ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(59) / 2026

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Регистрационный номер ПИ № ФС77-91645 от 27.05.2026

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76. ЮУрГУ, Издательский центр
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 1(59) / 2026

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Registration number
PI No. ФС77-91645 dd. 27.05.2026

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76 SUSU, Publishing Center
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

IN THIS ISSUE

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК 004.056.2; 316.334.3:324(470+571) Вестник УрФО № 1(59) / 2026, с. 5–19

Поршнев С.В., Рябко Н.Ю.

DOI: 10.14529/secur260101

ИССЛЕДОВАНИЕ МЕТОДОВ ЭЛЕКТОРАЛЬНОЙ КРИМИНАЛИСТИКИ (ЧАСТЬ 2)

В первой части статьи проведен обзор методов электоральной криминалистики (ЭК), наиболее часто используемых для анализа электоральных данных (ЭД) и вычисленных на их основе электоральных показателей (ЭП), публикуемых Центральной избирательной комиссией (ЦИК) по результатам проведенных выборов с целью выявления в них преднамеренно внесенных аномалий (фальсификации ЭД), в числе которых:

– методы ЭК, основанные проверке соответствия эмпирических плотностей распределений (ПР) и функций распределений (ФР) цифр и пар одинаковых цифр в ЭП законам Бенфорда, Стиглера и их известным модификациям, предложенным Л. Леманом и Д. Бохлером, а также Л. Перикки и Д. Торресом;

– метод А. Собянина и В. Суховольского;

– метод С. Шпилькина[1];

– метод А. Подлазова,

которые, однако, не имеются по собой научно-обоснованного базиса, в связи с чем требуется их целенаправленные исследования.

Далее в статье был проведен аналитического анализ метода А. Собянина и В. Суховольского, результаты которого опровергли гипотезу о возможности его использования для анализа ЭД и ЭП.

Во второй части статьи рассматриваются результаты применения перечисленных выше методов ЭК к модельным ЭД, в которые заведомо не вносились целенаправленно какие-либо искажения, синтезированные в соответствие с предложенным авторами алгоритмом. Анализ полученных результатов позволил сделать обоснованный вывод о том, что изученные методы ЭК обнаружили признаки целенаправленно внесенных аномалий в модельных заведомо нефальсифицированных электоральных данных. в том числе, и синтезированных заведомо нефальсифицированных ЭД. В этой связи изученные методы ЭК не должны использоваться в практике ЭК, а сделанные ранее на основе их применения выводы о выявлении масштабных фальсификаций ЭД, опубликованных по итогам выборов в органы государственной власти Российской федерации, органы местного самоуправления и референдумов, проводившихся в XXI в., требуют критического переосмысления.

Ключевые слова: *электоральная криминалистика, электоральные данные, электоральные показатели, фальсификация электоральных данных, избирательная комиссия, выборы, случайная величина с ограниченной областью рассеяния, случайные блуждания, плотность распределения, функция распределения.*

THE ELECTORAL FORENSICS METHODS RESEARCH (PART 2)

The first part article provides an overview of the electoral forensics methods (EF), which are most often used to analyze electoral data (ED) and calculated electoral indicators (EI) based on them, published by the Central Election Commission (CEC) based on of the result selections in order to identify intentionally introduced anomalies (ED falsifications), including which:

– the EF methods based on checking the empirical the EI digits distribution densities (PR) and the EI digits distribution functions (FR) of and the identical digits pairs correspondence to the Benford, Stigler laws and their well-known modifications proposed by L. Leeman and D. Bohler, as well as L. Pericchi and D. Torres;

– the method of A. Sobyanin and V. Sukhovolsky;

– the method of S. Shpilkin;

– the A. Podlazov's method,

which, however, do not have a scientifically sound basis, and therefore require their targeted research.

Further in the article, an analytical analysis of the A. Sobyanin and V. Sukhovolsky method was carried out, the results of which refuted the hypothesis about the possibility of its use for the analysis of ED and EI.

The second part article examines the applying the above-mentioned EF methods to model ED result, which obviously did not purposefully introduce any distortions synthesized in accordance with the algorithm proposed by the authors. The obtained results analysis allowed us to make a reasonable conclusion that the EF methods studied revealed signs of purposefully introduced anomalies in the deliberately unfixed model electoral data. including synthesized deliberately unfalsified ED. In this regard, the studied EF methods should not be used in EC practice, and the conclusions drawn earlier on the basis of their application on the identification of large-scale falsifications of ED published following the results of elections to state authorities of the Russian Federation, local governments and referendums held in the 21st century require critical rethinking.

Keywords: *electoral forensics, electoral data, electoral indicators, falsification of electoral data, electoral commission, elections, random variable with a limited scattering area, random walks, distribution density, distribution function.*

В связи с высокой социальной и политической значимостью публично озвучиваемых выводов о соответствии результатов проведенных выборов ействительным электоральным предпочтениям избирателей, сделанных на основе применения к публикуемым ЭД методов ЭК, очевидна необходимость оценки адекватности получаемых при этом результатов.

Для этого, как очевидно, достаточно провести анализ результатов применения методов ЭК к ЭД, опубликованным по результатам «абсолютно честных» выборов. Однако, способов получения прямых доказательств «абсолютной честности» проведенных выборов, признаваемых всеми участниками политического процесса, в настоящее время не существует. Выход из данной ситуации состоит в использовании наборов синтезированных (модельных) ЭД, в которые, заведомо, не вносились какие-либо изменения, статистические свойства которых должны быть подобными статистическим свойствам реальных ЭД.

Для обоснования алгоритма генерации модельных ЭД был проведен системный анализ структуры ЭД, публикуемых по окончанию выборов, проводимых с использованием 4-х уровневой избирательной системы, архитектура которой аналогична архитектуре избирательной системы Российской Федерации (РФ). Далее на основе использования

результатов, полученных на первом этапе исследования, был разработан алгоритм синтеза модельных ЭД, обоснован выбор математической модели функции распределения (ФР) ЭД, синтезированы модельные ЭД и проведено их сравнение, а также вычисленных на их основе ЭП, с аналогичными характеристиками реальных ЭД, опубликованных Центральной избирательной комиссией (ЦИК) РФ по результатам выборов в 2028 г. Президента России (далее Выборы-2018), подтвердивших непротиворечивость реальных и модельных ЭД. Далее синтезированные ЭД были использованы для оценки адекватности некоторых наиболее известных методов ЭК.

ВВЕДЕНИЕ

Данная статья является продолжением статьи [1], в которой было начато системное исследование известных методов ЭК, обеспечивающих по мнению их создателей и согласных с ними экспертов, занимающихся анализом и интерпретацией результатов проводимых выборов.

1. СТРУКТУРНЫЕ МОДЕЛИ ЭД И ВЫЧИСЛЯЕМЫХ НА ИХ ОСНОВЕ ЭП

Введем используемые далее понятия, используемые для описания первичных ЭД, и вычисляемых на их основе ЭП. Предположим, что в стране «N» создана иерархическая избирательная система, состоящая из 4 уровней иерархии: 1-ый уровень иерархии – ЦИК, 2-ой уровень иерархии – избирательные комиссии (ИК); 3-ый уровень иерархии – территориальные избирательные комиссии (ТИК); 4-ый уровень иерархии – участковые избирательные комиссии (УИК). При этом названия каждой из ИК, ТИК и УИК являются уникальными.

Обозначим:

– число ИК, созданных ЦИК $N^{EC}_{ЦИК}$;

– нумерованное множество, составленное из названий ИК, (в математике – кортеж)

$$Name_{\langle ИК\rangle} = \bigcup_{i=1}^{N^{EC}_{ЦИК}} \left[Name_{\langle ИК\rangle}\right]_i, \left(\left[Name_{\langle ИК\rangle}\right]_{i_1} \neq \left[Name_{\langle ИК\rangle}\right]_{i_2},\ i_1 \neq i_2\right);$$

– единичный вектор размерности $N^{EC}_{ЦИК} \times 1$:

$$\left[N^{EC}_{ИК}\right]_i = 1,\ i = \overline{1, N^{EC}_{ЦИК}},\ N^{EC}_{ЦИК} = \sum_{i=1}^{N^{EC}_{ЦИК}} \left[N^{EC}_{ИК}\right]_i;$$

– вектор, значения координат которого равняются числу ТИК, созданных i-ой ИК $\left[N^{EC}_{ТИК}\right]_i$;

– множество, составленное кортежей формата <Название i-ой ИК_Название j-ой ТИК, созданной i-ой ИК>:

$$Name_{\langle ТИК\rangle} = \bigcup_{i=1}^{N^{EC}_{ИК}} \bigcup_{j=1}^{\left[N^{EC}_{ТИК}\right]_i} \left[Name_{\langle ИК\rangle}\right]_i . \left[Name_{\langle ТИК\rangle}\right]_j,$$

при этом $\left[Name_{\langle ТИК\rangle}\right]_{j_1} \neq \left[Name_{\langle ТИК\rangle}\right]_{j_2}$, если $j_1 \neq j_2$;

– матрицу, элементы которой число ТИК, созданных в i-ой ИК, $\left[N^{EC}_{ТИК}\right]_{i,j}$, $i = \overline{1, N^{EC}_{ИК}}$, $j = \overline{1, \left[N^{EC}_{ИК}\right]_i}$;

– множество, составленное из матриц $\left[N^{EC}_{ТИК}\right]_{i,j}$:

$$N^{EC}_{ТИК} = \bigcup_{i=1}^{N^{EC}_{ИК}} \bigcup_{j=1}^{\left[N^{EC}_{ТИК}\right]_i} \left[N^{EC}_{ТИК}\right]_{i,j},$$

где $\sum_{j=1}^{\left[N^{EC}_{ИК}\right]_i} \left[N^{EC}_{ТИК}\right]_{i,j} = \left[N^{EC}_{ТИК}\right]_i$;

– множество, составленное кортежей формата <Название i-ой ИК.Название j-ой ТИК, созданной в i-ой ИК. Название k-ой УИК, созданной в (i,j)-ой ТИК>:

$$Name_{\langle УИК\rangle} = \bigcup_{i=1}^{N^{EC}_{ИК}} \bigcup_{j=1}^{\left[N^{EC}_{ТИК}\right]_i} \bigcup_{k=1}^{\left[N^{EC}_{УИК}\right]_{i,j}} \left[Name_{\langle ИК\rangle}\right]_i . \left[Name_{\langle ТИК\rangle}\right]_j . \left[Name_{\langle УИК\rangle}\right]_k,$$

где $\left[Name_{\langle УИК\rangle}\right]_{k_1} \neq \left[Name_{\langle УИК\rangle}\right]_{k_2}$ для любых $k_1 \neq k_2$;

– тензор $\left[N^{EC}_{УИК}\right]_{i,j,k}$, $i = \overline{1, N^{EC}_{ИК}}$, $j = \overline{1, \left[N^{EC}_{ИК}\right]_i}$, $k = \overline{1, \left[N^{EC}_{УИК}\right]_{i,j}}$, элементы которого – число УИК, созданных (i,j)-ой ТИК, $\left[N^{EC}_{ТИК}\right]_{i,j} = \sum_{k=1}^{\left[N^{EC}_{ТИК}\right]_j} \left[N^{EC}_{УИК}\right]_{i,j,k}$.

– множество, составленное из тензоров $\left[N^{EC}_{УИК}\right]_{i,j,k}$:

$$N^{EC}_{УИК} = \bigcup_{i=1}^{N^{EC}_{ИК}} \bigcup_{j=1}^{\left[N^{EC}_{ТИК}\right]_i} \bigcup_{k=1}^{\left[N^{EC}_{УИК}\right]_{i,j}} \left[N^{EC}_{УИК}\right]_{i,j,k}.$$

Поясним введенные обозначения следующими примерами.

1. «Виртуальные» выборы проводились в стране с избирательной системой, имеющей следующую структуру: ЦИК, создавший 3 ИК, далее в каждой ИК – 2 ТИК, и затем в каждой ТИ – 2 УИК. Следовательно, на уровнях:

1) ЦИК и ИК:

$$N^{EC}_{ЦИК} = 3,\ N^{EC}_{ИК} = (1,1,1),\ Name_{\langle ИК\rangle} = \{ИК_1, ИК_2, ИК_3\},\ N^{EC}_{ТИК} = (2,2,2);$$

2) ТИК:

$$\left[N^{EC}_{ТИК}\right]_{1,1} = 2, \left[N^{EC}_{ТИК}\right]_{1,2} = 2, \left[N^{EC}_{ТИК}\right]_{2,1} = 2, \left[N^{EC}_{ТИК}\right]_{2,2} = 2, \left[N^{EC}_{ТИК}\right]_{3,1} = 2, \left[N^{EC}_{ТИК}\right]_{3,2} = 2;$$

$$Name_{\langle ТИК\rangle} = \bigcup_{i=1}^{3} \bigcup_{j=1}^{\left[N^{EC}_{ТИК}\right]_i} \left[Name_{\langle ИК\rangle}\right]_i - \left[Name_{\langle ТИК\rangle}\right]_j =$$

$$\{ИК_1.ТИК_1, ИК_1.ТИК_2, ИК_2.ТИК_1, ИК_2.ТИК_2, ИК_3.ТИК_1, ИК_3.ТИК_2\};$$

3) УИК:

$$\left[N^{EC}_{УИК}\right]_{1,1,1} = 2, \left[N^{EC}_{УИК}\right]_{1,1,2} = 2, \left[N^{EC}_{УИК}\right]_{1,2,1} = 2, \left[N^{EC}_{УИК}\right]_{1,2,2} = 2,$$

$$\left[N^{EC}_{УИК}\right]_{2,1,1} = 2, \left[N^{EC}_{УИК}\right]_{2,1,2} = 2, \left[N^{EC}_{УИК}\right]_{2,2,1} = 2, \left[N^{EC}_{УИК}\right]_{2,2,2} = 2,$$

$$\left[N^{EC}_{УИК}\right]_{3,1,1} = 2, \left[N^{EC}_{УИК}\right]_{3,1,2} = 2, \left[N^{EC}_{УИК}\right]_{3,2,1} = 2, \left[N^{EC}_{УИК}\right]_{3,2,2} = 2,$$

$$Name_{\langle УИК\rangle} = \bigcup_{i=1}^{3} \bigcup_{j=1}^{\left[N^{EC}_{ТИК}\right]_i} \bigcup_{k=1}^{\left[N^{EC}_{УИК}\right]_{i,j}} \left[Name_{\langle ИК\rangle}\right]_i - \left[Name_{\langle ТИК\rangle}\right]_j - \left[Name_{\langle УИК\rangle}\right]_k =$$

$$\{ИК_1.ТИК_1.УИК_1, ИК_1.ТИК_1.УИК_2, ИК_1.ТИК_2.УИК_1, ИК_1.ТИК_2.УИК_2,$$
$$ИК_2.ТИК_1.УИК_1, ИК_2.ТИК_1.УИК_2, ИК_2.ТИК_2.УИК_1, ИК_2.ТИК_2.УИК_2,$$
$$ИК_3.ТИК_1.УИК_1, ИК_3.ТИК_1.УИК_2, ИК_3.ТИК_2.УИК_1, ИК_3.ТИК_2.УИК_2\}.$$

Таким образом, мощности множеств, состоящих из описанных выше структур составляют:

$$\left|N^{EC}_{ИК}\right| = 3,\ \left|N^{EC}_{ТИК}\right| = 3,\ \left|Name_{\langle ИК\rangle}\right| = 3,\ \left|N^{EC}_{ТИК}\right| = 6,\ \left|Name_{\langle ТИК\rangle}\right| = 6,\ \left|N^{EC}_{УИК}\right| = 12,$$
$$\left|Name_{\langle УИК\rangle}\right| = 12.$$

2. «Виртуальные» выборы проводились в стране с избирательной системой, имеющей

следующую структуру: ЦИК, создавший 3 ИК, далее в каждой в ИК № 1 созданы– одна ТИК, в ИК № 2 – две ТИК, в ИК № 3 –три ТИК и далее в каждой из ТИК – две УИК. Следовательно, на уровнях:

1) ЦИК и ИК:

$N_{ЦИК}^{EC}=3,\ N_{ИК}^{EC}=(1,1,1),\ Name_{\langle ИК\rangle}=\{ИК_1,ИК_2,ИК_3\},\ N_{ТИК}^{EC}=(1,2,3);$

2) ТИК:

$\left[N_{ТИК}^{EC}\right]_{1,1}=1,\left[N_{ТИК}^{EC}\right]_{2,1}=2,\left[N_{ТИК}^{EC}\right]_{2,2}=2,\left[N_{ТИК}^{EC}\right]_{3,1}=3,\left[N_{ТИК}^{EC}\right]_{3,2}=3,\left[N_{ТИК}^{EC}\right]_{3,2}=3;$

$Name_{\langle ТИК\rangle}=\{ИК_1.ТИК_1,ИК_2.ТИК_1,ИК_2.ТИК_2,ИК_3.ТИК_1,ИК_3.ТИК_2,ИК_3.ТИК_2\}$

3) УИК:

$$\left[N_{УИК}^{EC}\right]_{1,1,1}=2,\left[N_{УИК}^{EC}\right]_{1,1,2}=2,$$
$$\left[N_{УИК}^{EC}\right]_{2,1,1}=2,\left[N_{УИК}^{EC}\right]_{2,1,2}=2,\left[N_{УИК}^{EC}\right]_{2,2,1}=2,\left[N_{УИК}^{EC}\right]_{2,2,2}=2,$$
$$\left[N_{УИК}^{EC}\right]_{3,1,1}=3,\left[N_{УИК}^{EC}\right]_{3,1,2}=3,\left[N_{УИК}^{EC}\right]_{3,2,1}=3,\left[N_{УИК}^{EC}\right]_{3,2,2}=3,\left[N_{УИК}^{EC}\right]_{3,3,1}=3,\left[N_{УИК}^{EC}\right]_{3,3,2}=3;$$

$$Name_{\langle УИК\rangle}=\{ИК_1.ТИК_1.УИК_1,ИК_1.ТИК_1.УИК_2,$$
$$ИК_2.ТИК_1.УИК_1,ИК_2.ТИК_1.УИК_2,ИК_2.ТИК_2.УИК_1,ИК_2.ТИК_2.УИК_2,$$
$$ИК_3.ТИК_1.УИК_1,ИК_3.ТИК_1.УИК_2,$$
$$ИК_3.ТИК_2.УИК_1,ИК_3.ТИК_2.УИК_2,$$
$$ИК_3.ТИК_3.УИК_1,ИК_3.ТИК_3.УИК_2\}.$$

Таким образом, в рассматриваемом случае мощности множеств $\left|Name_{\langle ИК\rangle}\right|$, $\left|N_{ТИК}^{EC}\right|$, $\left|Name_{\langle ТИК\rangle}\right|$, $\left|N_{УИК}^{EC}\right|$, $\left|Name_{\langle УИК\rangle}\right|$ оказываются аналогичными мощностям, изученных ранее множеств: $\left|N_{ТИК}^{EC}\right|=3,$ $\left|Name_{\langle ИК\rangle}\right|=3,\left|N_{ТИК}^{EC}\right|=6,\ \left|Name_{\langle ТИК\rangle}\right|=6,\ \left|N_{УИК}^{EC}\right|=12,\ \left|Name_{\langle УИК\rangle}\right|=12.$

По аналогии с введенными параметрами электорального процесса обозначим.

1) На уровне УИК:

– число, зарегистрированных в (i,j,k)-ой УИК с названием $ИК_i.ТИК_j.УИК_k$:

$\left[N_{УИК}^{ER}\right]_{i,j,k},\ i=\overline{1,N_{ИК}^{EC}},\ j=\overline{1,\left[N_{ИК}^{EC}\right]_i},\ k=\overline{1,\left[N_{ИК}^{EC}\right]_{i,j}};$

– множество, составленное из тензоров $\left[N_{УИК}^{ER}\right]_{i,j,k}$:

$$N_{УИК}^{ER}=\bigcup_{i=1}^{N_{ИК}^{EC}}\bigcup_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\bigcup_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{ER}\right]_{i,j,k};$$

– количество избирателей, проголосовавших в (i,j,k)-ой УИК с названием $ИК_i.ТИК_j.УИК_k$, $\left[N_{УИК}^{V}\right]_{i,j,k}$;

– количество избирателей, проголосовавших в (i,j,k)-ой УИК с названием $ИК_i.ТИК_j.УИК_k$ за m-го кандидата (партию), $\left[N_{УИК}^{V}\right]_{i,j,k}^{\langle m\rangle}$, $m=\overline{1,N_C}$, (N_C– число кандидатов (партий), принявших участие в выборах).

2) На уровне ТИК:

– число избирателей, зарегистрированных в (i,j)-ой ТИК с названием $ИК_i.ТИК_j$, $\left[N_{ТИК}^{ER}\right]_{i,j}=$

$$=\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{ER}\right]_{i,j,k};$$

– число избирателей, проголосовавших в (i,j)-ой ТИК с названием $ИК_i.ТИК_j$, $\left[N_{ТИК}^{V}\right]_{i,j}=$

$$=\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{V}\right]_{i,j,k};$$

– число избирателей, проголосовавших в (i,j)-ой ТИК с названием $ИК_i.ТИК_j$ за m-го кандидата: $\left[N_{ТИК}^{V}\right]_{i,j}^{\langle m\rangle}=\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{V}\right]_{i,j,k}^{\langle m\rangle},\ \sum_{m=1}^{N_C}\left[N_{ТИК}^{V}\right]_{i,j,m}=\left[N_{ТИК}^{V}\right]_{i,j}.$

3) На уровне ИК:

– число избирателей, зарегистрированных в i-ой ИК с названием $ИК_i$:

$$\left[N_{ИК}^{ER}\right]_i=\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\left[N_{ТИК}^{ER}\right]_{i,j}=\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{ER}\right]_{i,j,k};$$

– число избирателей, проголосовавших в i-ой ИК с названием $ИК_i$,

$$\left[N_{ИК}^{V}\right]_i=\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\left[N_{ТИК}^{V}\right]_{i,j}=\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{V}\right]_{i,j,k};$$

– число избирателей, проголосовавших в i-ой ИК с названием $ИК_i$ за m-го кандидата,

$$\left[N_{ИК}^{V}\right]_i^{\langle m\rangle}=\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\left[N_{ТИК}^{V}\right]_{i,j}^{\langle m\rangle}=\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{V}\right]_{i,j,k}^{\langle m\rangle}.$$

4) На уровне ЦИК:

– число зарегистрированных избирателей

$$N_{ЦИК}^{ER}=\sum_{i=1}^{N_{ЦИК}^{EC}}\left[N_{ИК}^{ER}\right]_i=\sum_{i=1}^{N_{ЦИК}^{EC}}\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\left[N_{ТИК}^{ER}\right]_i=\sum_{i=1}^{N_{ЦИК}^{EC}}\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{ER}\right]_{i,j,k};$$

– число избирателей, принявших участие в выборах

$$N_{ЦИК}^{V}=\sum_{i=1}^{N_{ЦИК}^{EC}}\left[N_{ИК}^{V}\right]_i=\sum_{i=1}^{N_{ЦИК}^{EC}}\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\left[N_{ТИК}^{V}\right]_i=\sum_{i=1}^{N_{ЦИК}^{EC}}\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{V}\right]_{i,j,k};\quad(1)$$

– число избирателей, проголосовавших за m-го кандидата,

$$\left[N_{ЦИК}^{V}\right]^{\langle m\rangle}=\sum_{i=1}^{N_{ЦИК}^{EC}}\left[N_{ИК}^{V}\right]_i^{\langle m\rangle}=\sum_{i=1}^{N_{ЦИК}^{EC}}\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\left[N_{ТИК}^{V}\right]_{i,j}^{\langle m\rangle}=\sum_{i=1}^{N_{ЦИК}^{EC}}\sum_{j=1}^{\left[N_{ТИК}^{EC}\right]_i}\sum_{k=1}^{\left[N_{УИК}^{EC}\right]_{i,j}}\left[N_{УИК}^{V}\right]_{i,j,k}^{\langle m\rangle}.\quad(2)$$

Таким образом, структура ЭД, публикуемых после проведения выборов, на уровнях ЦИК, ИК, ТИК, УИК задаются кортежами:

$$\left\langle N_{ЦИК}^{EC},N_{ЦИК}^{V},\left[N_{ЦИК}^{V}\right]^{\langle m\rangle}\right\rangle,\ \left\langle N_{ИК}^{EC},Name_{\langle ИК\rangle},N_{ИК}^{V},\left[N_{ИК}^{V}\right]^{\langle m\rangle}\right\rangle,$$
$$\left\langle N_{ТИК}^{EC},Name_{\langle ТИК\rangle},N_{ТИК}^{V},\left[N_{ТИК}^{V}\right]^{\langle m\rangle}\right\rangle,\ \left\langle N_{УИК}^{EC},Name_{\langle УИК\rangle},N_{УИК}^{V},\left[N_{УИК}^{V}\right]^{\langle m\rangle}\right\rangle,$$

соответственно. При этом:

1) на уровне ЦИК количественные показатели $N_{ЦИК}^{EC},N_{ЦИК}^{V},\left[N_{ЦИК}^{V}\right]^{\langle m\rangle},\ m=\overline{1,N_C}$ являются скалярными величинами;

2) на уровне ИК количественные показатели $N_{ИК}^{EC},N_{ИК}^{V},\left[N_{ИК}^{V}\right]^{\langle m\rangle}$ являются множествами, составленными из векторов размерности $N_{ЦИК}^{EC}\times 1$, $Name_{\langle ИК\rangle}$ – множество, составленное из названий ИК $\left(\left\{ИК_1,ИК_2,\ldots,ИК_{N_{ИК}^{EC}}\right\}\right)$;

3) на уровне ТИК количественные показатели $N_{ТИК}^{EC},N_{ТИК}^{V}$, являются множествами, составленными из матриц $\left[N_{ТИК}^{EC}\right]_{i,j}$, $\left[N_{ТИК}^{V}\right]_{i,j}$, $\left[N_{ТИК}^{V}\right]_{i,j}^{\langle m\rangle}$, $i=\overline{1,N_{ИК}^{EC}}$, $j=\overline{1,\left[N_{ТИК}^{EC}\right]_i}$, $Name_{\langle ТИК\rangle}$ – множество составленное из записей типа $\left\langle ИК_i.ТИК_j\right\rangle$;

4) на уровне УИК количественные показатели $N_{УИК}^{EC},N_{УИК}^{V},\left[N_{УИК}^{V}\right]^{\langle m\rangle}$ являются множествами, составленными из тензоров $\left[N_{ТИК}^{EC}\right]_{i,j,k}$, $\left[N_{ТИК}^{V}\right]_{i,j,k}$, $\left[N_{ТИК}^{V}\right]_{i,j,k}^{\langle m\rangle}$, $i=\overline{1,N_{ИК}^{EC}}$, $j=\overline{1,\left[N_{ТИК}^{EC}\right]_i}$, $k=\overline{1,\left[N_{УИК}^{EC}\right]_{i,j}}$.

На основе использования описанных выше ЭД вычисляют следующие ЭП.

1. Явка избирателей на выборы на уровнях ЦИК, ИК, ТИК, УИК: $\alpha_{ЦИК} = \frac{N^V_{ЦИК}}{N^{ER}_{ЦИК}}$, $[\alpha_{ИК}]_i = \frac{[N^V_{ИК}]_i}{[N^{ER}_{ИК}]_i}$, $[\alpha_{ТИК}]_{i,j} = \frac{[N^V_{ИК}]_{i,j}}{[N^{ER}_{ИК}]_{i,j}}$, $[\alpha_{ТИК}]_{i,j,k} = \frac{[N^V_{ИК}]_{i,j,k}}{[N^{ER}_{ИК}]_{i,j,k}}$ соответственно.

