

Тесты случайности, основанные на тестах diehard [4], а также на бесплатном приложении Cryptool [5], были реализованы для оценки уровня безопасности предлагаемых модели шифрования. Результатом каждого теста является основной фактор, который сообщает нам об эффективности полученной случайности в зашифрованных данных. Его значения варьируется от 0 до 1, и необходимо всегда стремиться к значениям, близким к 0.5. Если значение равно 0 или 1, это означает, что зашифрованные данные не проходят данный тест на случайность. Полученные результаты для выбранных испытаний на случайность для обоих алгоритмов шифрования приведены в Таблицах 1 и 2 соответственно

Таблица 1 – Результаты тестов Diehard оригинального шифра

Birthdayspicing	Binaryrank	Parkinglot	3D Sphere	rank	Craps	operm5	diehardsums
0.792	0.665	0.112	0.364	0.196	0.615	0.564	0.548

Таблица 2 – Результаты тестов Diehard модифицированного шифра

Birthdayspicing	Binaryrank	Parkinglot	3D Sphere	rank	Craps	operm5	diehardsums
0.475	0.547	0.622	0.723	0.457	0.491	0.415	0.451

Значение близкое к 0.5 показывает, что последовательность входных символов сгенерирована с вероятностью, близкой к случайной. Сравнение Таблиц 1 и 2 свидетельствует, что модифицированный шифр имеет преимущества перед оригинальным, так как корреляция между зашифрованным сообщением и исходным практически отсутствует.

Литература:

1. Sastry V. U. K, Anup Kumar K., A Modified Feistel Cipher Involving ModularArithmetic Addition and Modular Arithmetic Inverse of a Key Matrix.

(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 3, No. 7, 2012, pp. 40-43.
2. Духнич Е.И., Демищенко Д.А. Модификация шифра Фейстеля с инволютивной кватернионной матрицей // Вестник ГМУ им. адмирала Ф.Ф. Ушакова.– 2020. – №3 (32).– С.92-96.
3. Mariusz Dzwonkowski, Michal Papaj, and Roman Rykaczewski. A New Quaternion-Based Encryption Method for DICOM Images. IEEE Transactionsonimageprocessing, vol. 24, no. 11, November 2015, pp. 4614-4622.
4. Ключарев П.Г. О статическом тестировании блочных шифров. // Математика и математическое моделирование – 2018 – №5 – С. 35-36.
5. https://webhome.phy.duke.edu/~rgb/General/dieharder.php
6. https://www.cryptool.org/en/

References

1. Sastry V. U. K, K. Anup Kumar, A Modified Feistel Cipher Involving ModularArithmetic Addition and Modular Arithmetic Inverse of a Key Matrix. (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 3, No. 7, 2012, pp. 40-43.
2. E.I. Duhnich, D.A. Demishchenko. Modifikaciya shifra Fejstelya s involyutivnojkvaternionnoj matricej. Vestnik GMU im. Admirala F.F. Ushakova.-2020. -№3 (32).-S.92-96.
3. Mariusz Dzwonkowski, Michal Papaj, and Roman Rykaczewski. A New Quaternion-Based Encryption Method for DICOM Images. IEEE Transactionsonimageprocessing, vol. 24, no. 11, November 2015, pp. 4614-4622.
4. Klyucharyov P.G. O staticheskom testirovanii blochnyh shifrov. Matematika i matematicheskoe modelirovanie- 2018 №5. C. 35-36.
5. https://webhome.phy.duke.edu/~rgb/General/dieharder.php
6. https://www.cryptool.org/en/

УДК 004.032.2
DOI: 10.34046/aumsuomt100/25

СРАВНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ МЕДИЦИНСКОЙ МАСКИ НА ФОТО И ВИДЕО

Г. Е. Панамарев, доктор технических наук, профессор
И.В. Родыгина, кандидат технических наук, доцент
А.А. Шевченко, магистрант

Во время пандемии COVID-19 во всём мире приняты рекомендации к ношению медицинских масок и ограничен допуск в места массового скопления людей тех, кто игнорирует это требование. С помощью свёрточных нейронных сетей и глубокого обучения есть возможность анализировать видеопоток, чтобы облегчить работу на пропускных пунктах и отмечать людей без масок. В данной статье рассматриваются три нейронные сети, их обучение и сравнительных анализ. Данный пример показывает, как можно легко подготовить нейронную сеть под определённую задачу.
Ключевые слова: нейронная сеть, глубокое обучение, CNN, свёрточная сеть, компьютерное зрение, обучение нейронных сетей, анализ видеопотока, MobileNet V2, Xception, Inception V3

COMPARISON OF NEURAL NETWORKS FOR DETECTING A MEDICAL MASK ON PHOTOS AND VIDEOS

G.E. Panamarev, I.V. Rodygina, A.A. Shevchenko

During the COVID-19 pandemic, recommendations for wearing medical masks have been adopted around the world and admission to crowded places of those who ignore this requirement is limited. With the help of convolutional neural networks and deep learning, it is possible to analyze the video stream to facilitate work at checkpoints and mark people without masks. This article examines three neural networks, their training and comparative analysis. This example shows how you can easily prepare a neural network for a specific task.
Keywords: neural network, deep learning, CNN, machine learning, computer vision, MobileNet V2, Xception, Inception V3.

Введение. Болезнь, вызванная коронавирусной инфекцией COVID-2019, – это инфекционное заболевание, вызванное новым, ранее неизвестным коронавирусом. У большинства заболевших COVID-19 наблюдаются легкие или умеренные симптомы, выздоровление происходит без специфического лечения [2].

Одной из мер защиты от распространения COVID-19 является ношение медицинской маски, поэтому во всех общественных местах требуют выполнять эту рекомендацию. Для этого на входах в торговые центры, метро, транспорт и т.д. стоят пропускные пункты, где измеряют температуру и проверяют наличие защитных средств. Но,