2. Доля голосов избирателей проголосовавших на выборах на уровнях ЦИК, ИК, ТИК, УИК за m-го кандидата: $[\gamma_{ЦИК}]^{\langle m\rangle} = \frac{[N^V_{ЦИК}]^{\langle m\rangle}}{N^V_{ЦИК}}$, $[\gamma_{ИК}]^{\langle m\rangle}_i = \frac{[N^V_{ИК}]^{\langle m\rangle}_i}{[N^V_{ИК}]_i}$, $[\gamma_{ТИК}]^{\langle m\rangle}_{i,j} = \frac{[N^V_{ТИК}]^{\langle m\rangle}_{i,j}}{[N^V_{ИК}]_{i,j}}$, $[\gamma_{ТИК}]^{\langle m\rangle}_{i,j,k} = \frac{[N^V_{ТИК}]^{\langle m\rangle}_{i,j,k}}{[N^V_{ИК}]_{i,j,k}}$.

Таким образом, ЭП на уровнях ЦИК, ИК, ТИК и УИК задаются кортежами:

$$\langle \alpha_{ЦИК}, [\gamma_{ЦИК}]^{\langle m\rangle} \rangle, \quad \langle [\alpha_{ИК}]_i, [\gamma_{ИК}]^{\langle m\rangle}_i \rangle, \quad \langle [\alpha_{ИК}]_{i,j}, [\gamma_{ИК}]^{\langle m\rangle}_{i,j} \rangle, \quad \langle [\alpha_{ИК}]_{i,j,k}, [\gamma_{ИК}]^{\langle m\rangle}_{i,j,k} \rangle,$$

$$\alpha_{ЦИК}, [\alpha_{ИК}]_i, [\alpha_{ТИК}]_{i,j}, [\alpha_{УИК}]_{i,j,k} \in [0,1], \qquad \gamma_{ЦИК}, [\gamma_{ИК}]_i, [\gamma_{ТИК}]_{i,j}, [\gamma_{УИК}]_{i,j,k} \in [0,1],$$

соответственно. При этом, очевидно, что, в общем случае,

$$\alpha_{ЦИК} \neq [\alpha_{ИК}]_i \neq [\alpha_{ТИК}]_{i,j} \neq [\alpha_{УИК}]_{i,j,k},$$

$$[\gamma_{ЦИК}]^{\langle m\rangle} \neq [\gamma_{ИК}]^{\langle m\rangle}_i \neq [\gamma_{ТИК}]^{\langle m\rangle}_{i,j} \neq [\gamma_{ТИК}]^{\langle m\rangle}_{i,j,k}.$$

Отметим, что в случае проведения «абсолютно» честных выборов и отсутствия возможных непреднамеренных (технических) ошибок, допускаемых членами ЦИК, ИК, ТИК, УИК, соотношения (1), (2) выполняются точно. Непреднамеренные ошибки, допущенные членами избирательных комиссий различных уровней, будут приводить к возникновению в ЭД «случайного шума» не выходящего за пределы среднестатистической статистической погрешности. При наличии преднамеренно внесенных аномалий в ЭД (фальсификации ЭД) соотношения (1), (2) выполняться заведомо не будут.

2. АЛГОРИТМ ГЕНЕРАЦИИ МОДЕЛЬНЫХ ЭД

Результаты теоретико-множественного анализа ЭД и ЭП, изложенные в разделе 1, позволяют сделать выводы о том, что ЭД и вычисленные на их основе ЭП с точки зрения типов используемых для их представления чисел и природы данных чисел декомпозируются на следующие группы показателей.

Группа № 1 – целочисленные константы: $N^{EC}_{ЦИК}$, $[N^{EC}_{ИК}]_i$, $[N^{EC}_{ТИК}]_{i,j}$, $[N^{ER}_{УИК}]$, $i = \overline{1, N^{EC}_{ИК}}$, $j = \overline{1, [N^{EC}_{ТИК}]_i}$, $k = \overline{1, [N^{EC}_{УИК}]_{i,j}}$, N_C;

Группа № 2 – случайные целые числа $N^V_{ЦИК}$, $[N^V_{ИК}]_i$, $[N^V_{ТИК}]_{i,j}$, $[N^V_{УИК}]_{i,j,k}$, $i = \overline{1, N^{EC}_{ИК}}$, $j = \overline{1, [N^{EC}_{ТИК}]_i}$, $k = \overline{1, [N^{EC}_{УИК}]_{i,j}}$, $[N^V_{УИК}]^{\langle m\rangle}_{i,j,k}$, $m = \overline{1, N_C}$, значения которых определяются активностью избирателей;

Группа № 3 – случайные действительные числа $\alpha_{ЦИК}$, $[\alpha_{ИК}]_i$, $[\alpha_{ИК}]_{i,j}$, $[\alpha_{ИК}]_{i,j,k}$, $[\gamma_{ЦИК}]^{\langle m\rangle}$, $[\gamma_{ИК}]^{\langle m\rangle}_i$, $[\gamma_{ИК}]^{\langle m\rangle}_{i,j}$, $[\gamma_{ИК}]^{\langle m\rangle}_{i,j,k}$.

Отметим, что ЭП, отнесенные к группам № 2, 3, представляют собой случайные последовательности (СП), область значений которых ограничена. При этом, понятно, что для синтеза модельных ЭД (ЭД «виртуальных» выборов) на уровнях ТИК, ИК и ЦИК, достаточно, генерировать обсуждаемые СП на уровне УИК и далее вычислить значения ЭП на уровнях ТИК, ИК и ЦИК. Таким образом, алгоритм генерации модельных ЭД, достаточно очевиден.

1) Задать целочисленные значения констант, отнесенных к группе № 1.

2) Сгенерировать в соответствие с выбранными функциями (ФР) (выбор вида ФР и их параметров обсуждается в Разделе 3) целочисленные СП, содержащие значения $[N^{ER}_{УИК}]_{i,j,k}$, $[N^V_{УИК}]_{i,j,k}$, $[N^V_{УИК}]^{\langle m\rangle}_{i,j,k}$, $i = \overline{1, N^{EC}_{ИК}}$, $j = \overline{1, [N^{EC}_{ТИК}]_i}$, $k = \overline{1, [N^{EC}_{УИК}]_{i,j}}$, $m = \overline{1, N_C}$.

3) Вычислить значения ЭП на уровне ТИК: $[N^{ER}_{ТИК}]_{i,j}$, $[N^V_{ТИК}]_{i,j}$, $[N^V_{ТИК}]^{\langle m\rangle}_{i,j}$; уровне ИК: $[N^{ER}_{ИК}]_i$, $[N^V_{ИК}]_i$, $[N^V_{ИК}]^{\langle m\rangle}_i$; уровне ЦИК $N^V_{ЦИК}$, $[N^V_{ИК}]^{\langle m\rangle}$.

Для целей нашего исследования можно упростить обсуждаемую модель «виртуальных» выборов, предположив, что в них участвуют два кандидата (де-факто, это означает объединение ЭД и ЭП каждого кандидата, проигравшего выборы, в ЭД и ЭП «единого» кандидата, проигравшего выборы), а также синтезировать ЭД на уровне УИК, пересчитываемые далее ЭД на уровне ЦИК.

Модифицированный алгоритм реализуется выполнением следующей последовательности действий.

1. Задать число зарегистрированных УИК $N_{УИК}$.

2. Выбрать закон распределения и область рассеяния случайной величины (СВ) $[N^{ER}_{УИК}]_k$, $k = \overline{1, N_{УИК}}$.

3. Сгенерировать $N_{УИК}$ целых случайных чисел (СЧ) в соответствие с выбранными в п. 2 законом распределения и областью рассеяния – последовательность $[N^{ER}_{УИК}]_k$, $k = \overline{1, N_{УИК}}$.

4. Выбрать законы распределения и области рассеяния СВ $[\gamma_{УИК}]^{\langle 1\rangle}_k$, $[\gamma_{УИК}]^{\langle 2\rangle}_k$ так, чтобы $\left([\gamma_{УИК}]^{\langle 1\rangle}_k + [\gamma_{УИК}]^{\langle 2\rangle}_k\right) \le 1$, $k = \overline{1, N_{УИК}}$.

5. В соответствие с выбранными в п. 6 законами распределения и областью рассеяния сгенерировать действительные СП $\left\{[\gamma_{УИК}]^{\langle 1\rangle}_k\right\}$, $\left\{[\gamma_{УИК}]^{\langle 2\rangle}_k\right\}$, $k = \overline{1, N_{УИК}}$.

6. Вычислить число избирателей, проголосовавших за каждого из кандидатов, в k-ой УИК: $[N^V_{УИК}]^{\langle 1\rangle,\langle 2\rangle}_k = \mathrm{round}\left([\gamma_{УИК}]^{\langle 1\rangle,\langle 2\rangle}_k [N^{ER}_{УИК}]_k\right)$.

7. Вычислить число избирателей, принявших участие в выборах в k-ой УИК:

$$\left[N^{V}_{УИК}\right]_k = \text{round}\left(\left(\left[\gamma_{УИК}\right]^{\langle 1\rangle}_k + \left[\gamma_{УИК}\right]^{\langle 1\rangle}_k\right)\left[N^{ER}_{УИК}\right]_k\right).$$

Вопросы, связанные с выбором математической модели ПР и ФР синтезированных модельных ЭД и их параметров обсуждаются в следующем разделе статьи.

3. МАТЕМАТИЧЕКАЯ МОДЕЛЬ ФУНЦИЙ РАСПРЕДЕЛЕНИЙ И ПЛОТНОСТЕЙ РАСПРЕДЕЛЕНИЙ СИНТЕЗИРОВАННЫХ ЭЛЕКТОРАЛЬНЫХ ДАННЫХ И ЭЛЕКТОРАЛЬНЫХ ПОКАЗАТЕЛЕЙ

Для практического использования модифицированного алгоритма синтеза ЭД, рассмотренного в предыдущем разделе статьи, необходимо выбрать вид и параметры ПР, используемой для синтеза СП $\left[N^{ER}_{УИК}\right]_k$, $\left[N^{V}_{УИК}\right]_k$, $\left[N^{ER}_{УИК}\right]^{\langle 1\rangle,\langle 2\rangle}_k$, $\left[\mu_{УИК}\right]^{\langle 1\rangle,\langle 2\rangle}_k$, $\left[N^{V}_{УИК}\right]^{\langle 1\rangle,\langle 2\rangle}_j$, $k=\overline{1,N_{УИК}}$.

При этом следует учитывать:

1) СП $\left[N^{ER}_{УИК}\right]_j$, $\left[N^{V}_{УИК}\right]_j$, $\left[N^{ER}_{УИК}\right]^{\langle i\rangle}_j$, $\left[N^{V}_{УИК}\right]^{\langle i\rangle}_j$, $\left[\alpha^{\%}_{УИК}\right]_j$, $\left[\mu^{\%}_{УИК}\right]^{\langle 1\rangle,\langle 2\rangle}_j$, $\left[N^{V}_{УИК}\right]^{\langle 1\rangle,\langle 2\rangle}_j$, $j=\overline{1,N_{УИК}}$, $i=\overline{1,N_C}$, представляют собой выборки, извлеченные из генеральных совокупностей, у которых области определения ПР представляют собой отрезки конечной длины (ограниченная область рассеяния);

2) часть методов ЭК, основано на гипотезе, постулированной, но не доказанной математически, о том, что СП, составленные из ЭД и вычисленных на их основе ЭП, имеют нормальный закон распределения, поэтому обнаруживаемые отличия эмпирических ПР от нормального закона распределения ЭК, их авторы, как признак внесения преднамеренно созданных аномалий в ЭД;

3) статистические свойства СП, области значений членов которых ограничены, аналогичны статистическим свойствам одномерных случайных (броуновских) блужданий в ограниченной с двух сторон области рассеяния (см., [2–4], а также [5]), эквивалентно, статистическим свойствам СВ с ограниченной областью рассеяния.

Математическая модель ПР СВ с ограниченной областью рассеяния, построенная в соответствие с методом мнимых источников, представляется выражением (см., например, [6,7]):

$$f_{LAD}(x;x_0,\sigma,l) = A\left[\varphi(x;x_0,\sigma,l) + \sum_{g=0}^{\infty}\varphi^{\pm}_{2g+1}(x;x_0,\sigma,l) + \sum_{g=1}^{\infty}\varphi^{\pm}_{2g}(x;x_0,\sigma,l)\right], \quad (1)$$

где A – коэффициент, выбираемый из условия нормировки:

$$\int_{x_{\min}}^{x_{\max}} f_{LAD}(\xi;x_0,\sigma,l)\,d\xi = 1,$$

$$\varphi(x;x_0,\sigma) = \exp\left[-(x-x_0)^2/2\sigma^2\right],$$

$$\varphi^{\pm}_{2g+1}(x;x_0,\sigma,l) = \exp\left[-\left(x-x^{\pm}_{2g+1}\right)^2/2\sigma^2\right],$$

$$\varphi^{\pm}_{2g}(x;x_0,\sigma,l) = \exp\left[-\left(x-x^{\pm}_{2g}\right)^2/2\sigma^2\right],$$

здесь x_0 – координата порождающего источника, ПР которого описывается функцией $\varphi(x;x_0,\sigma,l)$, $[x_{\min},x_{\max}]$, – область рассеяния СВ, $l=x_{\max}-x_{\min}$ – размер области рассеяния, σ – параметр распределения, $x^{\pm}_{2g+1}, x^{\pm}_{2g}$ – координаты мнимых источников, вычисляемые по формулам:

$$x^{\pm}_{2g} = \pm 4gl + x_0, \quad x^{\pm}_{2g+1} = \pm(4g+2)l - x_0,$$

где $g = 0,1,....$

Соответственно, ФР СВ величины с ограниченной областью рассеяния вычисляется по формуле:

$$F_{LAD}(x;x_0,\sigma,l) = \int f_{LAD}(\xi;x_0,\sigma,l)\,d\xi = 1. \quad (2)$$

На практике, удовлетворительная точность вычисления ПР (10) и ФР (11) достигается при $g = 5$ [6].

Описания алгоритмов для оценки параметров ФР (10) и ПР (2) СВ с ограниченной областью рассеяния, моделирования случайных блужданий в неограниченных и ограниченных областях рассеяния, генерации СВ в соответствие с (2) приведены в [6, 7]. Их программные реализации размещены в программной MATLAB-библиотеке ES&RP [7], которая была использована авторами для синтеза ЭД, опубликованных по результатам «виртуальных» выборов, обсуждаемых далее.

Напомним, что в задачах оценки надежности технических систем и точности производства [8–11] используется известное в прикладной статистике усеченное нормальное распределение (УНР), которое имеет формальное сходство с рассмотренным выше распределением СВ с ограниченной областью рассеяния. Однако, у обсуждаемых распределений оказываются принципиально отличными способы генерации СВ и, соответственно, математические модели ФР. При генерации СП, ПР которых соответствуют УНР, используют алгоритм, реализующийся выполнением следующей последовательности действий.

1. Генерация в соответствие с нормальным законом распределения СП $N(\mu,\sigma),\text{СП}\{x\}$.

2. Извлечение из СП $\{x\}$ СП $\{x'\}$, члены которой удовлетворяют следующему условию:

$$x_{\min} \le x'_k \le x_{\max},$$

где $x_{\min}, x_{\max}$ – точки усечения нормального распределения.

ПР УНР $N'(\mu,\sigma,x_{\min},x_{\max})$ вычисляется по формуле:

$$f_{LIM}(x;\mu,\sigma,x_{\min},x_{\max}) = \frac{1}{\sigma}\frac{\varphi\left(\frac{x-\mu}{\sigma}\right)}{F\left(\frac{x_{\max}-\mu}{\sigma}\right) - F\left(\frac{x_{\min}-\mu}{\sigma}\right)},$$

где $\varphi(\xi)=\frac{1}{\sqrt{2\pi}}e^{-\frac{1}{2}\xi^2}$, $F(x)=\int_{-\infty}^{x}\varphi(\xi)d\xi$ – функция Лапласа, μ,σ – параметры исходного (порождающего) нормального распределения.

ФР УНР $N'(\mu,\sigma,x_{\min},x_{\max})$ вычисляется по формуле:

$$F_{LIM}(x;\mu,\sigma,x_{\min},x_{\max})=A\int_{-\infty}^{x}f_{LIM}(x;\mu,\sigma,x_{\min},x_{\max})d\xi,$$

где A – нормировочный коэффициент, обеспечивающий выполнение условия

$$A\int_{-\infty}^{\infty}f_{LIM}(x;\mu,\sigma,x_{\min},x_{\max})d\xi=1.$$

4. АНАЛИЗ РЕЗУЛЬТАТОВ ПРИМЕНИЯ МЕТОДОВ ЭК К СИНТЕЗИРОВАННЫМ ЭД И ЭП

4.1. ПАРАМЕТРЫ ГЕНЕРАЦИИ МОДЕЛЬНЫХ ДАННЫХ

Параметры имитационной модели, использованные для генерации модельных ЭД в предположении, что в выборах принимали участие два кандидата, представлены в таблице 1.

Таблица 1

Параметры имитационной модели, сгенерировавшей модельные ЭД

Название параметра	Обозначение параметра	Значение
Параметры, используемые для генерации числа избирателей, зарегистрированных в данных УИК		
Число участковых избирательных комиссий	$N_{УИК}$	$9\cdot10^4$
Математическое ожидание порождающего нормального распределения	μ	1017
Дисперсия порождающего нормального распределения	σ	502
Левая граница области рассеяния	a_1	6
Правая граница области рассеяния	a_2	10000
Параметры, используемые для генерации доли избирателей, проголосовавших в данной УИК за победившего на выборах кандидата		
Математическое ожидание порождающего нормального распределения	$\mu^{\langle1\rangle}$	0,60
Дисперсия порождающего нормального распределения	σ_1^1	0,07
Левая граница области рассеяния	a_1^1	0,51
Правая граница области рассеяния	a_2^1	1,00
Параметры, используемые для генерации доли избирателей, проголосовавших в данной УИК за проигравшего на выборах кандидата		
Математическое ожидание порождающего нормального распределения	$\mu^{\langle2\rangle}$	$\left(1-z_j\right)/2$ *
Дисперсия порождающего нормального распределения	$\sigma^{\langle2\rangle}$	0,01
Левая граница области рассеяния	$a_1^{\langle2\rangle}$	0,05
Правая граница области рассеяния	$a_2^{\langle2\rangle}$	$1-z_j$ *

* z_j – доля избирателей, проголосовавших на i-ом участке за победителя выборов.

Отметим, что выбор значений параметров модели, представленных в таблице 3, обеспечил выполнение условия $\left[\gamma_{УИК}\right]_i^{\langle1\rangle}+\left[\gamma_{УИК}\right]_i^{\langle2\rangle}\in[0,9;1,0]$.

Вычисленные на основе использования модельных ЭД значения левой и правой границ интервалов изменения описанных выше ЭП, а также их средние значения приведены в таблице 2. Также отметим, что значения оценок ЭП, вычисленных на основе анализа модельных ЭД, оказались сравнимыми с соответствующими ЭП, опубликованным ЦИК РФ по результатам Выборов–2018 г. [12]. Например, число зарегистрированных избирателей, имевших право участвовать в «виртуальных» выборах, составило (соответственно, Выборах–2018 – 109 008 428), число избирателей, принявших участие в «виртуальных» выборах, составило (соответственно, в Выборах–2018 – 73 578 992,), явка избирателей на «виртуальные» выборы составила 80,31 % (соответственно, на Выборы–2018 – 67,54 %). В этой связи, был сделан вывод о том, что сгенерированные модельные ЭД, в которые заведомо не вносилось каких-либо изменений, можно использовать для оценки адекватности методов ЭК.

Таблица 2

Оценки минимального, среднего и максимального значений ЭП

ЭП	Минимальное значение	Среднее значение*	Максимальное значение
$\left[N_{УИК}^{ER}\right]_j$	11	1023	3179
$\left[\alpha_{УИК}^{\%}\right]_j^{\langle 1\rangle}$	0,5102	0,5995	0,8844
$\left[\alpha_{УИК}^{\%}\right]_j^{\langle 2\rangle}$	0,1001	0,1124	0,1703
$\left[N_{УИК}^{V}\right]_j^{\langle 1\rangle}$	11	621	2278
$\left[N_{УИК}^{V}\right]_j^{\langle 2\rangle}$	1	117	421
$\left[N_{УИК}^{V}\right]_j$	7	738	2589
$\left[\gamma_{УИК}^{\%}\right]_j$	0,6060	0,7205	0,9958

* средние значения СП, составленных из значений соответствующего ЭП, вычислялись по формуле:

$$\bar{x} = \int_{x_{\min}}^{x_{\max}} \xi\, \hat{p}(\xi)\, d\xi,$$

где $\hat{p}(\xi)$ – аппроксимация Розенблатта-Парзена ПР соответствующей СП (см., например [13]).

4.2. АНАЛИЗ ФР ЦИФР В ЭП

Методы ЭК, основанные на анализе ФР, описаны в [14–21]. В ходе проведенных исследований были использованы СП, составленные из следующих ЭП: $\left\{\left[\gamma_{УИК}\right]_j^{\langle 1\rangle}\right\}$, $\left\{\left[\gamma_{УИК}\right]_j^{\langle 2\rangle}\right\}$, $\left\{\left[\alpha_{УИК}\right]_j\right\}$, значения членов которых округленные с точностью до второй цифры после запятой преобразовывались в целые числа:

$\left[\Gamma_{УИК}^{\langle 1\rangle}\right]_j = \text{round}\left(\left[\gamma_{УИК}\right]_j^{\langle 1\rangle} \cdot 10^4\right) \Big/ 10^2$ – (показатель № 1);

$\left[\Gamma_{УИК}^{\langle 2\rangle}\right]_j = \text{round}\left(\left[\gamma_{УИК}\right]_j^{\langle 2\rangle} \cdot 10^4\right) \Big/ 10^2$ – (показатель № 2);

$\left[A_{УИК}^{\langle 1\rangle}\right]_j = \text{round}\left(\left[\alpha_{УИК}\right]_j \cdot 10^4\right) \Big/ 10^2$ – (показатель № 3).

Далее был проведен анализ встречаемости цифр d в последнем разряде показателей (ПРП) № 1–3 $\left(\left[d_{ПРП}\right]^{\langle k\rangle}, k = \overline{1,3}\right)$,, результаты которого представлены в таблице 3, из которой видно, что частоты встречаемости цифр $\left[d_{ПРП}\right]^{\langle 1\rangle}, \left[d_{ПРП}\right]^{\langle 2\rangle}, \left[d_{ПРП}\right]^{\langle 3\rangle}$ оказались СВ с ограниченными областями рассеяния: $\left[d_{ПРП}\right]^{\langle 1\rangle} \in \in [8591,9440],, \left[d_{ПРП}\right]^{\langle 2\rangle} \in [8727,9579],, \left[d_{ПРП}\right]^{\langle 2\rangle} \in \in [8755,9687]$.

Данный результат, как очевидно, оказался отличным от результата, ожидавшегося, априори, – 9000 [14–21]. В связи с тем, что совокупности значений $\left[d_{ПРП}\right]^{\langle 1\rangle}, \left[d_{ПРП}\right]^{\langle 2\rangle}, \left[d_{ПРП}\right]^{\langle 3\rangle}$ оказались некоторыми СП, с помощью критерия χ^2 была проверена статистическая гипотеза о соответствии их ФР и ПР, априори, ожидаемому равномерному закону распределения. Значения критерия χ^2 для обсуждаемых СП оказались равными $\left[\chi^2\right]^{\langle 1\rangle} = 117,067$, $\left[\chi^2\right]^{\langle 2\rangle} = 62,08$, $\left[\chi^2\right]^{\langle 3\rangle} = 91,35$. Так как $\left[\chi^2\right]^{\langle 1\rangle,\langle 2\rangle,\langle 3\rangle} >$

Таблица 3

Результаты анализа распределений последней цифры ЭП

Цифра (d)	$\left[d_{ПРП}\right]^{\langle 1\rangle}$	$\left[d_{ПРП}\right]^{\langle 2\rangle}$	$\left[d_{ПРП}\right]^{\langle 3\rangle}$
0	9038	8926	9086
1	9312	9579	9070
2	9440	8999	8755
3	8612	8983	9181
4	8659	8937	8609
5	8892	9089	9095
6	9324	9197	8901
7	9384	8738	9687
8	8591	8727	8799
9	8749	8826	8818

$> \chi^2_{теор}(9), = 15,51$ гипотеза о равномерном законе распределении изучаемых случайных последовательностей была отвергнута.

Следовательно, исследованный метод ЭК, обнаруживший признаки преднамеренно внесенных аномалий в модельные ЭД, не может использоваться для анализа реальных ЭД.

Результаты анализа распределений двух одинаковых цифр, находящихся в последнем и предпоследнем разрядах показателей (ПиПрРП) № 1–3 , $\left[d_{ПиПрРП}\right]^{\langle 1\rangle}$, $\left[d_{ПиПрРП}\right]^{\langle 2\rangle}$, $\left[d_{ПиПрРП}\right]^{\langle 3\rangle}$ представлены в таблице 4, из которой видно, что частоты встречаемости пар одинаковых цифр в исследуемых ЭП $\left[d_{ПиПрРП}\right]^{\langle 1\rangle}$, $\left[d_{ПиПрРП}\right]^{\langle 2\rangle}$, $\left[d_{ПиПрРП}\right]^{\langle 3\rangle}$ оказались СВ с ограниченными областями рассеяния: $\left[d_{ПиПрРП}\right]^{\langle 1\rangle} \in [705,1066]$,, $\left[d_{ПиПрРП}\right]^{\langle 2\rangle} \in [682,1069]$, $\left[d_{ПиПрРП}\right]^{\langle 3\rangle} \in [850,1048]$.

Таблица 4

Результаты анализа распределений пар одинаковых последних цифр

Пары цифра	$\left[d_{ПиПрРП}\right]^{\langle 1\rangle}$	$\left[d_{ПиПрРП}\right]^{\langle 2\rangle}$	$\left[d_{ПиПрРП}\right]^{\langle 2\rangle}$
00	920	721	920
11	935	1030	885
22	912	1069	850
33	1039	897	950
44	705	899	895
55	797	835	1048
66	1066	847	910
77	774	798	1041
88	884	784	943
99	803	682	912

Данный результат, как очевидно, оказался отличным от результата ожидавшегося, априори, – 900 [14–21]. В связи с тем, что совокупности значений $\left[d_{ПиПрРП}\right]^{\langle 1\rangle}$, $\left[d_{ПиПрРП}\right]^{\langle 2\rangle}$, $\left[d_{ПиПрРП}\right]^{\langle 3\rangle}$ некоторыми СП с помощью критерия χ^2 была проверена статистическая гипотеза о соответствии их ФР и ПР равномерному, априори ожидаемому, закону распределения. Значения критерия χ^2 для обсуждаемых СП оказались равными: $\left[\chi^2\right]^{\langle 1\rangle} = 136,4878$, $\left[\chi^2\right]^{\langle 2\rangle} = 173,2552$, $\left[\chi^2\right]^{\langle 2\rangle} = 55,0311$, соответственно Так как $\left[\chi^2\right]^{\langle 1\rangle,\langle 2\rangle,\langle 3\rangle} > \chi^2_{теор}(9), = 15,51$ гипотеза о равномерном законе распределении изучаемых СП была отвергнута.

Следовательно, исследованные методы ЭК, обнаруживающие признаки преднамеренно внесенных аномалий в модельные ЭД, не могут использоваться для анализа реальных ЭД.

4.3 АНАЛИЗ РЕЗУЛЬТАТОВ ПРИМЕНЕНИЯ К МОДЕЛЬНЫМ ЭД МЕТОДОВ ЭК, ОСНОВАННЫХ НА АНАЛИЗЕ ФУНКЦИОНАЛЬНЫХ СВЯЗЕЙ МЕЖДУ ЭП

Рассмотрим зависимости $\left[\gamma_{УИК}\right]_k^{\langle 1\rangle} = f\left(\left[\gamma_{УИК}\right]_i\right)$, $\left[\gamma_{УИК}\right]_k^{\langle 2\rangle} = f\left(\left[\gamma_{УИК}\right]_i\right)$, представленные на рис. 2, которые в соответствие с методом С. Шпилькинаі [22–26] при отсутствии целенаправленно внесенных аномалий в ЭД должны аппроксимироваться прямыми параллельными оси абсцисс, и результаты их линейной аппроксимации, приведенные ниже.

Анализ приведенных выше результатов, позволяет сделать следующие выводы:

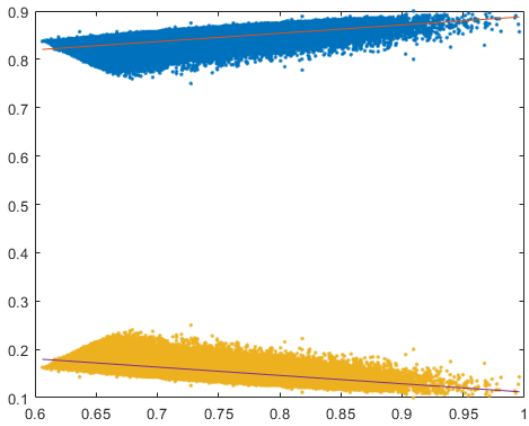

Рис. 2. Визуализация зависимостей $\left[\gamma_{УИК}\right]_k^{\langle 1\rangle} = f\left(\left[\gamma_{УИК}\right]_k\right)$ (вверху), $\left[\gamma_{УИК}\right]_k^{\langle 2\rangle} = f\left(\left[\gamma_{УИК}\right]_k\right)$ (снизу)

Количественные характеристики линейной аппроксимации зависимости $\left[\gamma_{УИК}\right]_k^{(1)} = f\left(\left[\gamma_{УИК}\right]_k\right)$

```
Linear regression model:
    y ~ 1 + x1
Estimated Coefficients:
                   Estimate        SE         tStat     pValue
                   ________    __________    _______    _______

    (Intercept)    0.71621     0.00057657    1242.2       0
    x1             0.17217     0.00079651    216.15       0

Number of observations: 90000, Error degrees of freedom: 89998
Root Mean Squared Error: 0.0147
R-squared: 0.342,  Adjusted R-Squared: 0.342
F-statistic vs. constant model: 4.67e+04, p-value = 0
```

Количественные характеристики линейной аппроксимации зависимости $\left[\gamma_{УИК}\right]_k^{(2)} = f\left(\left[\gamma_{УИК}\right]_i\right)$,

```
Linear regression model:
    y ~ 1 + x1
Estimated Coefficients:
                   Estimate        SE         tStat     pValue
                   ________    __________    _______    _______

    (Intercept)    0.71621     0.00057657    1242.2       0
    x1             0.17217     0.00079651    216.15       0

Number of observations: 90000, Error degrees of freedom: 89998
Root Mean Squared Error: 0.0147
R-squared: 0.342,  Adjusted R-Squared: 0.342
F-statistic vs. constant model: 4.67e+04, p-value = 0
Linear regression model:
    y ~ 1 + x1

Estimated Coefficients:
                   Estimate        SE          tStat     pValue
                   ________    __________    ________    _______

    (Intercept)     0.28379    0.00057657      492.2       0
    x1             -0.17217    0.00079651    -216.15       0

Number of observations: 90000, Error degrees of freedom: 89998
Root Mean Squared Error: 0.0147
R-squared: 0.342,  Adjusted R-Squared: 0.342
F-statistic vs. constant model: 4.67e+04, p-value = 0
```

– угловые коэффициенты прямых, аппроксимирующие зависимости $\left[\alpha_{УИК}\right]_i^1 = f\left(\left[\alpha_{УИК}\right]_i\right)$, $\left[\alpha_{УИК}\right]_i^2 = f\left(\left[\alpha_{УИК}\right]_i\right)$, статистических значимо отличаются от нуля, что свидетельствует о наличии линейной связи между анализируемыми показателями электорального процесса;

– доля голосов избирателей, проголосовавших за победителя выборов, при увеличении доли избирателей, принявших участие в выборах в данной УИК, линейно возрастает, в то время как доля избирателей, проголосовавших за кандидата, проигравшего выборы, линейно уменьшается.

Причины обусловившие полученные ре-

[i] С.А. Шпилькин 10.02.2023 включен Министерством юстиции Российской Федерации в реестр иностранных агентов в соответствие со статьей 7 Федерального закона от 14.07.2022 № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием».

зультаты, аналогичны причинам, позволившими отвергнуть метода Собянина-Суходольского в первой части статьи [1].

Таким образом, метод С. Шпилькина[i] в рассматриваемом случае совершил (в терминах теории обнаружения) ошибку второго рода.

Рассмотрим зависимость $\left[N^V_{УИК}\right]^{\langle 1\rangle}_k = f\left(\left[N^V_{УИК}\right]^{\langle 2\rangle}_k\right)$., представленную на рис. 3. (Напомним что в соответствие с методом А. Подлазова [28–30] при отсутствии аномалий, преднамеренно внесенных в ЭД, должна быть:

$$\left[N^V_{УИК}\right]^{\langle 1\rangle}_j = \eta\left[N^V_{УИК}\right]^{\langle 2\rangle}_j,$$

где $\eta = \text{const}$.) Случаи, в которых зависимость ЭД $\left[N^V_{УИК}\right]^{\langle 1\rangle}_j$ от ЭД $\left[N^V_{УИК}\right]^{\langle 2\rangle}_j$ отлична от линейной, интерпретируются автором обсуждаемого метода, как свидетельство искусственного увеличения $\left[N^V_{Level_k}\right]^{\langle 1\rangle}_j$ за счет уменьшения

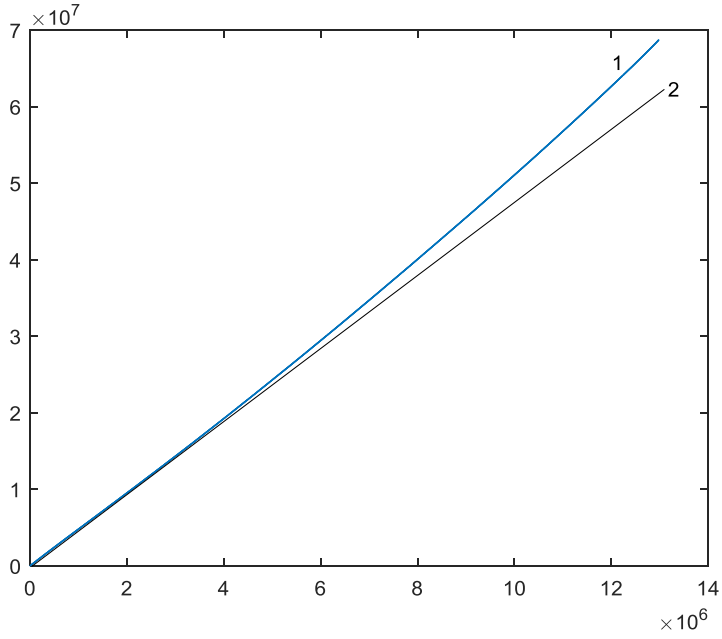

Рис. 3. Графики функций: $1 - \left[N^V_{УИК}\right]^{\langle 1\rangle}_k = f\left(\left[N^V_{УИК}\right]^{\langle 2\rangle}_k\right)$; $2 - \left[N^V_{УИК}\right]^{\langle 1\rangle}_K = \eta\left[N^V_{УИК}\right]^{\langle 2\rangle}_K$

$\left[N^V_{УИК}\right]^{\langle 2\rangle}_j$. Данный механизм фальсификации ЭД, по мнению А. Подлазова, используется, в первую очередь, на избирательных участках с высокой явкой избирателей.)

Из рисунка 3 видно, что зависимость $\left[N^V_{УИК}\right]^{\langle 1\rangle}_k = f\left(\left[N^V_{УИК}\right]^{\langle 2\rangle}_k\right)$, вычисленная на основе модельных заведомо нефальсифицированных ЭД, оказывается отличной от линейной. Таким образом, метод А. Подлазова в рассматриваемом случае в рассматриваемом случае совершил ошибку второго рода (в терминах теории обнаружения).

Следовательно, методы ЭК, рассмотренные в данном разделе, не должны применяться для выявления преднамеренно внесенных аномалий в ЭД.

Заключение

Выборы, призванные быть в демократических обществах инструментом мирного и легального решения разногласий между участниками политического процесса, зачастую, напротив, сами оказываются катализатором активизации противоборства политических сил, что подтверждается многочисленными примерами из истории история проведения выборов в конце XX – начале XXI в. в РФ, странах постсоветского пространства, других зарубежных странах. В ходе последующего обсуждения результатов проведенных выборов во многих случаях проигравшие кандидаты и их сторонники, исходя из собственных (зачастую субъективных) представлений о «действительных» электоральных настроениях, ставят под сомнение честность проведенных выборов, несмотря на принимаемые меры по противодействию потенциально возможной фальсификации ЭД, членами избирательных комиссий, в том числе: привлечение для мониторинга процесса голосования и подсчета голосов независимых наблюдателей (в том числе граждан других государств); оснащение избирательных участков средствами аудио- и видеофиксации; проведение социологических опросов

накануне и экзиполлов в ходе проведения выборов.

Однако, оказывается, что применение перечисленных выше организационных и организационно-технических мер, а также наличие законодательных норм, регулирующих избирательный процесс, по мнению известных экспертов, занимающихся интерпретацией результатов проводимых выборов и референдумов (в первую очередь в РФ), отнюдь не являются гарантией недопущения масштабных фальсификаций электоральных данных в пользу победителя выборов. Выявить подобные факты призваны методы ЭК, основанные на сравнении тех или иных статистических характеристик ЭД и вычисляемых на их основе ЭП с некоторыми эталонами, которые, как показали результаты проведенного анализа зачастую, выбираются их авторами, субъективно, без должного научного обоснования.

В этой ситуации возникает бесконечная рекурсия, так для доказательства факта честного проведения выборов нужно использовать методы ЭК, для доказательства адекватности которых, в свою очередь, нужно использовать ЭД, опубликованные по результатам честно проведенных выборов, и т.д. (аналогично, известной истории о служителе культа и его любимой собаке). По мнению авторов возможный выход из описанной ситуации состоит в использовании синтезированных ЭД, статистические свойства которых близки к статистическим свойствам реальных электоральных данных.

Для подтверждения адекватности выбранного подхода решаемой задаче был разработан алгоритм синтеза ЭД, его программная реализация и подтверждена их работоспособность.

Проведенный анализ результатов применения популярных в настоящее время методов ЭК к синтезированным модельным ЭД и вычисленным на их основе ЭП позволил сделать обоснованный вывод о том, что все изученные методы ЭК обнаружили признаки фальсификаций модельных заведомо нефальсифицированных ЭД.

Следовательно, данные методы не должны использоваться в практике ЭК, а выводы, сделанные на основе результатов их применения, требуют критического переосмысления. Также необходимо отметить, что разработанный авторами статьи подход можно использовать для оценки адекватности как любого существующих сегодня, так и вновь разработанных методов ЭК.

Литература

1. Поршнев С.В., Рябко Н.Ю. Исследование методов электоральной криминалистики// Вестник УрФО. Безопасность в информационной сфере. –2025. –№ 4(58). – С. –21–35. DOI: 10.14529/secur250403.

2. Смолуховский М. Броуновское молекулярное движение под действием внешних сил и его связь с обобщенным уравнением диффузии// Броуновское движение. –М.: ОНТИ-НКТП-СССР, 1936. – С. 319–331.

3. Смолуховский М. Несколько примеров броуновского молекулярного движения под действием внешних сил// Броуновское движение. –М.: ОНТИ-НКТП-СССР, 1936. – С. 205–225.

4. Смолуховский М. Три доклада о диффузии, броуновском молекулярном движении и коагуляции коллоидных частиц// Броуновское движение. –М.: ОНТИ-НКТП-СССР, 1936. – С. 33–416.

5. Гнеденко Б.В. Курс теории вероятностей. –М.: Физматгиз, 1961. –407 с.

6. Копосов А.С., Поршнев С.В. Случайные величины с ограниченной областью рассеяния: математическое и алгоритмическое обеспечение для оценивания плотностей вероятностей и функций распределений. –М.: Горячая линия-Телеком, 2019. –184 с.

7. Поршнев С.В., Копосов А.С. Программная библиотека ES&RP// Свидетельство о государственной регистрации программы для ЭВМ № 2016614275 (Заявка № 2016611747. Дата поступления 2 марта 2016 г. Дата государственной регистрации в Реестре программ для ЭВМ 20 апреля 2016 г.)

8. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. – М.: Наука, 1965. –524 с.

9. Матвиевский В.Р. Надежность технических систем. – М: Московский государственный институт электроники и математики, 2002. –113 с.

10. Острейковский В.А. Теория надёжности. 2-е изд., испр. – М.: Высшая школа, 2008. –464 с.

11. Половко А.М., Гуров С.В. Основы теории надёжности. – СПб.:БХВ-Петербург, 2006. –702 с.

12. . Поршнев С.В., Рябко Н.Ю. Опыт многомерного статистического анализа электоральных данных// Вестник УрФО. Безопасность в информационной сфере. –2023. – № 2(48). – С. 5–29. DOI: 10.14529/secur230201

13. Сызранцев В.Н. Расчет прочностной надежности изделий на основе методов непараметрической статистики/В.Н. Сызранцев, Я.Н. Невелев, С.Л. Голофаст// – Новосибирск: Наука, 2008. –128 с.

14. Benford F. The Law of Anomalous Numbers// Proceedings of the American Philosophical Society. –1938. –Mar. 31. – Vol. 78. – № 4. – P. 551–572.

15. Deckert J., M. Myagkov, Ordeshook P.C. The Irrelevance of Benford's Law for Detecting Fraud in Elections [Электронный ресурс] // Caltech/MIT Voting Technology Project Working Paper. №. 9. 2010. URL: http://vote.caltech.edu/content/irrelevance-benfords-law-detecting-fraud-elections (Дата обращения: 4.02.2023).

16. Diekmann A. Benford's Law and Fraud Detection: Facts and Legends/ Diekmann, Andreas, Ben Jann// German Economic Review. –2010. – Vol. 11 (3). – P. 397–401.

17. Shikano S. When Does the Second-Digit Benford's Law-Test Signal an Election Fraud? Facts or Misleading Test Results // Jahrbucher f. Nationalokonomie u. Statistik (Lucius & Lucius, Stuttgart 2011). – Bd. (Vol.) 231/5+6. – P. 719–732.

18. Breunig C. Searching for electoral irregularities in an established democracy: Applying Benford's Law tests to Bundestag elections in Unified Germany// Electoral Studies. –2011. – Vol. 30. – P. 534–545.

19. Leemann L., Bochsler D. A systematic approach to study electoral fraud// Electoral Studies. –2014. – Vol. 35. – P. 33–47.

20. Pericchi L., Torres D. Quick Anomaly Detection by the Newcomb-Benford Law, with Applications to Electoral Processes Data from the USA, Puerto Rico and Venezuela// Statistical Science. –2011. – Vol. 26. – №. 4. – P. 502–516.

21. Шалаев Н.Е. Электоральные аномалии в постсоциалистическом пространстве: опыт политологического анализа. Дисс…канд. политических наук по специальности 23.00.02 – Политические институты, процессы и технологии. – Санкт-Петербург: СПбГУ, 2016 г. –191 с.

22. Шпилькині С. Статистическое исследование результатов российских выборов 2007–2009 гг. // Троицкий вариант – наука. –2009. – № 21(40). – С. 2–4.

23. Шпилькині С. Математика выборов – 2011 // Троицкий вариант – наука. –2011. – № 25(94). – С. 2–4.

24. Шпилькині С. Двугорбая Россия // Троицкий вариант – наука. –2016. № 20(214). – С. 1–3.

25. Шпилькині С. Выборы 2018 года: Фактор X и «пила Чурова» // Троицкий вариант – наука. –2018. – № 8(252). – С. 8–10.

26. Шпилькині С. Поправки на 27 миллионов // Троицкий вариант – наука. –2020. – № 14(308). – С. 4–5.

27. Собянин А.А., Суховольский В.Г. Демократия, ограниченная фальсификациями. – М.: ИНТУ, 1995. –263 с.

28. Подлазов А.В. Формальные методы выявления масштабных электоральных фальсификаций на материале федеральных выборов1999-2018 гг. / Препринты ИПМ им. М.В. Келдыша. –2019. – № 2. –28 с. doi:http://doi.org/10.20948/prepr-2019-2. URL: http: //library. keldysh.ru/preprint.asp?id=2019-2 (Дата обращения: 25.11.2025).

29. Подлазов А.В. Исследование статистических методов выявления выдуманных результатов выборов: Часть 1. Круглые числа // Препринты ИПМ им. М.В. Келдыша. –2019. – № 147. – 28 с. DOI: http://doi.org/10.20948/prepr-2019-147. URL: http://library.keldysh.ru/preprint.asp? id=2019-147 (Дата обращения: 25.11.2025).

30. Подлазов А.В. Реконструкция фальсифицированных результатов выборов с помощью интегрального метода Шпилькина // Проектирование будущего. Проблемы цифровой реальности: труды 4-й Международной конференции (4–5 февраля 2021 г., Москва). –М.: ИПМ им. М.В. Келдыша, 2021. – С. 193–208// URL: https://keldysh.ru/future/2021/18.pdf (Дата обращения: 25.11.2025).

References

1. Porshnev S.V., Ryabko N.YU. Issledovaniye metodov elektoral'noy kriminalistiki// Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. –2025. – № 4(58). – S. –21–35. DOI: 10.14529/secur250403.

2. Smoluhovskij M. Brounovskoe molekuljarnoe dvizhenie pod dejstviem vneshnih sil i ego svjaz' s obobschennym uravneniem diffuzii// Brounovskoe dvizhenie. – M.: ONTI-NKTP-SSSR, 1936. – S. 31–331.

3. Smoluhovskij M. Neskol'ko primerov brounovskogo molekuljarnogo dvizhenija pod dejstviem vneshnih sil// Brounovskoe dvizhenie. – M.: ONTI-NKTP-SSSR, 1936. – S. 205–225.

4. Smoluhovskij M. Tri doklada o diffuzii, brounovskom molekuljarnom dvizhenii i koaguljatsii kolloidnyh chastits// Brounovskoe dvizhenie. – M.: ONTI-NKTP-SSSR, 1936. – S. 33– 416.

5. Gnedenko B.V. Kurs teorii verojatnostej. – M.: Fizmatgiz, 1961. – 407 s.

6. Koposov A.S., Porshnev S.V. Sluchajnye velichiny s ogranichennoj oblast'ju rassejanija: matematicheskoe i algoritmicheskoe obespechenie dlja otsenivanija plotnostej verojatnostej i funktsij raspredelenij. – M.: Gorjachaja linija-Telekom, 2019. – 184 s.

7. Porshnev S.V., Koposov A.S. Programmnaja biblioteka ES&RP// Svidetel'stvo o gosudarstvennoj registratsii programmy dlja EVM № 2016614275 (Zajavka № 2016611747. Data postuplenija 2 marta 2016 g. Data gosudarstvennoj registratsii v Reestre programm dlja EVM 20 aprelja 2016 g.)

8. Gnedenko B.V., Beljaev Ju.K., Solov'ev A.D. Matematicheskie metody v teorii nadezhnosti. – M.: Nauka, 1965. – 524 s.

9. Matvievskij V.R. Nadezhnost' tehnicheskih sistem. – M: Moskovskij gosudarstvennyj institut elektroniki i matematiki, 2002. –113 s.

10. Ostrejkovskij V.A. Teorija nadjozhnosti. 2-e izd., ispr. – M.: Vysshaja shkola, 2008. – 464 s.

11. Polovko A.M., Gurov S.V. Osnovy teorii nadjozhnosti. – SPb.: BHV-Peterburg, 2006. – 702 s.

12. Porshnev S.V., Rjabko N.Ju. Opyt mnogomernogo statisticheskogo analiza `elektoral'nyh dannyh// Vestnik UrFO. Bezopasnost' v informatsionnoj sfere. –2023. – № 2(48). – S. 5–29. DOI: 10.14529/secur230201

13. Syzrancev V.N. Raschet prochnostnoj nadezhnosti izdelij na osnove metodov neparametricheskoj statistiki/V.N. Syzrancev, YA.N. Nevelev, S.L. Golofast// – Novosibirsk: Nauka, 2008. –128 s.

14. Benford F. The Law of Anomalous Numbers// Proceedings of the American Philosophical Society. –1938. – Mar. 31. – Vol. 78. – № 4. – P. 551–572.

15. Deckert J., M. Myagkov, Ordeshook P.C. The Irrelevance of Benford's Law for Detecting Fraud in Elections [Электронный ресурс] // Caltech/MIT Voting Technology Project Working Paper. №. 9. 2010. URL: http://vote.caltech.edu/content/irrelevance-benfords-law-detecting-fraud-elections (Дата обращения: 4.02.2023).

16. Diekmann A. Benford's Law and Fraud Detection: Facts and Legends/ Diekmann, Andreas, Ben Jann// German Economic Review. –2010. – Vol. 11 (3). – P. 397– 401.

17. Shikano S. When Does the Second-Digit Benford's Law-Test Signal an Election Fraud? Facts or Misleading Test Results // Jahrbucher f. Nationalokonomie u. Statistik (Lucius & Lucius, Stuttgart 2011). – Bd. (Vol.) 231/5+6. – P. 719 –732.

18. Breunig C. Searching for electoral irregularities in an established democracy: Applying Benford's Law tests to Bundestag elections in Unified Germany// Electoral Studies. – 2011. – Vol. 30. – P. 534 –545.

19. Leemann L., Bochsler D. A systematic approach to study electoral fraud// Electoral Studies. –2014. – Vol. 35. – P. 33– 47.

20. Pericchi L., Torres D. Quick Anomaly Detection by the Newcomb-Benford Law, with Applications to Electoral Processes Data from the USA, Puerto Rico and Venezuela// Statistical Science. –2011. – Vol. 26. – №. 4. – P. 502–516.

21. Shalaev N.E. Elektoral'nye anomalii v postsotsialisticheskom prostranstve: opyt politologicheskogo analiza. Diss…kand. politicheskih nauk po spetsial'nosti 23.00.02 – Politicheskie instituty, protsessy i tehnologii. – Sankt-Peterburg: SPbGU, 2016. –191 s.

22. Shpil'kini S. Statisticheskoe issledovanie rezul'tatov rossijskih vyborov 2007–2009 gg.// Troitskij variant – nauka. –2009. – № 21(40). – S. 2– 4.

23. Shpil'kini S. Matematika vyborov – 2011 // Troitskij variant – nauka. – 2011. – № 25(94). – S. 2– 4.

24. Shpil'kini S. Dvugorbaja Rossija // Troitskij variant – nauka. – 2016. № 20(214). – S. 1–3.

25. Shpil'kini S. Vybory 2018 goda: Faktor H i «pila Churova» // Troitskij variant – nauka. –2018. – № 8(252). – S. 8 –10.

26. Shpil'kini S. Popravki na 27 millionov // Troitskij variant – nauka. – 2020. – № 14(308). – S. 4 –5.

27. Sobjanin A.A., Suhovol'skij V.G. Demokratija, ogranichennaja fal'sifikatsijami. – M.: INTU, 1995. – 263 s.

28. Podlazov A.V. Formal'nye metody vyjavlenija masshtabnyh `elektoral'nyh fal'sifikatsij na materiale federal'nyh vyborov1999-2018 gg. / Preprinty IPM im. M.V. Keldysha. – 2019. – № 2. –28 s. doi:http://doi.org/10.20948/prepr-2019-2. URL: http: //library. keldysh.ru/preprint.asp?id=2019-2 (Data obraschenija: 25.11.2025).

29. Podlazov A.V. Issledovanie statisticheskih metodov vyjavlenija vydumannyh rezul'tatov vyborov: Chast' 1. Kruglye chisla // Preprinty IPM im. M.V. Keldysha. –2019. – № 147. – 28 s. DOI: http://doi.org/10.20948/prepr-2019-147. URL: http://library.keldysh.ru/preprint.asp? id=2019-147 (Data obraschenija: 25.11.2025).

30. Podlazov A.V. Rekonstruktsija fal'sifitsirovannyh rezul'tatov vyborov s pomosch'ju integral'nogo metoda Shpil'kina // Proektirovanie buduschego. Problemy tsifrovoj real'nosti: trudy 4-j Mezhdunarodnoj konferentsii (4–5 fevralja 2021 g., Moskva). – M.: IPM im. M.V. Keldysha, 2021. – S. 193–208. URL: https://keldysh.ru/future/2021/18.pdf (Data obraschenija: 25.11.2025)

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, профессор Учебно-научного центра «Информационная безопасность» ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32.; ФГБОУ ВО «Уральский государственный экономический университет».620144, г. Екатеринбург, ул. 8 Марта/Народной Воли, 62/45. E-mail: s.v.porshnev@urfu.ru

РЯБКО Николай Юрьевич, аспирант, ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: N.Yu.Ryabko@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32.; Ural State University of Economics. 620144, Yekaterinburg, 8 Marta/Narodnoy Voli St., 62/45. E-mail: N.Yu.Ryabko@urfu.ru

RYABKO Nikolay Yurievich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: N.Yu.Ryabko@urfu.ru

УДК 004.032.26:336.71 Вестник УрФО № 1(59) / 2026, с. 20–27

Япарова Н.М., Щеголев А.В.

DOI: 10.14529/secur260102

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ КРЕДИТОВАНИЯ НА ОСНОВЕ НЕЙРОСЕТЕВОЙ МОДЕЛИ

Статья посвящена разработке нейросетевой модели кредитного скоринга физических лиц, направленной на обеспечение достоверности информации о платёжеспособности заёмщиков в условиях неполных или потенциально искажённых данных. Предметом исследования выступают методы построения нейросетевых моделей для кредитного скоринга, ориентированные на обработку и анализ данных заемщиков. Целью работы является разработка и оптимизация нейросетевой архитектуры, способной получить наивероятнейший прогноз исполнения кредитных обязательств и сформировать рекомендации по выдаче кредита. Прогнозирование осуществляется на основе обработки информации о наборе признаков заемщика. В набор входит стандартная информация о заемщике, такая как объем доходов, кредитная история, а также информация о недавней активности заёмщика, отраженных в открытых источниках. В качестве объекта исследования использованы данные из реальных кредитных заявок. На основе данных построена и оптимизирована полносвязная нейронная сеть с тремя скрытыми слоями, функцией активации ReLU в промежуточных слоях и сигмоидной функцией на выходе. Обучение осуществлялось с использованием оптимизатора Adam и регуляризации Dropout для предотвращения переобучения и повышения устойчивости модели к шуму и аномалиям во входных данных. Экспериментальная валидация и сравнительный анализ с классическими методами машинного обучения подтвердил превосходство нейросети, демонстрируя лучшую устойчивость к целенаправленным искажения входных данных. Результаты исследования подтверждают высокую надежность глубокого обучения в условиях несбалансированных данных и сложных нелинейных зависимостей, а также его практическую применимость для внедрения в автоматизированные системы кредитного скоринга финансовых организаций.

Ключевые слова: *нейронные сети, кредитный скоринг, анализ данных, оценка метода, устойчивость к манипуляциям, принятие решений.*

A DECISION SUPPORT SYSTEM IN THE FIELD OF LENDING BASED ON A NEURAL NETWORK MODEL

The article is devoted to the development of a neural network model of credit scoring of individuals aimed at improving the accuracy, reliability and stability of forecasting borrowers' solvency in conditions of unreliable, incomplete or potentially distorted data. The subject of the research is the methods of building neural network models for credit scoring, focused on the processing and analysis of borrowers' data. The aim of the work is to develop and optimize a neural network architecture capable of reliably assessing the probability of fulfilling credit obligations based on a comprehensive set of features, including both traditional and behavioral sources of information that are resistant to manipulation. The data from real loan applications was used as the object of the study. Based on the data, a fully connected neural network with three hidden layers, a ReLU activation function in the intermediate layers and a sigmoid function at the output was built and optimized. The training was carried out using the Adam optimizer and Dropout regularization to prevent overfitting and increase the model's resilience to noise and anomalies in the input data. Experimental validation and comparative analysis with classical machine learning methods have confirmed the superiority of the neural network, demonstrating better resistance to targeted distortion of input data. The results of the study confirm the high reliability of deep learning in conditions of unbalanced data and complex nonlinear dependencies, as well as its practical applicability for implementation in automated credit scoring systems of financial organizations.

Keywords: *neural networks, credit scoring, data analysis, method evaluation, resistance to manipulation, decision making.*

Введение

Существенным фактором, угрожающим финансовой безопасности как отдельных институтов, так и экономики в целом, является рост закредитованности населения и корпоративного сектора на фоне увеличения неопределенности в поведении заемщиков. В условиях стремительной цифровизации финансовых потоков и экспоненциального роста объема циркулирующих данных традиционные статистические и экспертные методы оценки кредитных рисков все чаще оказываются неспособными обеспечить надежную защиту от дефолтов, особенно при работе с неполной, зашумленной или намеренно искажённой информацией, что создаёт предпосылки для ошибочных решений и повышает уязвимость финансовых институтов к мошенническим действиям. [1-8]. В этом контексте системы кредитного скоринга, направленные на анализ широкого спектра параметров заемщика и прогнозирующего вероятность своевременного погашения долга, приобретают особую значимость, выступая ключевым инструментом объективной оценки индекса надежности заемщиков, что в конечном итоге приводит к существенному снижению рисков, связанных с достоверностью кредитоспособности [9-12].

Применение нейронных сетей в кредитном скоринге способных учитывать сложные нелинейные зависимости и выявлять скрытые паттерны в поведении заемщиков, что позволяет решать проблему надежности и устойчивости моделей кредитного скоринга на качественно новом уровне. Среди работ, связанных с этим направлением исследований отметим работу Д. В. Исаева [13] в которой применяются рекуррентные нейронные сети, обученные на данных карточных транзакций. Принципиальной особенностью данного подхода является отказ от традиционных анкетных признаков в пользу поведенческих характеристик, формируемых автомати-

чески. Такой подход потенциально снижает уязвимость скоринговой модели к искажению самоотчётных данных и демонстрирует перспективность использования альтернативных источников информации для повышения надёжности оценки кредитоспособности, особенно в сегменте заёмщиков с ограниченной кредитной историей. Другим примером является работа В. С. Чуба, в которой для решения задачи кредитного скоринга применялся оптимизированный многослойный персептрон на основе традиционных финансово-демографических признаков. Полученные результаты подтверждают высокую эффективность нейросетевых моделей по сравнению с классическими методами машинного обучения. Вместе с тем использование преимущественно анкетных данных повышает чувствительность моделей к их качеству и достоверности, что в реальных условиях может создавать дополнительные риски при намеренном искажении входной информации.

В рассмотренных работах, в которых анализ финансового поведения заемщика осуществляется лишь в одном направлении либо на основе традиционных демографических и кредитных, либо исключительно на поведенческих транзакционных сигналах. В настоящей работе предлагается гибридный подход, объединяющий оба типа признаков, что позволяет не только повысить точность прогнозирования, но и снизить уязвимость скоринговой модели к мошенническим действиям, ошибкам самоотчёта и неполноте данных. Такой гибридный подход позволяет не только повысить точность прогноза, но и повышает надёжность автоматизированных решений в условиях потенциально манипулируемой информации.

Структура и предобработка исходных данных

Исходный датасет, полученный из открытых источников, содержит данные о 1 000 реальных заемщиках с 20 параметрами. В качестве входных признаков использовались 20 характеристик, включая текущий баланс счёта, кредитную историю, сумму кредита, стаж работы, семейное положение, возраст и другие релевантные параметры, а также поведенческие и контекстуальные признаки, устойчивые к манипуляциям, – в частности, своевременная оплата коммунальных услуг или связи за последние 30 дней, наличие регулярных поступлений на счёт, отсутствие просрочек по обязательствам за 90 дней, а также активность в официальных цифровых сервисах. Эти сигналы повышают достоверность оценки платёжеспособности, снижают уязвимость модели к искажению анкетных данных и позволяют безопасно охватывать клиентов с ограниченной кредитной историей.

Целью этапа предобработки данных является не только обеспечение устойчивости процесса обучения нейронной сети, но и снижение чувствительности модели к зашумлённым, неполным и потенциально искажённым входным данным. Для корректной валидации моделей исходная выборка случайным образом делилась на обучающую и тестовую подвыборки в соотношении 70:30, что позволило оценить обобщающую способность модели в условиях, приближённых к реальной эксплуатации скоринговых систем. Качественная оценка значимости признаков проводилась с помощью алгоритма SHAP. В результате были выделенные наиболее информативные и исключены наименее надежные переменные. С точки зрения устойчивости и безопасности скоринговой системы данный подход позволяет снизить влияние шумовых и наименее надёжных признаков, а также уменьшить «площадь атаки» модели, ограничивая возможности манипулирования результатами за счёт целевых искажений отдельных входных характеристик. После предобработки окончательный набор значимых параметров для нейронный сети составил 15 признаков. Выходными данными модели является бинарная функция платежеспособности заемщика: принимающая значение 1, что соответствует вероятности своевременного погашения кредита — то есть заемщик успешно погасил кредит в срок продемонстрировав свою платежеспособность (надежный заемщик), и принимающая значение 0, что соответствует риску дефолта (неплатежеспособный заемщик).

Нейросетевая модель кредитного скоринга

Предлагаемая нейронная сеть представлена следующим уравнением:

$$z^{(l)} = \sum_{i=1}^{n_l} W_i^{(l)} a_i^{(l-1)} + b_i^{(l)},\ a^{(l)} = g^{(l)}\left(z^{(l)}\right)$$

где:

$W_i^{(l)} \in R^{n_l \times n_{l-1}}$ – веса слоя l,

$b_i^{(l)} \in R^{n_l}$ – вектор смещения слоя l,

$a^{(l)}$ – выходы слоя l

$a_i^{(l-1)}$ – выходы предыдущего слоя l,

$g^{(l)}$ – функция активации, используемая в слое l,

n_l – число нейронов в слое l.

$z^{(l)}$ – выход предыдущего слоя l

$z^{(l-1)}$ – выход предыдущего слоя до функции активации

l – количество слоев

Разработка нейронной сети сопровождалась систематической оптимизацией ее архитектуры с учётом требований информационной безопасности кредитных решений. Оптимизация заключалась в подборе количества скрытых слоев и нейронов, выборе функций активации, настройке гиперпараметров обучения, а также в применении методов регуляризации. Каждая конфигурация обучалась на одном и том же наборе данных, включающем как традиционные признаки, так и поведенческие данные, которые менее подвержены манипуляциям и повышают достоверность оценки. Цель оптимизации заключается в повышении точности предсказаний нейронной сети на тестовой выборке, а также в обеспечении устойчивости модели к переобучению за счет минимизации значения функции потерь, что особенно важно при работе с несбалансированными данными. Оптимальная модель включает 3 скрытых слоя, такая архитектура показала наилучший баланс между точностью и стабильностью при кросс-валидации. Полученная оптимальная архитектура представлена на рис. 1.

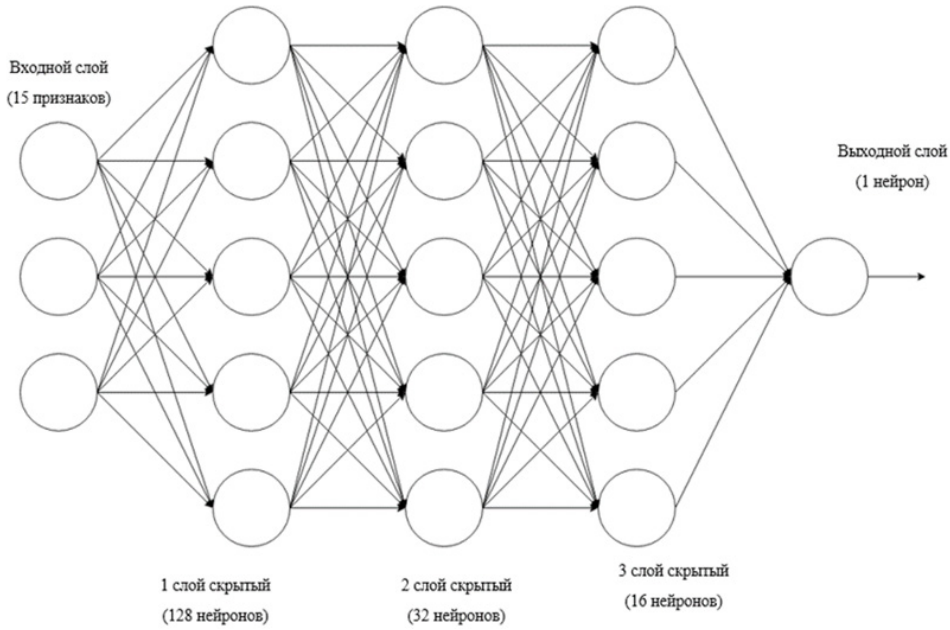

Рис. 1. Архитектура нейронной сети

При построении более глубоких архитектур, включавшей более 3 слоев начиналось переобучение, уменьшение количества слоев приводило к уменьшению способности к извлечению сложных паттернов. Для регуляризации модели и повышения ее устойчивости к шумам в данных был применен метод Dropout. Это достигается за счет случайного отключения части нейронов на каждом шаге обучения, что предотвращает чрезмерную взаимозависимость между ними и снижает риск запоминания шумовых или специфических особенностей обучающей выборки.

Динамика обучения

График точности нейронной сети на этапе обучения представлен на рис. 2 и иллюстрирует динамику изменения метрики точности как на обучающей, так и на тестовой выборках в зависимости от количества эпох

Из результатов, представленных на рис. 2 следует что после 120–130 эпох точность начинает колебаться и перестает следовать за улучшениями на обучающих данных, что указывает на начало переобучения. Наиболее оптимальная производительность на тестовой выборке достигается в диапазоне 80–100 эпох, где разница между обучением и тестированием минимальна. Зависимость значений точности от количества эпох представлена в табл. 1.

На основании результатов, представленных на таблице 1 получаем, что оптимальной

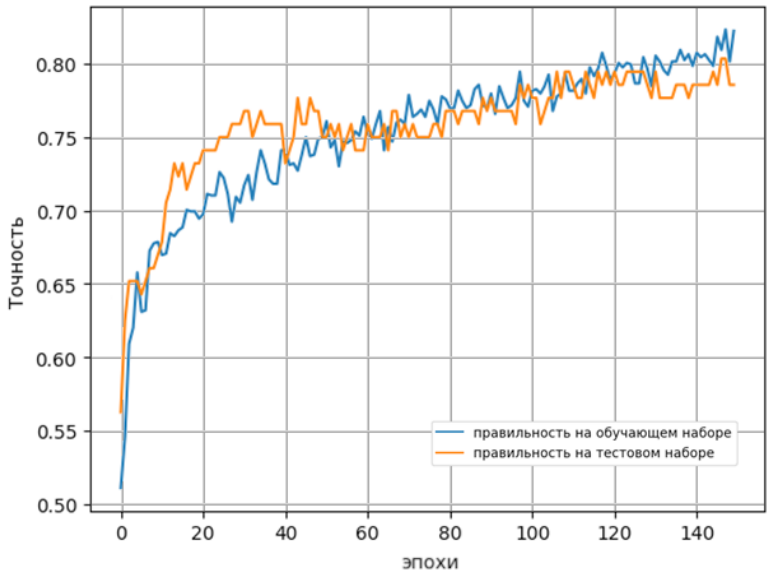

Рис. 2. График точности нейронной сети

Таблица 1

Результаты работы нейросети на тестовой выборке

Количество эпох	Точность
97	0.7768
98	0.7589
99	0.7679
100	0.7752
101	0.7768
102	0.7946
103	0.7768
104	0.7935
105	0.7936
106	0.7857
107	0.7768

точке баланса между обучением и обобщением достигается на 102 эпохе. После этого момента рост потерь на тестовых данных при сохранении снижения на обучающей выборке свидетельствует о начале переобучения.

Результаты экспериментальных исследований

С целью оценки надёжности и практической применимости разработанной нейросетевой модели в условиях реальной эксплуатации автоматизированных систем кредитного скоринга были проведены экспериментальные исследования, включающие сравнительный анализ с классическими методами машинного обучения. В качестве тестовых методов использовались методы основанные на алгоритме дерева решений, случайного леса и наивного байесовского классификатора, применяемых для решения задачи кредитного скоринга. Оценка моделей осуществлялась по двум ключевым критериям: точности классификации на тестовой выборке, отражающей предсказательную способность модели, и коэффициенту устойчивости к целевым атакам — доле заявок, сохранивших исходный прогноз при попытке намеренного искажения входных данных, например, за счёт завышения дохода, стажа или добавления «надёжных» признаков, что напрямую характеризует робастность модели к мошенническим сценариям. Результаты работы всех рассмотренных методов предоставлены на табл. 2.

Таблица 2

Результаты работы методов машинного обучения

Модель	Точность классификации	Коэффициент устойчивости к целевым атакам
Дерево решений	0.707	0.832
Случайный лес	0.792	0.879
Наивный байесовский классификатор	0.732	0.715
Нейронная сеть	0.794	0.931

Сравнение точности моделей показало, что случайный лес и разработанная нейронная сеть демонстрируют наилучшие результаты среди всех протестированных подходов, существенно превосходя традиционные методы, такие как наивный байесовский классификатор и дерево решений. Это подтверждает, что предложенная нейросетевая архитектура – с тремя скрытыми слоями и регуляризацией Dropout – обеспечивает оптимальный баланс между предсказательной способностью и защитой от намеренных искажений входных данных, что делает её наиболее надёжным и практичным решением для внедрения в реальные системы кредитного скоринга, где критически важны как точность, так и безопасность принятия решений.

Заключение

В работе предложена полносвязная нейронная сеть для поддержки принятия решений в области кредитования, ориентированная на обеспечение безопасности и надёжности при оценке вероятности исполнения кредитных обязательств на основе комплексного набора признаков – включая как традиционные, так и поведенческие данные. Экспериментальная валидация подтвердила приемлемую точность прогнозирования даже в условиях сложных нелинейных зависимостей. Сравнительный анализ показал, что предложенная нейросеть превосходит базовые методы машинного обучения по точности и демонстрирует устойчивость к целенаправленным искажениям входных данных. Эти результаты подтверждают практическую пригодность и безопасность разработанной модели для внедрения в автоматизированные системы кредитного скоринга финансовых организаций. В перспективе планируется расширить рамки исследования за счет разработки универсальных архитектур, способных прогнозировать финансовую стабильность не только физических лиц, но и юридических — в частности, малого и среднего бизнеса. Это позволит создать интегрированную систему оценки кредитного риска, применимую в различных сегментах финансового рынка, включая корпоративное кредитование, факторинг и инвестиционный анализ. Особое внимание будет уделено адаптации моделей под специфику бухгалтерской отчетности, макроэкономических индикаторов и отраслевых особенностей компаний, что повысит надежность и интерпретируемость прогнозов в бизнес-среде.

Литература

1. Смирнов А.В., Петров Д.С. Современные подходы к оценке кредитного риска в условиях цифровой трансформации / А. В. Смирнов, Д. С. Петров // Финансы и кредит. 2020. – № 24(912). – С. 1120–1135.

2. Лебедев Е.А. Исследование достоверности оптимизированной модели скоринга путем прогнозирования кредитных историй заемщиков, данные которых не использовались при синтезе модели / Е. А. Лебедев // Научный журнал Кубанского государственного аграрного университета. 2007. – № 34. – С. 1–22.

3. Исаев Д.В. Динамическое ансамблевое обучение для оценки кредитоспособности / Д. В. Исаев // Инновации и инвестиции. 2022. – № 3. – С. 74–79.

4. Кадиев А.Д., Чибисова А.В. Нейросетевые методы решения задачи кредитного скоринга / А. Д. Кадиев, А. В. Чибисова // Математическое моделирование и численные методы. 2022. – № 4(36). – С. 81– 92.

5. Глинкина Е.В. Кредитный скоринг как инструмент эффективной оценки кредитоспособности / Е. В. Глинкина // Финансы и кредит. 2011. – № 16(448). – С. 43– 47.

6. Мельников А.А., Стельмаш Д.С., Ефимов С.Н. Разработка автоматизированной системы кредитного скоринга / А. А. Мельников, Д. С. Стельмаш, С. Н. Ефимов // Актуальные проблемы авиации и космонавтики. 2010. – № 6. – С. 233–234.

7. Симонов П.М., Збоев Е.В. Скоринговая оценка кредитоспособности физических лиц / П. М. Симонов, Е. В. Збоев // Вестник Дагестанского государственного университета. Серия 1: Естественные науки. 2020. Т. 35. – № 2. – С. 18 –26.

8. Кочеткова В.В., Ефремова К.Д. Обзор методов кредитного скоринга / В. В. Кочеткова, К. Д. Ефремова // Juvenis scientia. 2017. – № 6. – С. 22–25.

9. Митрофанова К.Б. Понятие кредитного риска и факторы, на него влияющие / К. Б. Митрофанова // Молодой ученый. 2015. – № 2. – С. 284 –288.

10. Абдуллаев Н.А. Перспективы внедрения современных технологий искусственного интеллекта в скоринговые системы / Н. А. Абдуллаев // Экономика и финансы (Узбекистан). 2023. – № 1(161). – С. 39 – 49.

11. Богданов А.Л., Дуля И.С. Применение нейронных сетей в решении задачи кредитного скоринга / А. Л. Богданов, И. С. Дуля // Вестник Томского государственного университета. Экономика. 2018. – № 44. – С. 173 –183.

12. Костикова А.В., Сайкина Ю.А., Попова А.А. Математические и интеллектуальные методы оценки кредитной платежеспособности физических лиц / А. В. Костикова, Ю. А. Сайкина, А. А. Попова // Вестник Астраханского государственного технического университета. Серия: Экономика. 2024. – № 2. – С. 127–137.

13. Исаев Д.В. Оценка кредитного скоринга на основе карточных транзакций / Д. В. Исаев // Инновации и инвестиции. 2021. – № 5. – С. 105 –109.

14. Чуб В.С. Сравнительный анализ методов машинного обучения в оценке кредитных рисков / В. С. Чуб // Образовательные ресурсы и технологии. 2023. – № 3(44). – С. 81– 92.

References

1. Smirnov A.V., Petrov D.S. Modern approaches to credit risk assessment in the context of digital transformation / A.V. Smirnov, D. S. Petrov // Finance and Credit. 2020. – No. 24(912). – pp. 1120 –1135.

2. Lebedev E.A. Investigation of the reliability of an optimized scoring model by predicting borrowers' credit histories, the data of which were not used in the synthesis of the model / E. A. Lebedev // Scientific Journal of the Kuban State Agrarian University. 2007. – No. 34. – pp. 1–22.

3. Isaev D.V. Dynamic ensemble training for assessing creditworthiness / D. V. Isaev // Innovations and investments. 2022. – No. 3. – pp. 74–79.

4. Kadiev A.D., Chibisova A.V. Neural network methods for solving the problem of credit scoring / A.D. Kadiev, A.V. Chibisova // Mathematical modeling and numerical methods. 2022. – No. 4(36). – pp. 81–92.

5. Glinkina E.V. Credit scoring as a tool for effective assessment of creditworthiness / E. V. Glinkina // Finance and Credit. 2011. – No. 16(448). – pp. 43– 47.

6. Melnikov A.A., Stelmash D.S., Efimov S.N. Development of an automated credit scoring system / A. A. Melnikov, D. S. Stelmash, S. N. Efimov // Actual problems of aviation and cosmonautics. 2010. – No. 6. – pp. 233-234.

7. Simonov P.M., Zboev E.V. Scoring assessment of the creditworthiness of individuals / P.M. Simonov, E. V. Zboev // Bulletin of Dagestan State University. Series 1: Natural Sciences. 2020. Vol. 35. – No. 2. – pp. 18–26.

8. Kochetkova V.V., Efremova K.D. Review of credit scoring methods / V. V. Kochetkova, K. D. Efremova // Juvenis scientia. 2017. – No. 6. – pp. 22–25.

9. Mitrofanova K.B. The concept of credit risk and the factors influencing it / K. B. Mitrofanova // Young Scientist. 2015. – No. 2. – pp. 284–288.

10. Abdullaev N.A. Prospects for the introduction of modern artificial intelligence technologies into scoring systems / N. A. Abdullaev // Economics and Finance (Uzbekistan). 2023. – No. 1(161). – pp. 39 – 49.

11. Bogdanov A.L., Dulya I.S. Application of neural networks in solving the problem of credit scoring / A. L. Bogdanov, I. S. Dulya // Bulletin of Tomsk State University. Economy. 2018. – No. 44. – pp. 173 –183.

12. Kostikova A.V., Saykina Yu.A., Popova A.A. Mathematical and intellectual methods for assessing the credit solvency of individuals / A.V. Kostikova, Yu.A. Saykina, A. A. Popova // Bulletin of the Astrakhan State Technical University. Series: Economics. 2024. – No. 2. – pp. 127–137.

13. Isaev D.V. Evaluation of credit scoring based on card transactions / D. V. Isaev // Innovations and investments. 2021. – No. 5. – pp. 105–109.

14. Chub V.S. Comparative analysis of machine learning methods in credit risk assessment / V. S. Chub // Educational Resources and Technologies. 2023. – No. 3(44). – pp. 81–92.

ЩЕГОЛЕВ Александр Владимирович, аспирант кафедры «Информационные Системы и Технологии» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, 76. E-mail: njznew@gmail.com

ЯПАРОВА Наталья Михайловна, доктор технических наук, доцент, профессор кафедры «Информационные Системы и Технологии» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, 76. E-mail: iaparovanm@susu.ru

SHCHEGOLEV Alexander Vladimirovich, Postgraduate Student, Department of Information Systems and Technologies, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: njznew@gmail.com

YAPAROVA Natalia Mikchailovna, Dr.of Sci, Associate Professor, Department of Information Systems and Technologies, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: iaparovanm@susu.ru

УДК 004.056 Вестник УрФО № 1(59) / 2026, с. 28–35

Зуев А.Д., Зюляркина Н.Д., Соколов А.Н.

DOI: 10.14529/secur260103

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ API-КЛЮЧЕЙ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА ШАМИРА

В статье рассматривается проблема обеспечения конфиденциальности API-ключей от банковских сервисов при интеграции финансовых сервисов в CRM-системы. Проанализирована архитектура распределенной информационной системы хранения ключей и выявлена уязвимость, связанная с централизованным хранением ключей шифрования на сервере-шифровальщике. Предложен метод повышения устойчивости системы к компрометации отдельных узлов посредством внедрения схемы разделения секрета Шамира. В отличие от существующих решений, использующих аппаратные модули безопасности (HSM) или единый сервер ключей, предложенная модель обеспечивает защиту данных даже при полной компрометации одного из узлов инфраструктуры. Описана математическая модель распределения ключей над конечными полями и архитектура новой информационной системы. Результаты апробированы на демонстрационном стенде с использованием сертифицированных средств защиты информации и отечественного программного обеспечения (ОС Astra Linux, шифр «Кузнечик»). Проведены замеры производительности с применением статистических методов оценки, показавшие приемлемые временные затраты на операции разделения и восстановления ключей.

Ключевые слова: *информационная безопасность, API-ключи, схема Шамира, разделение секрета, распределенные системы, шифр «Кузнечик», Astra Linux, криптографическая защита, производительность, доверительные интервалы.*

SECURING STORAGE OF API-KEYS IN DISTRIBUTED INFORMATION SYSTEMS USING SHAMIR'S SECRET SHARING SCHEMA

This paper investigates the problem of ensuring confidentiality of API-keys for external financial services during integration into CRM-platforms. A distributed API-key storage information system was analyzed and a vulnerability in centralized API-key storage was found. It is proposed to implement Shamir's secret sharing schema to resist data leaks from individual nodes in an information system. Unlike existing solutions using hardware security modules (HSM) or centralized key storage, the proposed model guarantees confidentiality even if an individual server in the architecture is fully compromised. A mathematical model for a secret sharing schema over finite fields and an improved information system structure are described. Results were obtained through testing on a demonstration testbed employing certified information security tools and domestic software (Astra Linux OS, "Kuznechik" encryption). Performance measurements were conducted using statistical evaluation methods, demonstrating acceptable time costs for key splitting and recovery operations.

Keywords: *information security, API-keys, Shamir's schema, secret sharing, distributed systems, "Kuznechik" encryption, Astra Linux, cryptographic security, performance, trust intervals.*

При цифровизации финансовых инструментов одной из важных задач является безопасная интеграция сторонних сервисов через программные интерфейсы (API). Вопросы защиты информации требуют решения при работе с API-ключами банковских сервисов, доступ к которым позволяет инициировать финансовые транзакции и получать конфиденциальные данные клиентов. Обычно на практике такие ключи хранятся в зашифрованном виде в базах данных информационных систем (ИС). При этом безопасность ИС в этом случае сводится к безопасности сервера, хранящего мастер-ключи для расшифровки [1].

Компрометация такого сервера ведет к полной утечке секретных данных. Существующие решения, такие как аппаратные модули безопасности (HSM), обеспечивают высокий уровень защиты, но характеризуются высокой стоимостью и сложностью интеграции в веб-ориентированные архитектуры на базе стека LAMP/LEMP. В связи с этим актуальной является разработка программных методов распределенного хранения ключей, обеспечивающих конфиденциальность даже при частичном перехвате контроля над инфраструктурой.

Целью данной работы является разработка архитектуры информационной системы, реализующей распределенное хранение ключей шифрования для API-ключей банков, на основе схемы разделения секрета Шамира [2]. В отличие от известных аналогов, предлагаемое решение адаптировано для веб-ориентированных архитектур на базе отечественного программного обеспечения и не требует приобретения специализированного аппаратного обеспечения.

Объектом исследования выступила распределенная информационная система, предназначенная для интеграции банковских сервисов в CRM-платформы (Битрикс, AmoCRM и др.). Архитектура системы включает три основных компонента (рис. 1):

1. **Пользовательский сервер** (обрабатывает запросы клиентов, управляет процессом получения данных, не хранит чувствительную информацию).

2. **Сервер работы с API** (реализует спец-

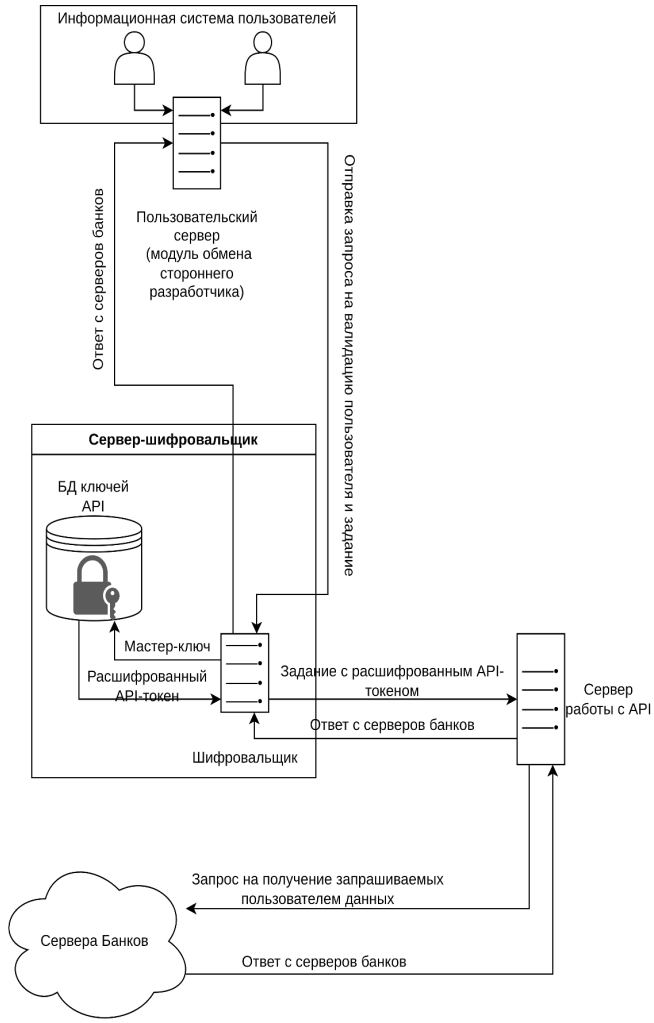

Рис. 1. Архитектура распределенной ИС, предназначенной для интеграции банковских сервисов в CRM-платформы

ифику обращений к API различных банков с целью генерации сертификатов, формирования запросов).

3. **Сервер-шифровальщик** (отвечает за хранение API-токенов в зашифрованном виде, валидацию запросов и инициирование работы сервера работы с API).

В текущей архитектуре сервер-шифровальщик локально хранит ключи для расшифровки базы данных (БД) API-ключей. Такая архитектура имеет критическую уязвимость: получение полного доступа к серверу-шифровальщику позволяет злоумышленнику извлечь ключи расшифровки БД и получить доступ к API-токенам пользователей [3]. Несмотря на валидацию запросов, защита данных ИС зависит от безопасности единственного узла.

Сравнение с существующими аналогами показывает следующие недостатки традиционных подходов:

• **аппаратные модули безопасности (HSM)** – обеспечивают высокий уровень защиты, но требуют значительных затрат и сложной интеграции с веб-приложениями;

• **централизованные серверы ключей** – упрощают управление, но создают единую точку отказа и могут стать основной целью для атакующих.

Предложенное в данной работе решение лишено указанных недостатков: оно реализуется программными средствами, не требует специализированного оборудования и обеспечивает распределенное хранение ключей без зависимости от внешних сервисов.

Для устранения выявленной уязвимости предложена модификация архитектуры, исключающая хранение полного ключа шифрования на одном узле. В основе метода лежит схема разделения секрета Шамира, использующая интерполяционные многочлены Лагранжа над конечными полями [2].

Пусть S — секрет (ключ шифрования БД),

который необходимо разделить. Выбираются параметры k (пороговое значение количества частей для восстановления), n (общее количество частей) и простое число q, определяющее конечное поле F_q, где $k \le n < q-1$.

Строится многочлен степени $k-1$:

$$f(x) = c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + ... + c_2x^2 + c_1x + S(mod\ q), \quad (1)$$

где $f(0)=S$, а коэффициенты $c_1,\ldots, c_{k-1}$ выбираются случайным образом из F_q, причем $c_{k-1} \neq 0$.

Для разделения секрета генерируется n различных точек $(x_i, f(x_i))$, где $x_i \neq 0$. Каждая точка передается на хранение в отдельный узел системы (базу данных частей ключей).

Восстановление секрета возможно при наличии любых k точек. Используя интерполяцию Лагранжа, восстанавливается многочлен $f(x)$:

$$f(x) = \Sigma^k_{i=1} l_i(x)(mod\ q)\ , \quad (2)$$

где базисные многочлены Лагранжа вычисляются как:

$$l_i(x) = f(x_i) \cdot (h_i(x_i))^{-1} \cdot h_i(x)(mod\ q) \quad (3)$$

$$h_i(x) = \Pi^k_{j=1, j\neq i}(x-x_j)(mod\ q) \quad (4)$$

Секрет восстанавливается вычислением $S = f(0)(mod\ q)$ [2].

В предложенной архитектуре сервер-шифровальщик не хранит ключи БД в явном виде. Вместо этого внедрены несколько серверов БД частей ключей. Ключ шифрования для каждой ячейки основной БД разделяется на n частей и распределяется между этими серверами (рис. 2).

Преимущества новой архитектуры по сравнению с аналогами:

1. **Устойчивость к компрометации** –

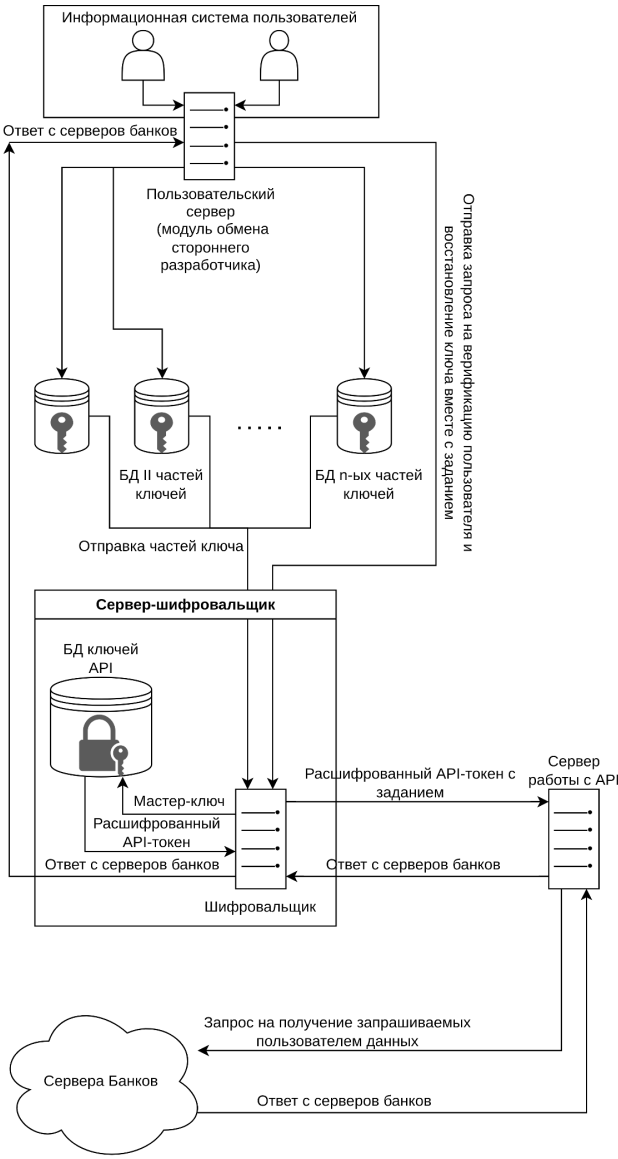

Рис. 2. Архитектура распределенной ИС с разделенной БД ключей шифрования

взлом одного сервера частей ключей не дает злоумышленнику никакой информации о секрете (при условии $k>1$). В отличие от HSM, где компрометация устройства ведет к утечке всех ключей, в предложенной схеме необходимо контролировать как минимум k узлов [4].

2. **Отказоустойчивость** – система сохраняет работоспособность при недоступности части узлов, если количество доступных частей не менее k. Это преимущество отсутствует в централизованных решениях.

3. **Экономическая эффективность** – решение реализуется на стандартном серверном оборудовании без необходимости приобретения специализированных криптографических средств.

Недостатком предложенной архитектуры распределенной ИС с разделенной БД ключей шифрования является переход сервера-шифровальщика из состояния «без сохранения» в состояние «с сохранением» данных, так как для операции расшифровки требуется процедура сбора и восстановления ключа, что предполагает необходимость дополнительных вычислений. Однако для обеспечения безопасности хранения ключей подобный компромисс является обоснованным.

Для оценки эффективности предложенной архитектуры разработан демонстрационный стенд. Выбор средств разработки обусловлен требованиями к использованию сертифицированных средств защиты информации (СЗИ) и импортозамещению:

1. **Операционная система** Astra Linux Special Edition 1.8 [5].

2. **Веб-сервер** Apache 2.4.65.

3. **Язык программирования** PHP 8.2.29 [6].

4. **СУБД** PostgreSQL 15.14.

Особое внимание уделено используемым криптографическим средствам. Для шифрования данных выбран алгоритм «Кузнечик» (ГОСТ Р 34.12-2015) [7]. Ввиду отсутствия официальной поддержки шифра «Кузнечик» и схемы Шамира в стандартных библиотеках PHP (включая расширения КриптоПРО на момент проведения исследования), алгоритмы были реализованы автором самостоятельно с соблюдением спецификаций ГОСТ [7], [8].

Для количественной оценки предложенного решения была разработана методика проведения экспериментов, включающая следующие этапы:

1. **Подготовка тестовой среды.** Все компоненты системы развернуты на одной машине со следующей конфигурацией: 8 ядер CPU (Intel Core i5-10210U, 1.60 ГГц), 16 ГБ ОЗУ, диск SSD NVMe 512 ГБ, сетевой интерфейс 1 Гбит/с. Общение узлов происходит через локальную сеть. Сетевая задержка между узлами эмулирована с помощью утилиты tc (trafficcontrol) и составляет 1 – 3 мс, что соответствует реалистичным условиям локального ЦОД.

2. **Формирование тестовой выборки**. Для каждой комбинации параметров (k, n) проведено $N=1000$ независимых измерений времени выполнения операций разделения и восстановления ключа. Ключ шифрования размером 256 бит выбирался случайным образом. Порядок поля q выбирался равным $2^{521} - 1$. Это наименьшее простое число Мерсенна, которое больше, чем 2^{256}.

3. **Измерение временных характеристик.** Замеры времени выполнялись с использованием функции hrtime() языка программирования PHP с точностью до 1 мкс [6]. Для каждой серии измерений вычислялись выборочное среднее $\overline{x}$, выборочное среднеквадратическое отклонение s и доверительный интервал для математического ожидания (при доверительной вероятности $\gamma = 0,95$).

4. **Статистическая обработка результатов.** Проверка по критерию Шапиро–Уилка с $p>0,05$ показала, что распределение времени выполнения операций асимптотически нормально, поэтому доверительный интервал для математического ожидания можно рассчитать по формуле:

$$\overline{x} \pm t_{\gamma,\nu} \cdot \frac{s}{\sqrt{N}}, \qquad (5)$$

где $t_{\gamma,\nu}$ – квантиль распределения Стьюдента; $\nu = N-1$ – количество степеней свободы.

При $\gamma = 0,95$ и $N=1000$ получим $t_{\gamma,\nu} \approx 1.96$[6].

5. **Контроль внешних факторов**. Перед началом измерений выполнялась предварительная серия из 100 итераций для исключения влияния кэширования кода и инициализации соединений. Во время тестирования нагрузка на хост-систему минимизировалась, фоновые процессы отключались.

В табл. 1 приведены результаты замеров времени разделения и восстановления ключа при различных значениях параметров k и n с указанием 95% доверительных интервалов.

Анализ данных табл. 1 показывает, что время операций растет приблизительно линейно в зависимости от параметра n, что говорит о задержках при сборе частей ключей на сервер-шифровальщике, так как базы данных опрашиваются последовательно. При

Таблица 1

Временные характеристики операций схемы Шамира (95% доверительные интервалы)

Параметры (k, n)	Время разделения ключа, мс	Время восстановления ключа, мс	Размер одной доли, бит
(2, 3)	125.67 ± 0.44	131.36 ± 1.03	521
(3, 5)	180.53 ± 0.54	171.03 ± 1.53	521
(4, 6)	201.17 ± 0.82	196.08 ± 1.96	521
(5, 7)	234.24 ± 0.69	220.94 ± 2.17	521

больших значениях $k \geq 30$ следует ожидать квадратичный рост времени восстановления ключа ввиду алгоритмической сложности интерполяции Лагранжа. Но такое количество серверов не имеет практического смысла. Узкие доверительные интервалы (относительная погрешность не превышает 1,5%) свидетельствуют о стабильности работы алгоритма и достаточном объеме выборки для статистических выводов [9].

Дополнительно были измерены накладные расходы на шифрование/расшифрование данных алгоритмом «Кузнечик» в программной реализации на PHP (100 тестов, входные данные – строка 16 кБ):

• Скорость шифрования: 17.30 ± 0.12кБ/с (95% ДИ);

• Скорость расшифрования: 16.80 ± 0.07 кБ/с (95% ДИ).

Применение новой архитектуры ИС привело к увеличению времени отклика на 100 – 200 мс по сравнению с архитектурой без схемы Шамира. Это связано, в основном, с сетевыми задержками при опросе серверов частей ключей.

Предложенное решение обеспечивает сопоставимый уровень защищенности при значительно меньших затратах времени на интеграцию по сравнению с известными решениями. Например, время доступа к ключу в HSM составляет 10 – 50 мс, а в разработанной архитектуре – 150 – 200 мс. Кроме того, стоимость внедрения предложенного решения гораздо ниже благодаря использованию имеющегося серверного оборудования.

Предложенная архитектура обеспечивает существенное повышение защищенности, поскольку для компрометации ключа шифрования злоумышленнику необходимо получить контроль как минимум над k серверами хранения долей, что экспоненциально снижает вероятность успешной атаки [4], но предполагает увеличение объемов вычислений.

Повышение защищенности ключей шифрования обеспечивается тем, что для компрометации ключа злоумышленнику необходимо получить контроль как минимум над k серверами хранения долей, что экспоненциально снижает вероятность успешной атаки [4]. Однако предложенная архитектура предполагает увеличение объемов вычислений.

Все компоненты системы реализованы на базе отечественного ПО ОС Astra Linux, СУБД PostgreSQL, что обеспечивает соответствие требованиям регуляторов в области импортозамещения и использования сертифицированных СЗИ [5]. Предложенное решение может быть интегрировано в действующие CRM-платформы (Битрикс, AmoCRM) без необходимости полной замены ПО, что минимизирует затраты на внедрение.

Ограничением подхода является увеличение объема хранимых данных: вместо одного ключа система хранит n долей, каждая из которых по размеру равна исходному секрету. Однако для ключей шифрования (типичный размер 256 бит) данное увеличение несущественно по сравнению с общим объемом данных системы.

Заключение

Таким образом, в ходе исследования разработана архитектура ИС, обеспечивающая повышенную защищенность API-ключей банковских сервисов. Внедрение схемы разделения секрета Шамира позволяет устранить риск массовой утечки данных при компрометации отдельного сервера инфраструктуры [2]. Реализация ИС на базе отечественного ПО с применением алгоритма «Кузнечик» обеспечивает соответствие требованиям ГОСТов [5], [7], [8].

В отличие от рассмотренных аналогов (HSM, централизованные серверы ключей), предложенная архитектура сочетает высокий уровень защищенности с возможностью интеграции в веб-архитектуры без дополнительного оборудования. Статистический ана-

лиз предложенного метода разделений ключей показал практическую применимость предложенного решения, так как накладные расходы на операции разделения и восстановления ключей не превышают 235 мс (с доверительной вероятностью 0,95), что допустимо для задач интеграции с внешними банковскими сервисами [9].

В перспективе предложенную архитектуру распределенной ИС с разделенной БД ключей шифрования можно адаптировать для динамического изменения параметров *k* и *n* без перевыпуска всех долей секрета и интегрировать с аппаратными доверенными платформами.

Литература

1. Соколов С.С., Новоселов Р.Ю., Митрофанова А.В. Методы обеспечения доступности информации в высоконагруженных информационных системах // Вестник УрФО № 2(28) / 2018, С. 31–35.

2. Шамир А. Как разделить секрет, чтобы обходиться без защищенного канала связи // Проблемы передачи информации. 1981. Т. 17. № 3. С. 3–14.

3. Повышев А.А., Соколов А.Н., Мищенко Е.Ю. Универсальная классификация угроз безопасности информации и её применение для разработки модели угроз и оценки рисков // Вестник УрФО № 3(49) / 2023, С. 68–80.

4. Шевяков И.А., Соколов А.Н. Метод определения уровня защищённости критических узлов информационной сети транспортного средства // Вестник УрФО № 3(45) / 2022, С. 83–91.

5. Операционная система специального назначения «Astra Linux Special Edition». Руководство по комплексу средств защиты. URL: https://wiki.astralinux.ru/download/attachments/371802537/1.8.3_Ruk_KSZ_1.pdf (дата обращения: 10.03.2026).

6. PHP: Hypertext Preprocessor. Official Documentation. URL: https://www.php.net/manual/ru/ (дата обращения: 01.03.2026).

7. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.

8. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования. М.: Стандартинформ, 2012.

9. ГОСТ Р ИСО/МЭК 17025-2019. Общие требования к компетентности испытательных и калибровочных лабораторий. М.: Стандартинформ, 2019.

References

1. Sokolov S.S., Novoselov R.Ju., Mitrofanova A.V. Metody obespechenija dostupnosti informacii v vysokonagruzhennyh informacionnyh sistemah // Vestnik UrFO № 2(28) / 2018, S. 31–35.

2. Shamir A. Kak razdelit' sekret, chtoby obhodit'sja bez zashhishhennogo kanala svjazi // Problemy peredachi informacii. 1981. T. 17. № 3. S. 3–14.

3. Povyshev A.A., Sokolov A.N., Mishhenko E.Ju. Universal'naja klassifikacija ugroz bezopasnosti informacii i ejo primenenie dlja razrabotki modeli ugroz i ocenki riskov // Vestnik UrFO No 3(49) / 2023, S. 68–80.

4. Shevjakov I.A., Sokolov A.N. Metod opredelenija urovnja zashhishhjonnosti kriticheskih uzlov informacionnoj seti transportnogo sredstva // Vestnik UrFO No 3(45) / 2022, S. 83–91.

5. Operacionnaja sistema special'nogo naznachenija «Astra Linux Special Edition». Rukovodstvo po kompleksu sredstv zashhity. URL: https://wiki.astralinux.ru/download/attachments/371802537/1.8.3_Ruk_KSZ_1.pdf (data obrashhenija: 10.03.2026).

6. PHP: Hypertext Preprocessor. Official Documentation. URL: https://www.php.net/manual/ru/ (data obrashhenija: 01.03.2026).

7. GOST R 34.12-2015. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Blochnyeshifry. M.: Standartinform, 2015.

8. GOST R 34.11-2012. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Funkcija heshirovanija. M.: Standartinform, 2012.

9. GOST R ISO/MJeK 17025-2019. Obshhie trebovanija k kompetentnosti ispytatel'nyh i kalibrovochnyh laboratorij. M.: Standartinform, 2019.

ЗУЕВ Александр Денисович, студент кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, 76. E-mail: zuev.ad@icloud.com

ЗЮЛЯРКИНА Наталья Дмитриевна, доктор физико-математических наук, доцент, профессор кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, 76. E-mail: ziuliarkinand@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, 76. E-mail: sokolovan@susu.ru

ZUEV Aleksandr Denisovich, Student of the Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: zuev.ad@icloud.com

ZYULYARKINA Natalia Dmitrievna, Doctor of Physical and Mathematical Sciences, Associate Professor of the Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: ziuliarkinand@susu.ru

SOKOLOV Aleksandr Nikolaevich, Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: sokolovan@susu.ru

УДК 004 Вестник УрФО № 1(59) / 2026, с. 36–47

Камель М.Х., Ахмед Т.Р., Авсиевич А.В.

DOI: 10.14529/secur260104

РАЗРАБОТКА БЕЗОПАСНОГО ПРОТОКОЛА И ANDROID-ПРИЛОЖЕНИЯ ДЛЯ УДАЛЕННОГО УПРАВЛЕНИЯ СИСТЕМОЙ ОХРАННОГО ОСВЕЩЕНИЯ ЖЕЛЕЗНОДОРОЖНЫХ СТАНЦИЙ

Статья посвящена разработке безопасного протокола и Android-приложения для удаленного управления системой охранного освещения железнодорожных станций. Предлагаемое решение основано на двухуровневой архитектуре безопасности, сочетающей аутентификацию на уровне приложений с использованием HMAC-SHA1 и шифрование транспортного уровня по протоколу TLS 1.3. В системе реализована многофакторная аутентификация, включающая биометрические методы (распознавание лиц), что повышает защиту от несанкционированного доступа. Проведенная верификация подтвердила работоспособность системы, ее соответствие современным требованиям безопасности для IoT-устройств критической инфраструктуры. Разработанное решение способствует повышению безопасности и эффективности управления объектами железнодорожной инфраструктуры за счет автоматизации процессов и минимизации человеческого фактора.

Ключевые слова: *система охранного освещения, железнодорожная станция, Android-приложение, безопасность IoT, TLS/SSL, HMAC-SHA1, биометрическая аутентификация.*

DEVELOPMENT OF SECURE PROTOCOL AND ANDROID APPLICATION FOR REMOTE MANAGEMENT OF RAILWAY STATION SECURITY LIGHTING SYSTEMS

This article presents the development of a secure protocol and Android application for remote management of railway station security lighting systems. The proposed solution is based on a two-tier security architecture combining application-level authentication using HMAC-SHA1 and transport-level encryption via TLS 1.3 protocol. The system implements multi-factor authentication, including biometric methods (facial recognition), which enhances protection against unauthorized access. The verification confirmed the system's functionality and its compliance with modern security requirements for IoT devices in critical infrastructure. The developed solution contributes to improving the security and management efficiency of railway infrastructure facilities through process automation and minimization of human factor.

Keywords: *security lighting system, railway station, Android application, IoT security, TLS/SSL, HMAC-SHA1, biometric authentication.*

Введение

Системы охранного освещения железнодорожных станций представляют собой критически важный компонент инфраструктуры, от которого зависит безопасность пассажиров, персонала и грузов. В контексте цифровизации и перехода к концепции «умных» станций возрастает потребность в эффективных решениях для удаленного управления такими системами. Однако интеграция технологий Интернета вещей (IoT) в системы управления освещением создает новые векторы кибератак, требуя разработки специализированных протоколов безопасности [1, 2].

Традиционные системы управления освещением часто ограничены локальным доступом или используют устаревшие протоколы связи, что делает их уязвимыми к несанкционированному вмешательству. В частности, для железнодорожных станций, где системы освещения тесно связаны с другими системами безопасности (видеонаблюдение, сигнализация), компрометация одной системы может привести к каскадным нарушениям [3]. Существующие коммерческие решения не всегда учитывают специфические требования критической инфраструктуры, такие как устойчивость к сетевым атакам, минимальное время отклика и строгая многофакторная аутентификация [4, 5].

Чтобы противостоять этим атакам, необходимо обеспечить интегрированную систему безопасности с новейшими технологиями шифрования, такими как TLS 1.3, системами обнаружения вторжений на основе машинного обучения и функциями управления идентификацией в основе [6]. Технологии блокчейна доказали свою эффективность в защите интеллектуальных систем освещения в недавних исследованиях, предлагая защищенные от несанкционированного доступа транзакционные записи [7].

В последнее десятилетие появилось множество значительных разработок в области проектирования систем цифровой проверки личности, особенно тех, которые разработаны для беспроводных сетей на основе интеллектуальных датчиков. Важность этих систем

заключается в их способности противостоять различным угрозам безопасности, начиная от попыток взлома учетных записей и заканчивая прослушиванием каналов связи. Недавние исследования были сосредоточены на разработке этих систем для удовлетворения инфраструктурных требований интеллектуальных городов, которые в значительной степени полагаются на распределенные сенсорные сети.

В этом контексте в 2015 году [8] исследовательская группа представила модель, которая опирается на механизм аутентификации для проверки личности пользователя с помощью пароля. Эта модель характеризуется своей способностью предотвращать многие распространенные атаки безопасности и кибератаки, сохраняя при этом конфиденциальность пользователя. Однако большая вычислительная нагрузка, которую она налагала на основные узлы сети, снижала ее практическую эффективность в крупномасштабных приложениях. Два года спустя другие исследователи [9] разработали усовершенствованную систему проверки личности с использованием интеллектуальных технологий, достигнув ощутимых результатов и хороших уровней производительности и безопасности. Однако она не устранила все уязвимости безопасности, которые остаются, особенно с точки зрения защиты полной личности пользователя и противодействия сложным атакам подмены.

В более поздней разработке в 2019 году [10] создали систему безопасности, основанную на передовых методах шифрования. Разработчики этой системы утверждали, что она способна обеспечить комплексную защиту от всех известных форм атак безопасности, при этом значительно снижая свои вычислительные требования по сравнению с предыдущими системами. Однако эти заявления все еще требуют дополнительных исследований для проверки их обоснованности в практических приложениях.

В 2020 году исследовательская группа под руководством Басудеба [11] разработала модель биометрической проверки личности для интеллектуальных городов. Эта модель очень гибкая, позволяет пользователям изменять свои учетные данные для входа с помощью методов биометрической аутентификации и может динамически управлять умными устройствами. Результаты анализа безопасности продемонстрировали способность модели эффективно противостоять различным известным угрозам безопасности.

Отдельно Гахрамани и коллеги [12] разработали систему проверки личности для мобильных сетей в умных городах, используя методы биометрической аутентификации. Результаты показали, что эта система может сократить время обработки до 53% по сравнению с традиционными системами.

В области беспроводных сенсорных сетей Ши и его команда [13] разработали усовершенствованную систему аутентификации и проверки личности, специально предназначенную для сред умных городов. Исследователи использовали методы формального математического анализа для проверки эффективности системы и ее способности улучшать управление ресурсами в различных областях, таких как транспортные системы, услуги здравоохранения и управление энергопотреблением.

Гупта С., Аль-Харби и др. [14] предложили разработать систему проверки личности, которая обеспечивает высокий уровень защиты и конфиденциальности для данных IoT. Результаты исследования показали, что предлагаемая система обеспечивает эффективную защиту при решении проблем и задач q-SDM и демонстрирует превосходную производительность по сравнению с другими решениями в этой области.

Как видно, в мире стремятся для улучшения систем безопасности доступа к объектам инфраструктуры создавать безопасные многофакторные алгоритмы аутентификации [15,16].

Исходя из выше сказанного, актуальность работы обусловлена ростом числа пользователей интернета, общим увеличением объемов трафика, ростом числа сетевых угроз, необходимостью в контроле доступа к информационным ресурсам и потребности ОАО РЖД по внедрению малолюдных и безлюдных средств управления процессами, которые позволяют минимизировать влияние человеческого фактора за счет стандартизации и автоматизации регулярных процессов, достигаемых в ходе развития информационных технологий и сервисно-ориентированных механизмов взаимодействия людей и систем в том числе промышленного интернета (IoT) [17].

В данной работе представлена разработка безопасного протокола и мобильного приложения для Android, предназначенных для удаленного управления системой охранного

освещения (СОО) железнодорожных станций. Основной целью исследования является создание двухуровневой системы безопасности, сочетающей криптографическую аутентификацию на уровне приложений (на основе HMAC-SHA1) и защищенный транспортный канал (TLS 1.3). Дополнительно в систему интегрирована биометрическая аутентификация по лицу для обеспечения многофакторной проверки пользователей.

Угрозы, актуальные для систем охранного освещения

При разработке систем охранного освещения необходимо анализировать угрозы информационной безопасности. Результаты анализа используются при разработке протокола управления светильниками. Особое внимание необходимо уделять моделям угроз и методам их предотвращения при управлении устройствами через интерфейс Ethernet. Существует следующий набор угроз:

– несанкционированный доступ к АРМ системы управления освещением. В рассматриваемых системах угрозы безопасности, связанные с утечкой информации по техническим каналам, характеризуются теми же условиями и факторами, что и для систем в локальной сети;

– проблемы, связанные с уровнем безопасности в сети при обмене данными между сервером и клиентом для управления охранным освещением. Возникают при сетевом управлении устройствами охранного освещения.

При подключении к сети с помощью приложения для смартфона существует множество угроз. Ваши данные уязвимы для атак злоумышленников, которые могут изменить настройки устройств СОО и вмешаться в процесс их работы.

Канал связи может быть подвержен атакам, и его нужно отстоять с поддержкой криптографических средств.

При управлении сетью освещения с использованием внешней сети Интернет злоумышленник может проводить разные типы атак. Потенциальные угрозы перечислены в табл. 1.

Таблица 1

Угрозы в АРМ для управления освещением

Угроза в АРМ для управления освещением	Описание	Противодействие в системе охранного освещения
Опасность «Анализ сетевого трафика» из наружных сеток информации	Наполняется с помощью особенной программы, анализирующей информацию, используемую сетевой картой	Внедрение криптографических протоколов
Опасность сканирования	Сбор информации о сети, предоставление запросов сетевым службам ИС и тест ответов на них	нет
Опасность на подобии «Отказ в обслуживании» (атаки на подобии DoS)	Происходит переполнение буферов и блокирование процедур обработки	нет
Проблемы, связанные со связью между сервером и клиентом	Наличие защищенной сети для управления охранным освещением без проблем при общении между клиентом и сервером устройство управления освещением	нет
Опасность выявления паролей	Перебор/тест сетевого трафика	Разовые пароли/криптографическая аутентификация
Опасность удаленного запуска приложения	Удаленное управление системой	нет
Опасность внедрения по сети вредных программ	Внедрение вредного кода в ПО прибора	Ознакомление пользователей с приборами системы охранного освещения, с правилами неопасного применения

Угроза несанкционированного доступа к сетевым настройкам управления освещением, таким, как сетевой адрес для управления освещением и настройками освещения, среди наиболее важных повреждений, угрожающих осветительной сети системы.

С учетом угрозы внедрения по сети вредоносных программ в результате неосторожного использования устройства самими пользователями, перед выделением работнику программного обеспечения АРМ, надо производить инструктаж по безопасному использованию мобильного устройства, который наполняется управлением освещением безопасности.

Материал и методы исследования

Рассматриваемая система управления сетью охранного освещения железной инфраструктуры состоит из приложения дистанционного управления на базе мобильного телефона, которое отправляет команды на сервер для управления включением/выключением сети охранного освещения. Клиент и сервер взаимодействуют через Интернет с использованием протокола TCP/IP. TLS/SSL используется для защиты соединения и шифрования данных между клиентом и сервером. Многофакторная аутентификация с использованием распознавания лиц также используется для повышения безопасности перед управлением сетью охранного освещения и предотвращения доступа неавторизованных пользователей к системе. На рис. 1 показана архитектура системы, используемой для управления и защиты сети охранного освещения.

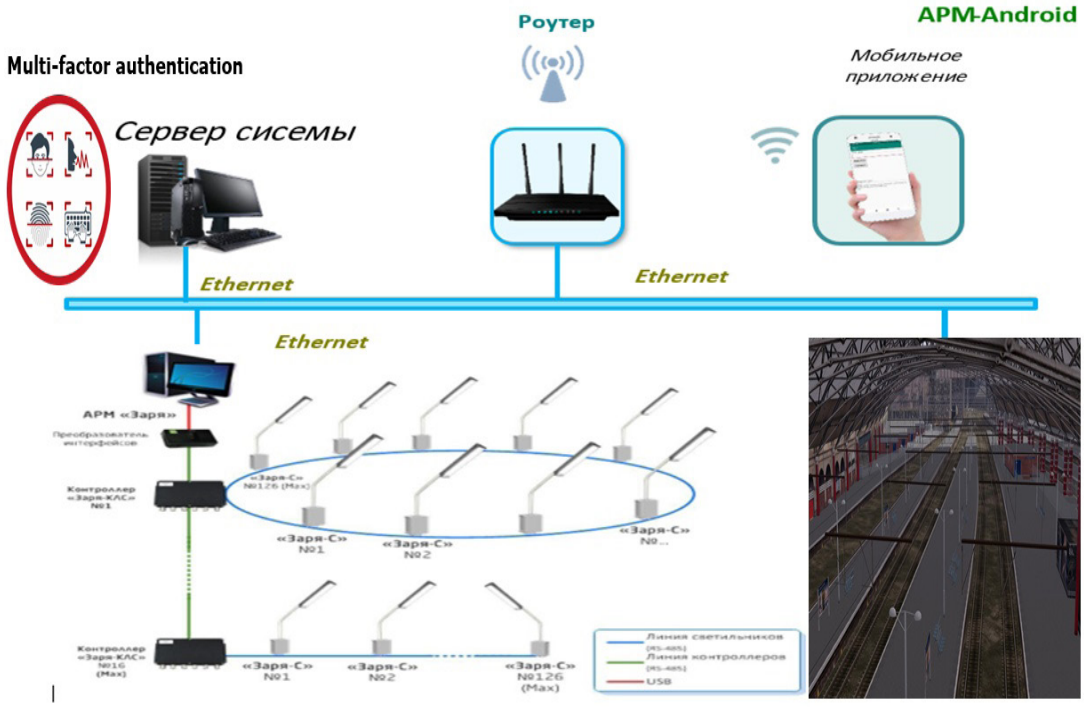

Рис. 1. Архитектура системы охранного освещения IoT

Интерфейс аутентификации пользователя для входа в систему. Интерфейс входа обеспечивает безопасный механизм аутентификации для проверки личности пользователя перед предоставлением доступа к системе управления охранным освещением. Интерфейс основан на двухфакторной аутентификации, где пользователь вводит действительное имя пользователя и пароль для входа в систему, с возможностью добавления биометрической проверки с помощью распознавания лиц.

Интерфейс реализуется путем создания нового действия в приложении, которое наследуется от класса AppCompatActivity. Затем пользовательский интерфейс определяется в отдельном XML-файле, содержащем поля ввода текста и различные элементы отображения. Основные элементы интерфейса включают два поля ввода текста: одно для имени пользователя и одно для пароля. Текст в поле пароля должен быть скрыт для повышения безопасности. Интерфейс также вклю-

чает кнопку для отображения информации о входе и текст для отображения количества оставшихся попыток для пользователя.

При создании действия элементы интерфейса привязываются к переменным в коде с помощью findViewById. Затем кнопке назначается прослушиватель событий (OnClickListener Login) для обработки процесса входа при нажатии на нее. Эта функция проверяет данные, сравнивая входные данные с ранее сохраненными значениями, которые могут находиться в базе данных или файле конфигурации.

Система безопасности или аутентификации также включает механизм ограничения количества неудачных попыток входа (рис. 2). Количество оставшихся попыток сохраняется в кэше приложения и обновляется после каждой неудачной попытки. Когда все разрешенные попытки входа исчерпаны или не увенчались успехом, кнопка входа отключается, чтобы предотвратить дальнейшие попытки.

Далее пользователю показывается информация с помощью элементов пользовательского интерфейса и всплывающих уве-

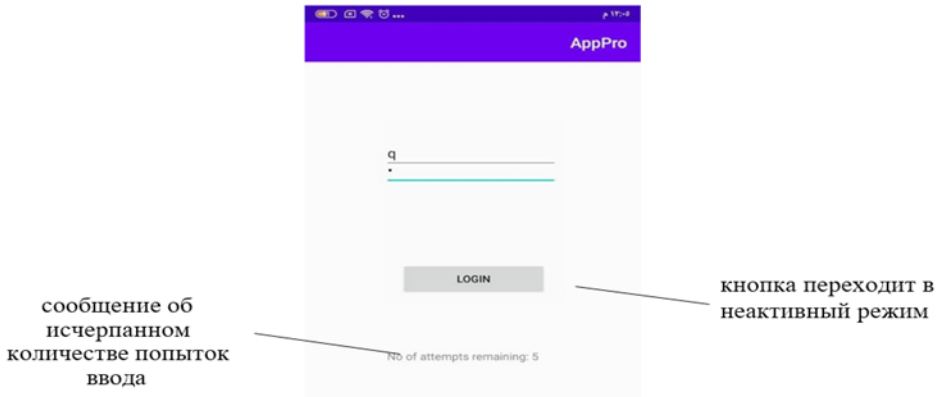

Рис. 2. Лицензия на вход в системы

домлений, информирующая его о статусе входа. В случае успеха пользователь перенаправляется в главный интерфейс приложения, а в случае неудачи он информируется об оставшихся попытках доступа к системе.

Для обеспечения безопасности входные данные проверяются, и поля не остаются пустыми, прежде чем данные входа обрабатываются в главном интерфейсе системы. Для повышения безопасности системы можно добавить дополнительные функции безопасности, такие как биометрическая аутентификация или сброс пароля по электронной почте.

Действие записывается в файл Android Manifest.xml и назначается в качестве основной точки входа для приложения. Это гарантирует, что экран входа в систему — это первое, что видит пользователь при запуске приложения или входе в систему. Это способствует повышению безопасности системы, гарантируя, что все пользователи должны пройти процесс аутентификации перед доступом к функциям управления освещением.

Android-приложение для управления СОО для отдельного устройства. Удаленное управление устройством случается с поддержкой взаимодействия по сокету между клиентом – APM, направляющим команду устройству и устройством – сервером. Для передачи устройству команды подключения или же выключения нужно подключить к устройству сетевой адаптер для обнаружения сокета с серверной стороны, квалифицировать *IP-адрес* и прослушиваемый порт.

Осуществление перечня возможностей функционала, позволяющего мобильному *Android-APM* ориентировать команды устройству, производится в классе *My-Application*, расширенным классом *AppCompatActivity*. Класс имеет способ *onCreate*, поддерживающий файл, описывающий тротуар управления светильником – *R. layout.myapplication*, и инициализирует содержащиеся в ресурсном файле составляющие *TextView, Switch, EditText, Button*. *Switch* выступает в роли указателя состояния осветительного прибора. Составляющие *Switchlamp, ButtonLampon, ButtonLampoff* переключают положение осветительного прибора из «включенного» в «выключенное» и в обратном порядке.

Обработчики нажатий кнопок *Lampon, Lampoff* реализуются с помощью *setOnClick Listener*, обработчик переключателя *switch* – при помощи *setOnCheckedChangeListener*, СОО связана с адресом сервера и портом для управления освещением.

Любой из переключателей при активации исполняет класс *privateTcpclient*, расширенный классом *privateTcpclient ()*, запускающим асинхронный клиентский сокет, и в согласовании с предназначением переключателя посылает удаленному светильнику команду *«LampOn»* – для подключения, или же *«Lampoff»* – для выключения.

Применяемые несколькими классами переменные можем огласить как статические: *String ip, command; int port.*

Экран панели управления отображен на рис. 3 для включенного и выключенного состояния в соответствии с этим.

На рис. 4 приведена схема взаимодействия приложения с сервером для управления сетью охранного освещения с использованием TCP/IP через сокеты.

Протоколы безопасного управления и связи. Для обеспечения безопасного и надежного удаленного управления системой охранного освещения была разработана двухуровневая архитектура безопасности. Она включает: 1) протокол аутентификации

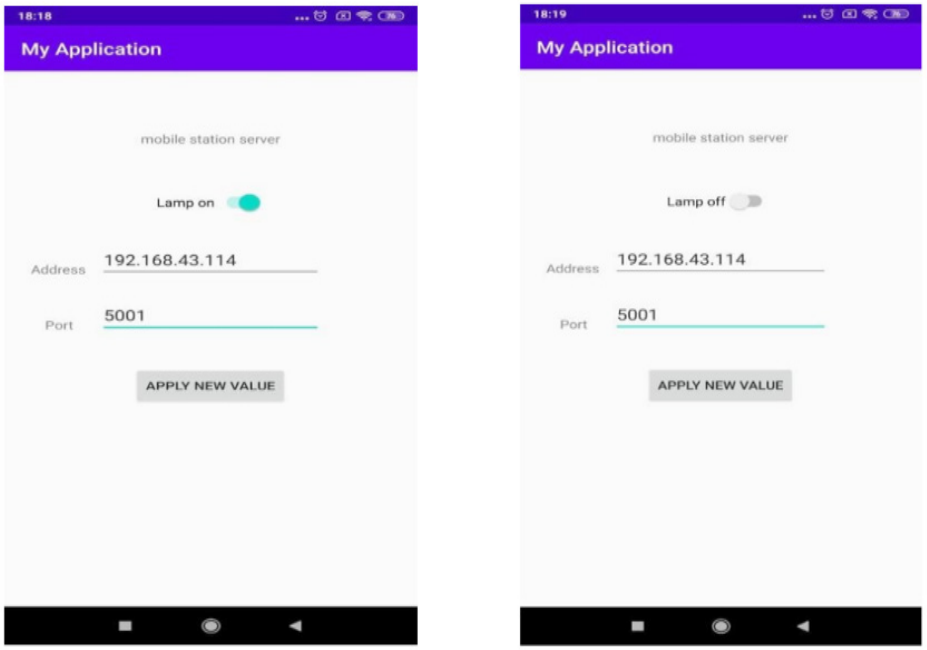

Рис. 3. Управляйте охранным освещением с помощью приложения Android

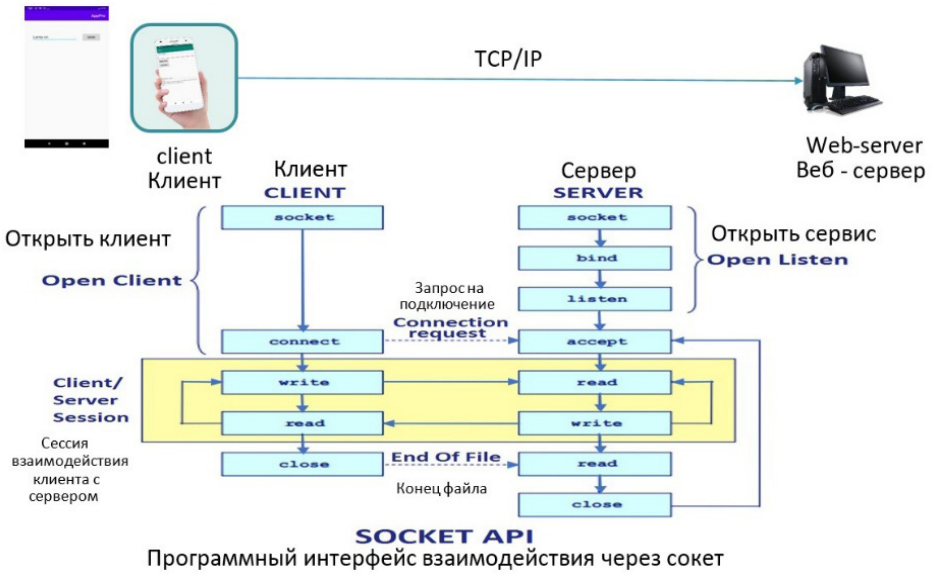

Рис. 4. Связь между клиентом и сервером по протоколу TCP/IP

на уровне приложений для проверки подлинности каждой команды и 2) защиту транспортного уровня с помощью TLS для шифрования всего сетевого трафика.

Протокол аутентификации на основе HMAC-SHA1. На уровне приложения реализован протокол, гарантирующий целостность, аутентичность и актуальность каждой управляющей команды. Клиентское Android-приложение формирует *HTTP POST*-запрос следующей структуры:

POST /xmlapi/std HTTP/1.1
Host: [адрес_сервера]
Date: [время_запроса_RFC_1123]
ECNC-Auth: Nonce="[NONCE]", Created= = "[CREATED]", Digest="[DIGEST]"
Content-Length: [длина]
Content-Type: application/xml
Connection: close

Ключевым элементом является специальный заголовок *ECNC-Auth:*

• ***Nonce:*** Уникальная случайная последовательность (20 байт) в кодировке Base64, генерируемая для каждого запроса для защиты от атак повторного воспроизведения (replay attacks).

• ***Created:*** Метка времени создания запроса в формате *ISO 8601*, обеспечивающая проверку актуальности.

• ***Digest:*** Криптографическая хэш-сумма, вычисляемая по алгоритму *HMAC-SHA1*. Дайджест формируется на основе конкатенации бинарных представлений полей *Nonce, Created, метода HTTP (POST), URI (/xmlapi/std)* и тела запроса. Секретный ключ для HMAC является комбинацией статического пароля оборудования и идентификатора бренда.

Верификация на стороне сервера происходит в три этапа:

1. Проверяется расхождение между временем в поле Created и временем сервера (допуск ±10 секунд).

2. Вычисляется ожидаемый дайджест с использованием общего секретного ключа.

3. При совпадении вычисленного и переданного дайджеста команда исполняется. В противном случае сервер возвращает ответ *HTTP*/1.1 401 Authentication Error.

Данный протокол обеспечивает строгую аутентификацию источника команд и защищает систему от несанкционированного доступа и манипуляции данными на уровне приложения (схема запроса представлена на рис. 5).

Защита транспортного уровня с помощью *TLS*. Протокол аутентификации приложения передается поверх защищенного транспортного канала, организованного с помощью *TLS 1.3*. Использование TLS решает следующие критически важные задачи:

• **Шифрование трафика:** предотвращает перехват и чтение управляющих команд и ответов.

• **Аутентификация сервера:** Клиент проверяет подлинность сервера по его SSL-сертификату *X.509*, что является основной защитой от атак типа «человек посередине» (*MITM*).

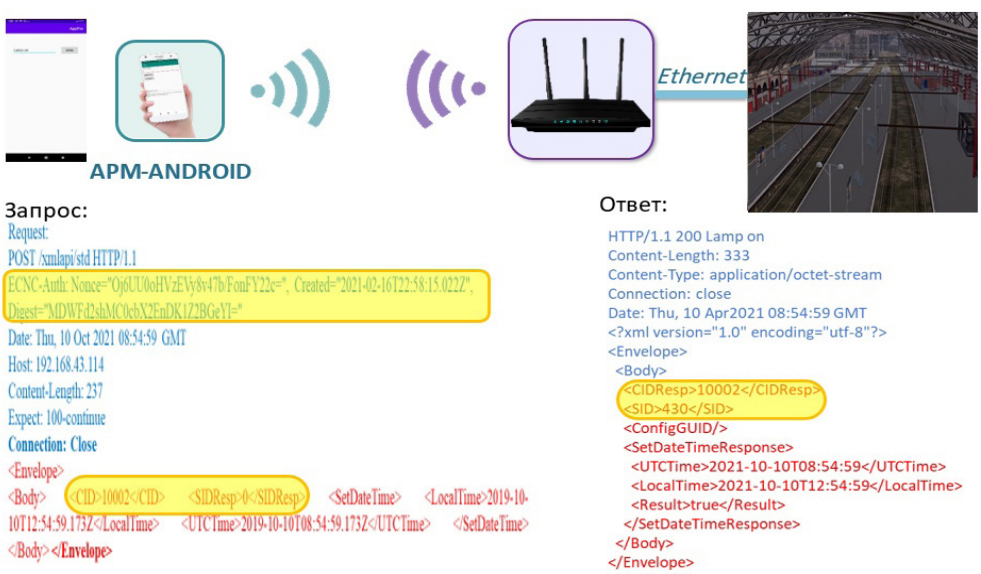

Рис. 5. Запрос клиента на подключение к серверу

• **Целостность данных:** Гарантирует, что данные не были изменены при передаче.

Внедрение *TLS* проводилось с учетом современных стандартов кибербезопасности. Были сгенерированы и настроены SSL-сертификаты, выбраны стойкие наборы шифров (например, *TLS_AES_256_GCM_SHA384*), а поддержка устаревших и небезопасных версий протокола (*SSL 3.0, TLS 1.0, TLS 1.1*) была отключена. Таким образом, весь обмен данными между мобильным приложением и сервером управления происходит по зашифрованному и аутентифицированному каналу.

Таким образом, весь обмен данными происходит по зашифрованному каналу (процесс установления соединения показан на рис. 6).

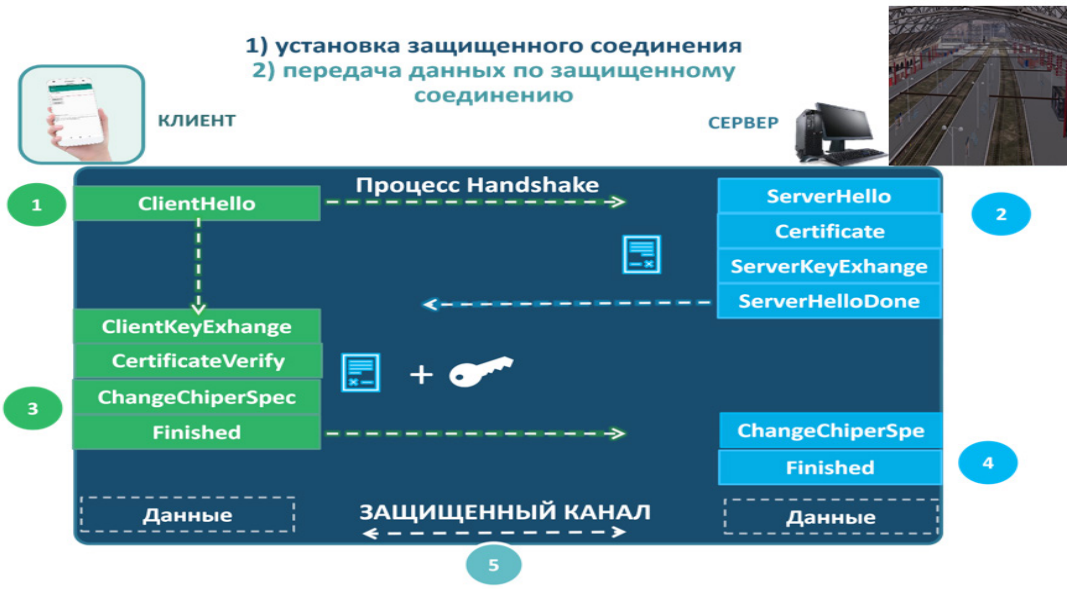

Рис. 6. Схема установления защищенного соединения по протоколу TLS 1.3 между клиентом и сервером.

Результаты и обсуждение

В ходе исследования была создана интегрированная система для безопасного управления сетями охранного освещения с помощью приложения для Android, основанного на современных протоколах шифрования. Система защищает каналы связи между центральными серверами и блоками управления с помощью передовых механизмов TLS/SSL, обеспечивая надежную защиту от взлома и попыток перехвата.

Технологические результаты подтвердили высокую эффективность системы с точки зрения производительности: среднее время отклика при передаче команд управления составляет от 120 до 250 миллисекунд, что соответствует приемлемым параметрам для систем безопасности, требующих высокой скорости реагирования. Система также показала энергоэффективность: благодаря использованию усовершенствованных алгоритмов шифрования расход заряда батареи не превышал 5% после длительного использования.

С точки зрения безопасности система эффективно предотвращала различные виды кибератак, такие как атаки типа «человек посередине» (MITM) и атаки с повторным воспроизведением, благодаря строгой реализации механизма закрепления сертификатов и применению высоконадежных протоколов шифрования. Тестирование сетевого анализа с использованием таких инструментов, как Wireshark, подтвердило отсутствие каких-либо уязвимостей безопасности в отправляемых пакетах, поскольку все данные были зашифрованы с использованием алгоритма TLS_AES_256_GCM_SHA384.

По сравнению с традиционными незащищенными альтернативами, система имеет значительное преимущество перед традиционными системами безопасности за счет умеренного компромисса во времени отклика, что является рациональным компромиссом для обеспечения безопасности данных. Система также обладает высокой степенью адаптации к работе на различных версиях Android, начиная с версии 7, благодаря правильной настройке файлов конфигурации сетевой безопасности.

В целом, исследование подтвердило возможность практического внедрения этой системы в таких критически важных средах без-

опасности, как интеллектуальные системы уличного освещения и правительственные здания. Кроме того, она имеет потенциал для будущего применения, выходящего за рамки предоставления более широкого спектра устройств или более передовых технологий, таких как промышленный Интернет вещей (IIoT) или блокчейн, для обеспечения более высокого уровня надежности и безопасности. Мы также рекомендуем включить биометрическую аутентификацию посредством распознавания лиц, создав алгоритм проверки распознавания лиц, основанный на машинном обучении, глубоком обучении и нейронных сетях.

Заключение

Выводы исследования представлены советами по разработке под систему Android для управления охранным освещением, а ещё способом разработки протокола управления охранным освещением.

В работе дан анализ предметной области, и, собственно, в том числе: управляемая система охранного освещения, структурный анализ составляющей системы охранного освещения, анализ угроз посту управления охранным освещением.

Предоставлен анализ актуального протокола для управления охранным освещением, анализ функций и составляющую разработки под Android для управления охранным освещением и анализ протокола SSL/TLS.

Выбраны инструменты разработки системы, произведена проверка среды, по результатам которой, определены возможности по созданию мобильного приложения, управляющего светильником СОО.

Разработано приложение для операционной системы Android для управления охранным освещением. Проведен анализ системы аутентификации и идентификации пользователей, выполнен анализ соединения между приложением Android и сервером на уровне сокетов. По результатам анализа спроектирован и реализован протокол удаленного и безопасного управления устройством системы охранного освещения.

Литература

1. Водовозов, А. М. Интеллектуальная система уличного освещения на основе парадигмы Интернета вещей / А. М. Водовозов, А. В. Бурцев // Вестник Череповецкого государственного университета. – 2021. – № 3(102). – С. 7-17. – DOI 10.23859/1994-0637-2021-3-102-1.

2. Hofer, Florian, and Barbara Russo. "Architecture and its vulnerabilities in smart-lighting systems." Technologies for Smart Cities. Cham: Springer International Publishing, 2022. 155–181.

3. Stellios, I., Mokos, K., & Kotzanikolaou, P. (2021, October). Assessing vulnerabilities and IoT-enabled attacks on smart lighting systems. In European Symposium on Research in Computer Security (pp. 199–217). Cham: Springer International Publishing.

4. Ma, Chen. "Smart city and cyber-security; technologies used, leading challenges and future recommendations." Energy Reports 7 (2021): 7999–8012.

5. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975–121995.

6. Abdalzaher, M. S., Fouda, M. M., Elsayed, H. A., & Salim, M. M. (2023). Toward secured iot-based smart systems using machine learning. IEEE access, 11, 20827–20841.

7. Namane, Sarra, et al. "Blockchain-based authentication scheme for collaborative traffic light systems using fog computing." Electronics 12.2 (2023): 431.

8. Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices: The case of smart lights." 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.

9. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.

10. Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications, 137, 1–10.

11. Zeng, Pengjie, et al. "A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology." IEEE access 8 (2020): 33644–33657.

12. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975–121995.

13. Khan, A., Jhanjhi, N. Z., & Humayun, M. (2022). The role of cybersecurity in smart cities. In Cyber Security Applications for Industry 4.0 (pp. 195-208). Chapman and Hall/CRC.

14. Gupta, S., Alharbi, F., Alshahrani, R., Kumar Arya, P., Vyas, S., Elkamchouchi, D. H., & Soufiene, B. O. (2023). Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. Sustainability, 15(6), 5346.

15. Камель, М. Х. К. Безопасный многофакторный алгоритм аутентификации для пользователей электросистемы / М. Х. К. Камель, Т. Р. Ахмед, А. В. Авсиевич // Мехатроника, автоматизация и управление на транспорте: Материалы vii всероссийской научно-практической конференции, Самара, 04 апреля 2025 года. – Самара: Приволжский государственный университет путей сообщения, 2025. – С. 67–70.

16. Камель, М. Х. К. Многофакторная аутентификация для мобильных систем контроля доступа / М. Х. К. Камель, Т. Р. Ахмед, А. В. Авсиевич // I-methods. – 2025. – Т. 17, № 2.

17. Распоряжение от 17 апреля 2018 г. N 769/р об утверждении стратегии научно-технологического развития холдинга «РЖД» на период до 2025 года и на перспективу до 2030 года (БЕЛАЯ КНИГА). URL: http://cipi.samgtu.ru/sites/cipi.samgtu.ru/files/belaya_kniga.pdf (дата посещения: 24.01.2026).

References

1. Vodovozov, A. M. Intellektual`naya sistema ulichnogo osveshheniya na osnove paradigmy` Interneta veshhej / A. M. Vodovozov, A. V. Burcev // Vestnik Cherepoveczkogo gosudarstvennogo universiteta. – 2021. – № 3(102). – S. 7-17. – DOI 10.23859/1994-0637-2021-3-102-1.

2. Hofer, Florian, and Barbara Russo. "Architecture and its vulnerabilities in smart-lighting systems." Technologies for Smart Cities. Cham: Springer International Publishing, 2022. 155–181.

3. Stellios, I., Mokos, K., & Kotzanikolaou, P. (2021, October). Assessing vulnerabilities and IoT-enabled attacks on smart lighting systems. In European Symposium on Research in Computer Security (pp. 199-217). Cham: Springer International Publishing.

4. Ma, Chen. "Smart city and cyber-security; technologies used, leading challenges and future recommendations." Energy Reports 7 (2021): 7999–8012.

5. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975–121995.

6. Abdalzaher, M. S., Fouda, M. M., Elsayed, H. A., & Salim, M. M. (2023). Toward secured iot-based smart systems using machine learning. IEEE access, 11, 20827–20841.

7. Namane, Sarra, et al. "Blockchain-based authentication scheme for collaborative traffic light systems using fog computing." Electronics 12.2 (2023): 431.

8. Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices: The case of smart lights." 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.

9. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.

10. Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications, 137, 1–10.

11. Zeng, Pengjie, et al. "A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology." IEEE access 8 (2020): 33644–33657.

12. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975–121995.

13. Khan, A., Jhanjhi, N. Z., & Humayun, M. (2022). The role of cybersecurity in smart cities. In Cyber Security Applications for Industry 4.0 (pp. 195–208). Chapman and Hall/CRC.

14. Gupta, S., Alharbi, F., Alshahrani, R., Kumar Arya, P., Vyas, S., Elkamchouchi, D. H., & Soufiene, B. O. (2023). Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. Sustainability, 15(6), 5346.

15. Kamel`, M. X. K. Bezopasny`j mnogofaktorny`j algoritm autentifikacii dlya pol`zovatelej e`lektrosistemy` / M. X. K. Kamel`, T. R. Axmed, A. V. Avsievich // Mexatronika, avtomatizaciya i upravlenie na transporte: Materialy` vii vserossijskoj nauchno-prakticheskoj konferencii, Samara, 04 aprelya 2025 goda. – Samara: Privolzhskij gosudarstvenny`j universitet putej soobshheniya, 2025. – S. 67–70.

16. Kamel`, M. X. K. Mnogofaktornaya autentifikaciya dlya mobil`ny`x sistem kontrolya dostupa / M. X. K. Kamel`, T. R. Axmed, A. V. Avsievich // I-methods. – 2025. – T. 17, № 2. Mnogofaktornaya autentifikaciya dlya mobil`ny`x sistem kontrolya dostupa / M. X. K. Kamel`, T. R. Axmed, A. V. Avsievich // I-methods. – 2025. – T. 17, № 2.

17. Rasporyazhenie ot 17 aprelya 2018 g. N 769/r ob utverzhdenii strategii nauchno-texnologicheskogo razvitiya xoldinga RZhD na period do 2025 goda i na perspektivu do 2030 goda (BELAYa KNIGA). URL: http://cipi.samgtu.ru/sites/cipi.samgtu.ru/files/belaya_kniga.pdf (data poseshheniya: 24.01.2026).

АСИЕВИЧ Александр Викторович, кандидат технических наук, доцент федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет», доцент федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации 443099, Российская Федерация, г. Самара, ул. Чапаевская, 89, E-mail: a.v.avsievich@samsmu.ru

АХМЕД Тамер Рашид, аспирант федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет», Преподаватель в университете Диялы в Республике Ирак, г. Баакуб. 443100, г. Самара, ул. Молодогвардейская, 244. E-mail: thameer987@gmail.com

КАМЕЛЬ Мохамад Хашим кахлил, аспирант федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет». 443100, г. Самара, ул. Молодогвардейская, 244. E-mail: mohkamel780@gmail.com

AVSIEVICH Alexander Viktorovich, Candidate of Technical Sciences, Associate Professor Federal Budgetary State Educational Institution of Higher Education "Samara State Technical University", Associate Professor of the Federal State Budgetary Educational Institution of Higher Education "Samara State Medical University" of the Ministry of Health of the Russian Federation, 89 Chapaevskaya str., Samara, 443099, Russian Federation. E-mail: a.v.avsievich@samsmu.ru

AHMED Tamer Rashid, postgraduate student of the Federal budgetary State Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str., 244. E-mail: thameer987@gmail.com

KAMEL Mohamad Hashim kahlil, postgraduate student at the Federal Budgetary State Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str., 244. E-mail: mohkamel780@gmail.com

УДК 004.056.53 Вестник УрФО № 1(59) / 2026, с. 48–57

Ощепков Н.В., Южаков А.А., Кротова Е.Л. DOI: 10.14529/secur260105

ВРЕМЕННЫЕ ИНТЕРВАЛЫ СВЯЗИ КАК ФАКТОР ДОВЕРИЯ В ПРОТОКОЛЕ MODBUS RTU

В работе предлагается метод повышения безопасности протокола Modbus RTU путём введения механизма временных контрактов и HMAC-аутентификации. Отсутствие встроенных средств защиты в протоколе Modbus делает системы АСУ ТП уязвимыми к атакам типа «человек посередине» и подмены узлов. Предложенный метод основан на предварительном согласовании временных интервалов обмена данными между ведущим и ведомыми устройствами с криптографической верификацией на основе HMAC. Метод обеспечивает совместимость с существующей инфраструктурой и не требует значительных вычислительных ресурсов, что делает его применимым для промышленных контроллеров с ограниченными возможностями. Экспериментальная проверка подтвердила эффективность метода в предотвращении несанкционированного доступа при минимальных накладных расходах.

Ключевые слова: *Modbus RTU, информационная безопасность АСУ ТП, HMAC, временные контракты, аутентификация устройств.*

Oshchepkov N.V., Yuzhakov A. A., Krotova E. L.

COMMUNICATION TIME INTERVALS AS A TRUST FACTOR IN THE MODBUS RTU PROTOCOL

This paper proposes a method for enhancing the security of the Modbus RTU protocol by introducing a time-based contract mechanism and HMAC authentication. The lack of built-in security features in the Modbus protocol makes ICS systems vulnerable to man-in-the-middle attacks and node spoofing. The proposed method is based on pre-negotiating data exchange time intervals between the master and slave devices with cryptographic verification based on HMAC. The method ensures compatibility with existing infrastructure and does not require significant computing resources, making it suitable for industrial controllers with limited capabilities. Experimental testing confirmed the method's effectiveness in preventing unauthorized access with minimal overhead.

Keywords: *Modbus RTU, ICS information security, HMAC, time-based contracts, device authentication.*

Введение

В связи с активным внедрением устройств, обеспечивающих автоматизацию различных технологических процессов, особую актуальность приобретает проблема доверия к сценариям функционирования вычислительных систем. Как известно, полностью защищённых информационных систем не существует [1],

что обусловливает необходимость реализации мер, направленных на снижение вероятности и последствий инцидентов информационной безопасности.

Протокол Modbus на протяжении десятилетий остаётся одним из наиболее распространённых средств обмена данными в промышленной автоматике. Простота его реализации, открытость спецификаций и совместимость с широким спектром оборудования способствуют его активному применению в различных отраслях промышленности [2]. Поэтому, согласно статистике, широко распространён и активно применяется в промышленной автоматизации в качестве основного или вспомогательного протокола связи [3].

Однако использование Modbus в режиме RTU сопровождается рядом существенных ограничений с точки зрения информационной безопасности. Отсутствие механизмов верификации узлов и защиты целостности сообщений создаёт предпосылки для реализации атак типа «человек посередине» и «подмена данных» [4, 5], что может представлять угрозу для надёжности функционирования критически важных систем. Даже при наличии физических ограничений доступа к инфраструктуре, использующей устройства автоматизации, сохраняется риск компрометации системы.

Протокол Modbus использует архитектуру «ведущий-ведомый» (master-slave) [6], в которой ведущее устройство инициирует запросы, а ведомые устройства отвечают на них. Базовая версия протокола Modbus определяет набор функций, обеспечивающих обмен данными между устройствами. При этом в спецификации протокола предусмотрены также зарезервированные коды функций, не имеющие программной реализации и предназначенные для пользовательского расширения. Такая архитектура делает протокол Modbus гибким и позволяет адаптировать его под специфические задачи, включая интеграцию дополнительных механизмов защиты и аутентификации.

Следует отметить, что спецификация протокола Modbus допускает использование широковещательных (broadcast) запросов, адресуемых всем узлам сети. В таких случаях в качестве идентификатора ведомого устройства используется значение 0 (нулевой slave ID). Особенность данного режима заключается в том, что он не позволяет однозначно идентифицировать конкретного получателя сообщения, что создаёт дополнительные требования к механизмам аутентификации.

Основные уязвимости

Ниже представлены основные уязвимости протокола, которые предполагается парировать на основании нового предложенного метода, а именно отсутствие:

• **аутентификации**. Протокол не содержит встроенных механизмов проверки подлинности отправителя и получателя сообщений. Любое устройство, подключённое к сети, может инициировать запросы или отвечать на них от имени легитимного узла

• **шифрования**. Все данные передаются в открытом виде, что позволяет злоумышленнику перехватывать и анализировать содержимое сообщений

• **контроля целостности**. Хотя протокол использует контрольную сумму CRC16 для обнаружения ошибок передачи, этот механизм не защищает от преднамеренной модификации данных злоумышленником, который может пересчитать CRC для изменённого пакета

• **защиты от повторного воспроизведения (replay attacks)**. Перехваченное легитимное сообщение может быть повторно отправлено в сеть для выполнения несанкционированных действий

Рассматриваемые типы атак на Modbus RTU

Рассмотрим в дальнейшем следующие виды возможных атак в промышленной системе:

Атака типа «подмена узла» (spoofing) [5]. Злоумышленник может выдавать себя за легитимное ведущее или ведомое устройство, отправляя команды или ложные ответы.

Атака типа «человек посередине» (MITM) [6]. Злоумышленник перехватывает коммуникацию между мастером и слейвом, имея возможность модифицировать, задерживать или подменять сообщения.

Атака повторного воспроизведения (replay attack). Перехваченные легитимные команды повторно отправляются для выполнения несанкционированных действий.

С учетом особенности функционирования протокола Modbus где в качестве двух взаимодействующих типов устройств действуют «ведущее устройство» (мастер), отправляющее команды, и «ведомое устройство» (слейв), принимающее команды, предлагается возложить инициативу на создание

контракта взаимодействия между устройствами на ведущее устройство.

Описание эксперимента

Для анализа возможностей реализации предлагаемого метода увеличения защищенности и получения оценок был проведен эксперимент с использованием программной реализации master на языке Python и библиотеки pyModbus и slave в виде запрограммированного микроконтроллера. В ходе эксперимента были произведены оценки задержек внутри сети. На рис. 1 представлена схема подключения микроконтроллера на базе ESP32 к ПК на операционной системе Windows 10 через интерфейс RS-485 [7].

Оценка задержки производилось на основе запрограммированной пользовательской функции. Суть функции заключается в том, что мастер формирует кадр данных с длиной 4 байта: адрес slave, код функции и 2 байта CRC16 [8]. В момент отправки мастер фиксирует время отправки. Slave, получив фрейм, добавляет в кадр количество времени, затраченное на вычисления при обработ-

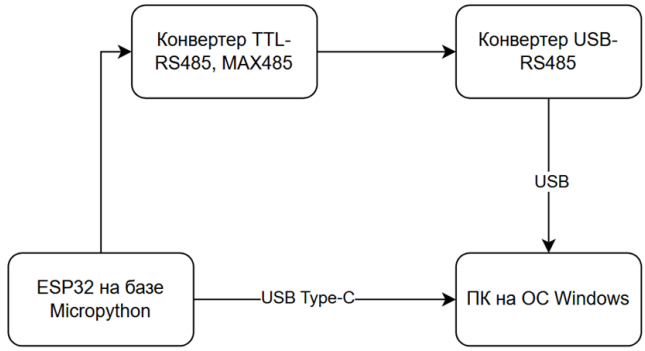

Рис. 1. Схема экспериментальной установки с подключением микроконтроллера к ПК по интерфейсу RS-485

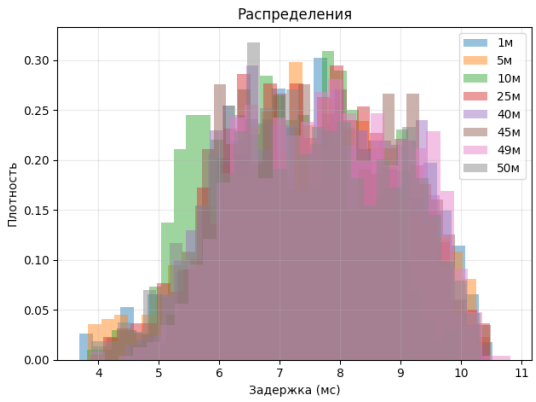

Рис. 2. Распределение задержек доставки кадра до слейва при скорости 9600 бит/с

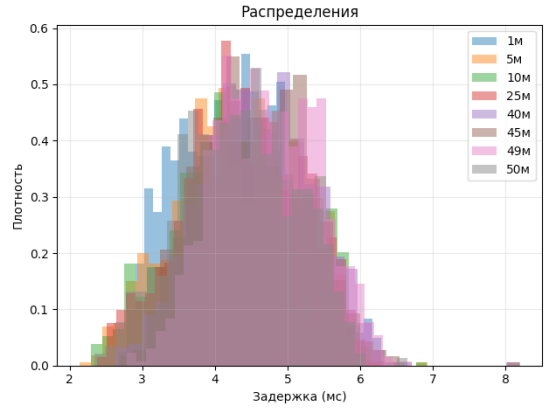

Рис. 3. Распределение задержек доставки кадра до слейва при скорости 19200 бит/с

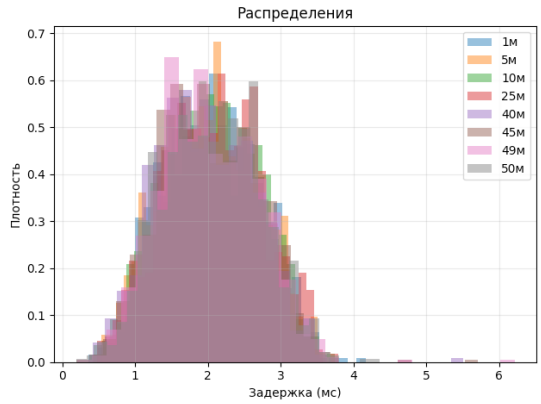

Рис. 4. Распределение задержек доставки кадра до слейва при скорости 115200 бит/с

Параметр	1м	5м	10м	25м	40м	45м	49м	50м
Среднее	7.59	7.47	7.08	7.50	7.55	7.63	7.78	7.43
Медиана	7.62	7.49	7.08	7.51	7.57	7.61	7.80	7.37
σ	1.42	1.43	1.25	1.34	1.32	1.32	1.30	1.40
Мин	3.68	3.83	3.82	3.87	4.45	4.52	3.88	3.89
Макс	10.53	10.48	9.95	10.48	10.46	10.50	10.81	10.32

Рис. 5. Сводная таблица значений для различных длин кабеля при скорости 9600 бит/с

Параметр	1м	5м	10м	25м	40м	45м	49м	50м
Среднее	4.24	4.34	4.38	4.38	4.58	4.54	4.71	4.32
Медиана	4.25	4.34	4.40	4.37	4.59	4.53	4.69	4.33
σ	0.76	0.83	0.84	0.79	0.75	0.73	0.70	0.78
Мин	2.67	2.13	2.29	2.38	2.62	2.69	2.79	2.34
Макс	6.29	6.93	6.92	6.33	8.20	8.20	6.71	6.64

Рис. 6. Сводная таблица значений для различных длин кабеля при скорости 19200 бит/с

Параметр	1м	5м	10м	25м	40м	45м	49м	50м
Среднее	2.05	2.02	2.04	2.08	1.96	2.01	2.01	2.07
Медиана	2.04	2.00	2.03	2.08	1.93	1.96	1.96	2.07
σ	0.63	0.64	0.64	0.66	0.66	0.66	0.66	0.66
Мин	0.36	0.54	0.43	0.47	0.41	0.19	0.20	0.20
Макс	4.17	3.62	3.75	3.79	5.51	5.71	6.21	4.36

Рис. 7. Сводная таблица значений для различных длин кабеля при скорости 115200 бит/с

ке кадра. После получения мастером ответа от slave, он рассчитывает полный период за исключением вычислений, которые поступили в кадре и делит полученное значение на 2. Это значение и является временем, через которое первый байт фрейма достигает целевого слейва. В качестве кабеля связи была использована витая пара типа CAT5e с длинами 1, 5, 10, 25, 40, 45, 49, 50 метров. Также стоит отметить, что оценка задержек производилась с различными значениями скоростей передачи (baudrate): 9600, 19200, 115200 бит/с. На рис. 2, 3, 4 представлены графики распределения длительности полного цикла общения для 1000 измерений с различным интервалом отправки кадра.

Выше представлены сводные таблицы с характеристиками системы для каждого из битрейтов.

Для корректного применения параметрических статистических методов анализа данных необходимо было проверить гипотезу о нормальности распределения полученных измерений задержек с помощью статистического критерия.

Для проверки гипотезы о нормальности эмпирических распределений задержек применялся критерий Шапиро–Уилка [9], являю-

щийся наиболее мощным непараметрическим критерием согласия при объёме выборки $n \leq 5000$.

При объёме выборки $n = 1000$ критерий Шапиро–Уилка обладает повышенной чувствительностью и отвергает нулевую гипотезу даже при незначительных отклонениях, не имеющих практического значения. Поэтому наряду с критерием Шапиро–Уилка выполнялась оценка коэффициентов асимметрии и эксцесса, а также проверка по эмпирическому правилу трёх сигм [10]. Расчёты выполнены для трёх скоростей передачи данных (9600, 19200 и 115200 бод) и восьми длин кабеля (1, 5, 10, 25, 40, 45, 49 и 50 м), объём каждой выборки 1000 измерений.

Статистика Шапиро–Уилка для 9600 бод: $W = 0{,}9751–0{,}9913$. Коэффициент асимметрии составил от −0,203 до +0,030, что свидетельствует о практически симметричном распределении. Отрицательный эксцесс в диапазоне от −0,510 до −1,014 указывает на незначительное уплощение вершины по сравнению с нормальным законом, обусловленное дискретностью системных таймеров операционной системы и джиттером интерпретатора Python.

Результаты проверки правила трёх сигм:

• интервал ±1σ: 59,80–66,30% (теор. 68,27%, среднее $\Delta = 5{,}67\%$);

• интервал ±2σ: 96,60–98,60% (теор. 95,45%, среднее $\Delta = 2{,}17\%$);

• интервал ±3σ: 100,00% для всех выборок (теор. 99,73%, $\Delta < 0{,}27\%$).

Статистика Шапиро–Уилка для 19200 бод: $W = 0{,}9836–0{,}9935$. Асимметрия: от −0,124 до +0,280, эксцесс: от -0,682 до -0,111 – отклонения минимальны.

Результаты проверки правила трёх сигм:

• интервал ±1σ: 64,00–67,40% (теор. 68,27%, среднее $\Delta = 3{,}04\%$);

• интервал ±2σ: 96,30–97,70% (теор. 95,45%, среднее $\Delta = 1{,}64\%$);

• интервал ±3σ: 99,90–100,00% ($\Delta < 0{,}27\%$).

Статистика Шапиро–Уилка для 115200 бод: $W = 0{,}9809–0{,}9936$. Асимметрия: от −0,007 до +0,390, эксцесс: от −0,676 до +1,025. При длинах кабеля 45–49 м наблюдается незначительный положительный эксцесс, что может объясняться увеличением доли передискретизированных пакетов на высокой скорости передачи.

Результаты проверки правила трёх сигм:

• интервал ±1σ: 63,90–66,80% (теор. 68,27%, среднее $\Delta = 2{,}68\%$);

• интервал ±2σ: 96,50–97,40% (теор. 95,45%, среднее $\Delta = 1{,}54\%$);

• интервал ±3σ: 99,80–100,00% ($\Delta < 0{,}27\%$).

По результатам проверки критерием Шапиро–Уилка и правилом трёх сигм установлено, что для всех исследуемых скоростей передачи данных и длин кабеля эмпирические распределения задержек Modbus RTU демонстрируют достаточную близость к нормальному закону. Отклонения эмпирических частот от теоретических значений не превышают 8,5% для интервала ±1σ, 3,2% - для ±2σ и 0,3% - для ±3σ. Умеренный отрицательный эксцесс, наблюдаемый преимущественно при скорости 9600 бод ($\gamma_2 = −0{,}51...−1{,}01$), обусловлен системными артефактами измерительной среды и не препятствует применению параметрических статистических методов для дальнейшего анализа зависимости задержек от длины кабеля и скорости передачи данных.

Важным результатом проведённых экспериментов является отсутствие статистически значимой зависимости между длиной кабеля в исследуемом диапазоне от 1 до 50 метров и величиной задержки передачи данных. Это свидетельствует о том, что время распространения сигнала по физической среде передачи пренебрежимо мало по сравнению с другими составляющими общей задержки, такими как время обработки запроса в микроконтроллере, формирование ответа и программные задержки в мастере-устройстве.

В тоже время, анализ измерений показал, что среднее значение стандартного отклонения задержек зависит от скорости передачи данных.

Для скорости 9600 бит/с среднее стандартное отклонение составило 1,35 мс, что отражает наибольшую вариабельность времени отклика в системе. При увеличении скорости передачи до 19200 бит/с среднее стандартное отклонение снизилось до 0,77 мс, демонстрируя повышение стабильности обмена данными. Наименьшая вариабельность наблюдалась при скорости 115200 бит/с, где среднее стандартное отклонение составило 0,65 мс. Результаты представлены в таблице 1.

Снижение стандартного отклонения с ростом скорости передачи данных может быть объяснено сокращением времени передачи кадра по физическому каналу, что уменьшает влияние временных флуктуаций в системе на общую задержку. При более высоких скоро-

Таблица 1

Среднее значение задержки и стандартное отклонение при различных скоростях передачи данных

baudrate, бит/с	$\bar{x}$, мс	σ, мс
9600	7,50	1,35
19200	4,44	0,77
115200	2,03	0,65

стях передачи относительный вклад времени передачи в общую задержку уменьшается, что приводит к более предсказуемому и стабильному времени отклика системы.

Предлагаемый метод заключения контракта

Суть предлагаемого метода заключения контракта состоит в предварительной договорённости между мастером и slave о сеансах связи, в которые мастер устройство посылает команды, а slave отвечает. Таким образом, предполагается, что наличие у мастера сведений о том, в какой временной интервал отправлять посылку, может служить критерием легитимности устройства.

Ключевое ограничение: мастера, которые не договорились со slave о временном интервале связи, не отвечают ни на одну команду чтения или записи, посылаемую им от любого slave в сети.

В рамках предложенного подхода реализован метод криптографической верификации узлов, основанный на механизме HMAC (Hash-based Message Authentication Code), подробно описанном в стандарте RFC 4226 [11]. Данный механизм представляет собой метод проверки подлинности сообщений, основанный на использовании криптографической хэш-функции в сочетании с общим секретным ключом. Основная цель HMAC - обеспечение целостности передаваемых данных и подтверждение аутентичности сторон, участвующих в обмене.

В разрабатываемой реализации в качестве входных данных для HMAC используется временная метка (Unix timestamp), для которой вычисляется хэш с применением алгоритма семейства SHA-1 и индивидуального секретного ключа ведомого устройства. Результат вычисления преобразуется в массив байтов, после чего выполняется динамическое усечение. Итоговое значение форматируется в строку фиксированной длины, что обеспечивает корректное отображение возможных лидирующих нулей (например, «003451»). Для сохранения таких нулей результат кодируется в ASCII, что гарантирует точную передачу данных при обмене.

Используя широковещательные запросы, каждый из slave получит сообщение о заключении контракта и произведёт вычисление HMAC на основе своего индивидуального ключа. Данный механизм позволяет slave убедиться в том, что инициатор взаимодействия (мастер) действительно является легитимным участником сети.

В рамках системы безопасности мастер хранит полный набор секретных ключей, каждый из которых индивидуально соответствует конкретному slave. Мастера, в свою очередь, содержат свои уникальные ключи, сохранённые в энергонезависимой памяти. Формат ключей представлен в виде base32-кодированных последовательностей символов, что обеспечивает их совместимость с текстовыми интерфейсами, средствами диагностики и стандартными инструментами обработки данных.

Описание алгоритма

Изначально необходимо задать 2 базовые величины:

- T – период открытия окна (Step)
- D – длительность окна приёма сигнала (Duration)

Как было описано ранее, протокол обладает рядом кодов функций, зарезервированных для реализации пользователем. Благодаря этому была запрограммирована функция заключения контракта, кадр которой представлен на рис. 8.

Поскольку запрос является широковещательным, ID slave – всегда 0. Благодаря включаемым в фрейм компонентам timestamp – временная метка отправки мастером сообщения и HMACm, вычисленной на основе временной метки и ключа slave, с которым мастер заключает контракт, лишь единственный slave, вычислив на своей стороне

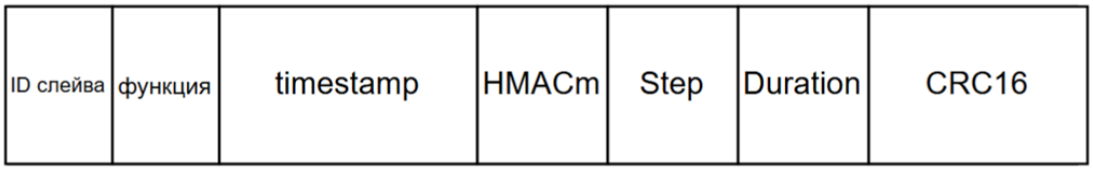

Рис. 8. Формат кадра для заключения контракта об окнах связи

HMAC(timestamp) и сравнив его с HMACm, полученным в фрейме, установит соответствие. Именно это и будет являться критерием, по которому данный slave поймет, что сообщение адресовано ему.

Получив запрос и проверив одноразовый код, slave сохраняет в памяти временную метку, в которую поступил запрос, чтобы в дальнейшем производить расчет попадания запросов мастера в окно длительности D через каждые T мс.

Оценка момента времени

Как было отмечено выше, время доставки пакета от мастера к слейву описывается нормальным распределением:

$$\tau \sim N(\mu,\sigma^2)$$

В момент времени $t_0^{(M)}$ (по локальным часам мастера) мастер отправляет сообщение синхронизации slave. Slave в свою очередь принимает фрейм в момент времени:

$$t_0^{(S)} = t_0^{(M)} + \tau_0,$$

где τ_0 – реализация случайной величины задержки для данной передачи.

Поскольку $\tau_0 \in [\mu - 3\sigma; \mu + 3\sigma]$, с высокой вероятностью оценка момента прибытия с точки зрения мастера:

$$t_0^{(S)} = t_0^{(M)} + \mu,$$

что соответствует математическому ожиданию интервала неопределенности.

Для определения момента отправки очередного запроса мастер вычисляет время, прошедшее с момента установления синхронизации:

$$\Delta t = t_{текущее}^{(M)} - t_0^{(M)}.$$

Полный период цикла рассчитывается по формуле :

$$C = T + D.$$

Тогда для определения момента отправки необходимо рассчитать фазу цикла (1):

$$\phi(t) = (\Delta t - \mu) \bmod C, \quad (1)$$

где вычитание μ компенсирует среднюю задержку при установлении контракта.

В свою очередь, границы, которым должна удовлетворять величина фазы соответствуют формулам (2) и (3):

$$\phi_{left} = k\sigma, \quad (2)$$

$$\phi_{right} = D - k\sigma, \quad (3)$$

где k – коэффициент безопасности.

Учитывая вышеизложенное передача разрешена при выполнении условия:

$$\phi_{left} \le \phi(t) \le \phi_{right}.$$

В условиях нестабильного сигнала и наличия в системе факторов, влияющих на задержку при обмене данными, в качестве коэффициента в (3) и (4) было выбрано число 4, а не 3, как это присуще для нормального распределения. Данный коэффициент исключает возможность выхода за границы доверительного интервала и ограничивает момент отправки на мастере. Таким образом (4), формируется ограничение для длительности окна D:

$$D>8\sigma. \quad (4)$$

В ходе проведения эксперимента были получены уточняющие положения, которые необходимо учитывать. Поскольку два устройства являются независимыми, то каждое из них обладает своим индивидуальным таймером, по которому определяется текущая временная метка. Как известно, существует понятие дрейфа таймеров, что со временем приводит к рассинхронизации. Именно поэтому необходимо производить ресинхронизацию с устройствами каждые 2-3 мин. Это позволит избежать проблемы оценки времени на мастере и slave.

С учетом представленных ранее видов атак, в алгоритме верификации на основе гаммирования с использованием секретного ключа, будут рассмотрены следующие сценарии атаки:

1. Злоумышленник отправляет кадр на slave, которое не заключило контракт.

2. Злоумышленник не знает об алгоритме гаммирования кадра и отправляет запрос на устройство, которое заключило контракт.

3. Злоумышленник знает алгоритм гаммирования кадра, но не знает ключ и временные интервалы.

В первом случае, поскольку злоумышленник отправляет кадр до того, как легитимный мастер заключил его, то ведомое устройство не отправляет ответ на запрос.

При реализации 2 сценария, необходимо предпринять следующие действия:

1. Изначально заключить контракт с использованием легитимного мастера.

2. Произвести подмену легитимного мастера на мастер злоумышленника.

3. Осуществить попытку отправки кадра.

Поскольку злоумышленник не знает об алгоритме гамирования, отправленная им команда не будет исполнена.

Реализация третьего сценария атаки может быть выполнена аналогично второму сценарию. Поскольку в данном этапе происходит двухфакторная верификация мастера как по гамирующему ключу, который может принимать значения [32768;65535], так и по временному окну, то можно вывести формулу расчета вероятности попадания кадра злоумышленника с угаданным ключом:

$$P = \frac{D}{(T+D)*32768}.$$

На рисунке 9 представлен график функции f(T,D) = D / (T+D). Из графика видно, что уменьшение величины D, и увеличение величины T приводит к уменьшению значения функции. Из этого следует, что чем реже возникает окно и чем оно короче, тем меньше вероятность реализации атаки подмены.

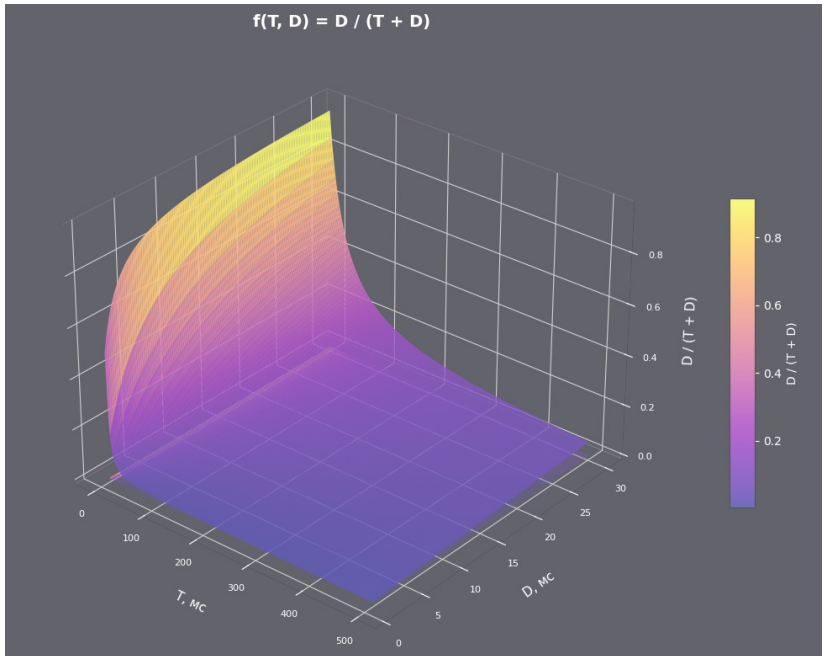

Рис. 9. График функции f(T,D) = D / (T+D)

Данная составляющая многоуровневой защиты slave от исполнения команд, полученных от мастера злоумышленника, сокращает вероятность успешной реализации атаки в 32768 раз, где 32768 – количество возможных ключей, используемых slave.

В разработанной модификации протокола первым этапом происходит применение функции гаммирования, а затем определение, попал ли кадр в заданный интервал. Благодаря этому, злоумышленник не определит, где он допустил ошибку: либо допущена ошибка при выборе ключа, либо некорректный момент отправки кадра. Именно это является двухэтапным методом проверки, что отправитель – легитимное устройство.

В качестве эксперимента для скорости 9600 бод/с и длины кабеля 10м были выбраны T = 250мс, D = 30мс. В случае, если верификация происходит только при гаммировании, то вероятность подбора ключа и исполнения команды равна 2^{15}. Та же атака, но при введении дополнительного этапа верификации по окнам связи снижает вероятность в $\frac{250+30}{30} = 9{,}33$ раза.

Выводы

Введение двухэтапной верификации, комбинирующей криптографическую аутентификацию через гаммирование и проверку посредством временных окон связи, фундаментально трансформирует модель угрозы в распределенных системах на базе протокола Modbus. При одноэтапной проверке злоумышленник решает задачу поиска в одномерном пространстве ключей мощностью N равной 32768. Двухэтапная схема переводит задачу атаки в двумерное пространство параметров, где необходимо одновременно подобрать корректный ключ и обеспечить попадание во временное окно длительностью D

внутри цикла C равного T+D. Статистическая независимость этих параметров даёт вероятность успешной атаки равную $\frac{D}{(T+D)*32768}$. Для экспериментальных параметров T равного 250 миллисекунд и D равного 30 миллисекунд достигается снижение вероятности атаки в 9.33 раза. Критическое свойство схемы заключается в принципе неразличимости ошибок. Система не предоставляет информации о причине отказа, формируя идентичный ответ при провале любой из проверок. Это лишает злоумышленника возможности декомпозиции задачи на последовательные этапы поиска временного окна и подбора ключа. Атакующий вынужден решать совместную задачу оптимизации без возможности адаптивной корректировки стратегии, что сохраняет мультипликативный характер защиты вместо аддитивного. Оптимальный выбор параметров обеспечивает коэффициент усиления защиты для промышленных сетей, что соответствует снижению вероятности успешной атаки на порядок величины при сохранении приемлемой пропускной способности канала.

Литература

1. Защита АСУ ТП: от теории к практике: сайт InformationSecurity. [Электронный ресурс]. – Режим доступа : https://lib.itsec.ru/articles2/Oborandteh/zaschita-asu-tp-ot-teorii-k-praktike (Дата обращения 01.03.2026)

2. Claudio Urrea, Claudio Morales, Enhancing Modbus-RTU Communications for Smart Metering in Building Energy Management Systems. Wiley. Online Library. [Электронный ресурс]. – Режим доступа : https://onlinelibrary.wiley.com/doi/full/10.1155/2019/7010717 (дата обращения 25.02.2026)

3. Industrial Network Market Analysis: сайт EBYTE. [Электронный ресурс]. – Режим доступа : https://www.cdebyte.com/news/1101 (дата обращения 01.03.2026)

4. Alakbarov R.G. Application and Security Issues of Internet of Things in Oil-Gas Industry // Alakbarov R.G., Hashimov M.A. // International Journal of Education and Management Engineering. – 2018. – №6, С. 24–36. https://doi.org/10.5815/ijeme.2018.06.03

5. Арзуманян Э.А. // МИТМ-атака. Угроза информационной безопасности в РФ // Арзуманян Э.А., Чумаков А.А. // Znanstvena Misel. – 2019. – № 8-1(33), С. 37–40.

6. Ведущий — ведомый: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Ведущий_—_ведомый (дата обращения 01.03.2026)

7. RS-485: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/RS-485 (дата обращения 01.03.2026)

8. Циклический избыточный код: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Циклический_избыточный_код (дата обращения 02.03.2026)

9. Shapiro, S. S. An analysis of variance test for normality (complete samples) // Shapiro, S. S. Wilk, M. B. // Biometrika. – 1965, T. 52, С. 591–611.

10. Gauss, C. F. Theoria motus corporum coelestium in sectionibus conicis solem ambientium // Cambridge University Press. – 2012.

11. RFC 4226: RFC Editor. [Электронный ресурс]. – Режим доступа: https://www.rfc-editor.org/info/rfc4226 (дата обращения 02.03.2026)

References

1. Zashchita ASU TP: ot teorii k praktike: sayt InformationSecurity. [Elektronnyy resurs]. – Rezhim dostupa: https://lib.itsec.ru/articles2/Oborandteh/zaschita-asu-tp-ot-teorii-k-praktike (Data obrashcheniya 01.03.2026)

2. Claudio Urrea, Claudio Morales, Enhancing Modbus-RTU Communications for Smart Metering in Building Energy Management Systems. Wiley. Online Library. [Электронный ресурс]. – Режим доступа : https://onlinelibrary.wiley.com/doi/full/10.1155/2019/7010717 (дата обращения 25.02.2026)

3. Industrial Network Market Analysis: сайт EBYTE. [Электронный ресурс]. – Режим доступа : https://www.cdebyte.com/news/1101 (дата обращения 01.03.2026)

4. Alakbarov R.G. Application and Security Issues of Internet of Things in Oil-Gas Industry // Alakbarov R.G., Hashimov M.A. // International Journal of Education and Management Engineering. – 2018. – №6, S. 24–36. https://doi.org/10.5815/ijeme.2018.06.03

5. Arzumanyan E.A. // MITM-ataka. Ugroza informatsionnoy bezopasnosti v RF // Arzumanyan E.A., Chumakov A.A. // Znanstvena Misel. – 2019. – № 8-1(33), S. 37–40.

6. Vedushchiy — vedomyy: Vikipediya. Svobodnaya entsiklopediya. [Elektronnyy resurs]. – Rezhim dostupa: https://ru.wikipedia.org/wiki/Vedushchiy_—_vedomyy (data obrashcheniya 01.03.2026)

7. RS-485: Vikipediya. Svobodnaya entsiklopediya. [Elektronnyy resurs]. – Rezhim dostupa: https://ru.wikipedia.org/wiki/RS-485 (data obrashcheniya 01.03.2026)

8. Tsiklicheskiy izbytochnyy kod: Vikipediya. Svobodnaya entsiklopediya. [Elektronnyy resurs]. – Rezhim dostupa: https://ru.wikipedia.org/wiki/Tsiklicheskiy_izbytochnyy_kod (data obrashcheniya 02.03.2026)

9. Shapiro, S. S. An analysis of variance test for normality (complete samples) // Shapiro, S. S. Wilk, M. B. // Biometrika. – 1965, T. 52, S. 591–611.

10. Gauss, C. F. Theoria motus corporum coelestium in sectionibus conicis solem ambientium // Cambridge University Press. – 2012.

11. RFC 4226: RFC Editor. [Электронный ресурс]. – Режим доступа: https://www.rfc-editor.org/info/rfc4226 (дата обращения 02.03.2026)

ЮЖАКОВ Александр Анатольевич, доктор технических наук, профессор, заведующий кафедрой Автоматика и телемеханика, Федеральное государственное автономное образовательное учреждение высшего образования «Пермский национальный исследовательский политехнический университет». 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: uz@at.pstu.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент кафедры Высшей математики, Федеральное государственное автономное образовательное учреждение высшего образования «Пермский национальный исследовательский политехнический университет». 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

ОЩЕПКОВ Никита Владимирович, аспирант кафедры Автоматика и телемеханика, Федеральное государственное автономное образовательное учреждение высшего образования «Пермский национальный исследовательский политехнический университет». 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: maserati_2000@mail.ru

YUZHAKOV Alexander Anatolyevich, Doctor of Technical Sciences, Professor, Head of the Department of Automation and Telemechanics, Federal State Autonomous Educational Institution of Higher Education “Perm National Research Polytechnic University”. 614990, Perm Region, Perm, Komsomolsky Prospekt, 29. E-mail: uz@at.pstu.ru

KROTOVA Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics, Federal State Autonomous Educational Institution of Higher Education “Perm National Research Polytechnic University”. 614990, Perm Region, Perm, Komsomolsky Prospekt, 29. E-mail: lenkakrotova@yandex.ru

OSHCHEPKOV Nikita Vladimirovich, postgraduate student of the Department of Automation and Telemechanics, Federal State Autonomous Educational Institution of Higher Education “Perm National Research Polytechnic University”. 614990, Perm Region, Perm, Komsomolsky Prospekt, 29. E-mail: maserati_2000@mail.ru

УДК 004.056:004.057.4 Вестник УрФО № 1(59) / 2026, с. 58–67

Сергин Д.А., Щерба Е.В.

DOI: 10.14529/secur260106

ПРОБЛЕМА ВЫБОРА БЕЗОПАСНОГО МНОЖЕСТВА ШЛЮЗОВ ПЕРЕСЫЛКИ В РАМКАХ ПРОТОКОЛА МАРШРУТИЗАЦИИ OLSR[1]

Концепция шлюзов пересылки в рамках протокола маршрутизации OLSR позволяет оптимизировать распространение сетевых пакетов в динамически организуемых сетях. В статье затрагивается проблема нарушения сетевой связности, связанная с некорректным выбором множества шлюзов пересылки. Представлен обзор и выполнен анализ научных работ, направленных на решение указанной проблемы. Определены отличительные особенности, достоинства и недостатки альтернативных подходов к выбору шлюзов пересылки. Обозначены перспективные направления для дальнейших исследований в рамках заданной проблематики.

Ключевые слова: *безопасность маршрутизации, сетевые атаки, задача о покрытии множества, протокол OLSR, выбор MPR.*

Sergin D. A., Shcherba E. V.

THE PROBLEM OF SELECTING A SECURE SET OF MULTIPOINT RELAYS WITHIN THE OLSR ROUTING PROTOCOL

The concept of multipoint relays (MPR) within the OLSR routing protocol enables optimization of network packet propagation in dynamically organized networks. This article addresses the problem of network node availability disruption due to the incorrect selection of multipoint relays. A review and analysis of papers aimed at solving this problem is presented. The distinctive features, advantages, and disadvantages of alternative approaches to multipoint relays selection are identified. Promising directions for further research within the given problems are outlined.

Keywords: *routing security, network attacks, set cover problem, OLSR protocol, MPR elections.*

[1] Исследование выполнено в ОмГТУ в рамках государственного задания Минобрнауки России на 2026–2028 годы НИР № FSGF-2026-0003.

Введение

Проактивный протокол маршрутизации OLSR [1] является одним из наиболее востребованных протоколов маршрутизации для динамически организуемых сетей различных типов. Ключевой особенностью протокола OLSR является процедура выбора подмножества шлюзов пересылки (MPR, Multipoint Relay) среди соседних узлов, которые дают возможность маршрутизации в пределах двушаговых соседних узлов. Узел, выбранный некоторым узлом в качестве шлюза MPR, отправляет служебные сообщения TC (Topology Control) на все доступные ему узлы, тем самым объявляя маршруты до каждого узла-селектора, выбравшего его в качестве шлюза MPR, в этих сообщениях. Все MPR-шлюзы выполняют пересылку полученных сообщений TC своим узлам-селекторам. После формирования базы данных топологии сети, каждый узел вычисляет оптимальные маршруты до всех доступных узлов.

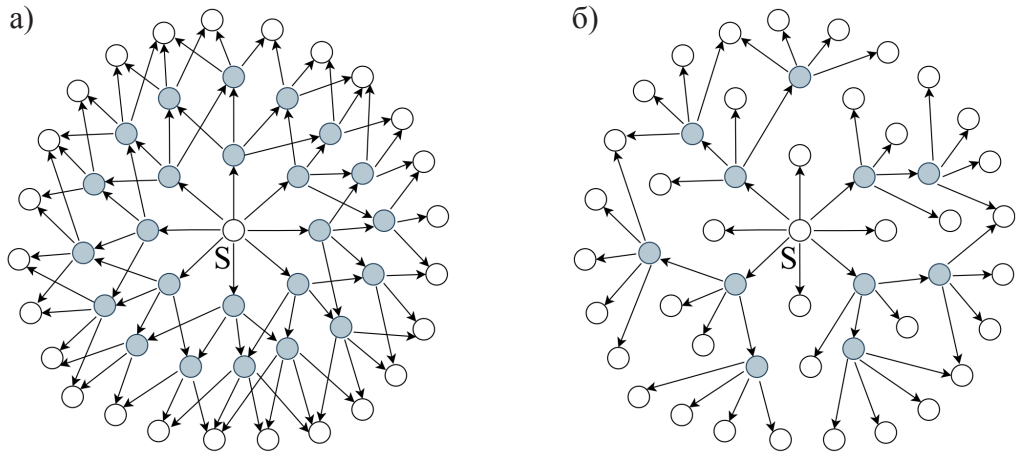

Рис. 1. Схема широковещательной рассылки: лавинная (а) и с использованием MPR (б)

Применение указанной концепции (рисунок 1) позволяет существенно сократить объём широковещательного трафика в сети путем исключения избыточных ретрансляций, производимых узлами в одной и той же физической сети.

Сама процедура выбора множества шлюзов пересылки узлом N предполагает, что узел определяет свой набор шлюзов MPR(N) из узлов, с которыми установлены симметричные отношения соседства. Выбор осуществляется таким образом, чтобы совокупные симметричные отношения соседства узлов, входящих в MPR(N), полностью охватывали все двушаговое окружение узла N (все соседи соседей узла N). То есть каждый узел в строгом симметричном двушаговом окружении узла N должен иметь хотя бы один симметричный канал с каким-нибудь узлом из MPR(N). Таким образом, чем меньше будет мощность множества MPR(N) для каждого узла сети N, тем меньше будет объём широковещательного трафика в сети.

Задача поиска оптимального множества шлюзов пересылки

Задача о покрытии множества (Set Cover Problem) широко известна в дискретной оптимизации [2] и имеет многочисленные приложения. Комбинаторная постановка задачи о покрытии множества состоит в следующем. Пусть даны множество $M = \{1, \ldots, m\}$ и набор его подмножеств $M_1, \ldots, M_n$, таких что $M_1 \cup \cup M_2 \cup \ldots \cup M_n = M$. Совокупность подмножеств M_j, $j \in J \subseteq \{1, \ldots, n\}$, называется покрытием множества M, если $\cup M_j = M$. Каждому M_j приписан вес $c_j \geq 0$. Требуется найти покрытие минимального суммарного веса. Задача называется невзвешенной, если все подмножества M_j имеют единичные веса.

Пусть задано множество вершин графа V, соответствующее множеству взаимодействующих узлов сети, множество дуг графа E, соответствующее множеству каналов связи, в множестве V задана вершина s, соответствующая узлу, для которого необходимо определить оптимальный набор шлюзов MPR. Пусть M представляет множество всех двушаговых симметричных соседей узла s, а для каждой вершины j, соседней к s, множество M_j соответствует множеству симметричных соседних узлов, за исключением самой вершины s. Тогда задача определения оптимального набора шлюзов MPR узлом s сводится к вышеприведенной постановке задачи поиска оптимального покрытия множества M.

В общем случае поиск покрытия минимального веса является NP-трудной задачей. Тем не менее для решения указанной задачи был предложен ряд приближенных алгоритмов, позволяющих осуществлять поиск решений, подходящих с некоторой погрешностью, и несколько эвристических алгоритмов, позволяющих оптимизировать поиск подходящего решения. Один из таких алгоритмов использован в рамках протокола маршрутизации OLSR для выбора оптимального множества шлюзов MPR.

В спецификациях протокола OLSR (RFC3626) [1] для выбора множества MPR предложен жадный эвристический алгоритм, целью которого является покрытие всех двушаговых соседей минимальным количеством шлюзов-ретрансляторов. Алгоритм оперирует двумя ключевыми множествами для каждого узла, выполняющего вычисления, а именно: множество одношаговых соседей (N) и множества двушаговых соседей (N2).

Ключевыми шагами алгоритма являются:

1. Во множество MPR включаются соседи из N, которые объявили готовность к ретрансляции (WILL_ALWAYS).

2. На втором этапе во множество MPR добавляются узлы из N, которые обеспечивают единственно возможный способ достижения узла из N2.

3. На третьем шаге, пока остаются непокрытые узлы из N2, происходит последовательный выбор узлов из N. Выбор происходит с учетом приоритета. В первую очередь оценивается количество узлов из N2, которые станут покрытыми с помощью выбора данного узла, во вторую очередь оценивается степень готовности к пересылке (willingness).

Таким образом, классическая реализация алгоритма позволяет минимизировать объем сетевого трафика при обеспечении полной сетевой связности, но не принимает во внимание аспекты безопасности, включая, например, обеспечение доступности сетевых узлов, что может быть использовано нарушителями для организации сетевых атак.

Модели нарушений безопасности, связанных с выбором множества шлюзов пересылки

К специфичным уязвимостям протокола маршрутизации OLSR можно отнести подверженность сетевым атакам, связанных с выбором множества шлюзов MPR [3]. В ходе подобных атак узел-нарушитель либо выбирает неполное множество шлюзов MPR, либо заставляет другие узлы вычислять некорректное множество MPR. Чтобы инициировать атаку, узел-нарушитель может либо генерировать управляющие пакеты с искажением идентификационной информации, либо сообщать о несуществующих каналах связи к другим узлам. Как следствие, узел-жертва вычисляет ошибочный набор шлюзов MPR, то есть некоторые из его соседей, доступных за два перехода, не охватываются по меньшей мере одним узлом в его множестве MPR.

Атака с подменой узла выполняется нарушителем, выдающим себя за другой узел в сети. В ходе данной атаки распространяется ложная информация об узлах, находящихся на расстоянии одного или двух шагов. Это позволяет повлиять на процесс выбора шлюзов. На рисунке 2(а) вредоносный узел x подменяет узел d и передает широковещательное сообщение HELLO, объявляющее канал связи с узлом c. Затем узел a получает сообщение HELLO от узла x, которое объявляет, что узел d имеет связь с узлами c и f. В этом случае узел a считает узел d единственным элементом в своем наборе MPR, что неверно. Таким образом, узел c становится недоступным и не сможет получить сообщения TC.

На рис. 2(б) представлен пример, когда нарушитель влияет на выбор MPR узла на расстоянии двух шагов. Вредоносный узел x подменяет узел c. Узлы f и e генерируют сообщения HELLO, в которых указывают узел c в качестве соседа с одним переходом. В результате атаки, узел a может неправильно выбрать узлы f или e в качестве шлюзов MPR. В этом случае узлы b и d не передают TC сообщения узлу c, поскольку они не включены в множество MPR.

Атака подмены канала связи выполняется вредоносным узлом, который сообщает о несуществующем канале другим узлам в сети. Цель нарушителя состоит в том, чтобы манипулировать информацией об узлах, находящихся на расстоянии одного или двух шагов, и быть выбранным в качестве шлюза MPR. После достижения указанной цели, вредоносный узел не генерирует и не пересылает сообщения TC, что приводит к нарушению доступности для узлов-селекторов.

На рис. 3(а) проиллюстрирована атака с нарушением лавинной рассылки из-за подмены канала. В этом примере узел x объявляет несуществующие каналы к существующим узлам e и c. Узел x отправляет сообщения HELLO и должен быть выбран в качестве шлю-

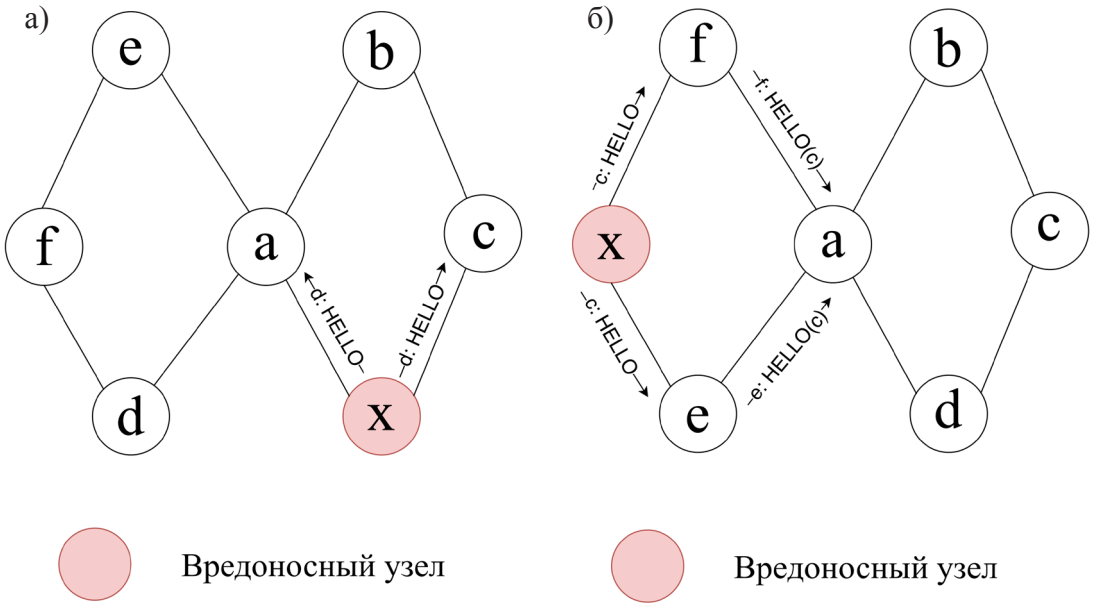

Рис. 2. Схема нарушений безопасности с подменой узла

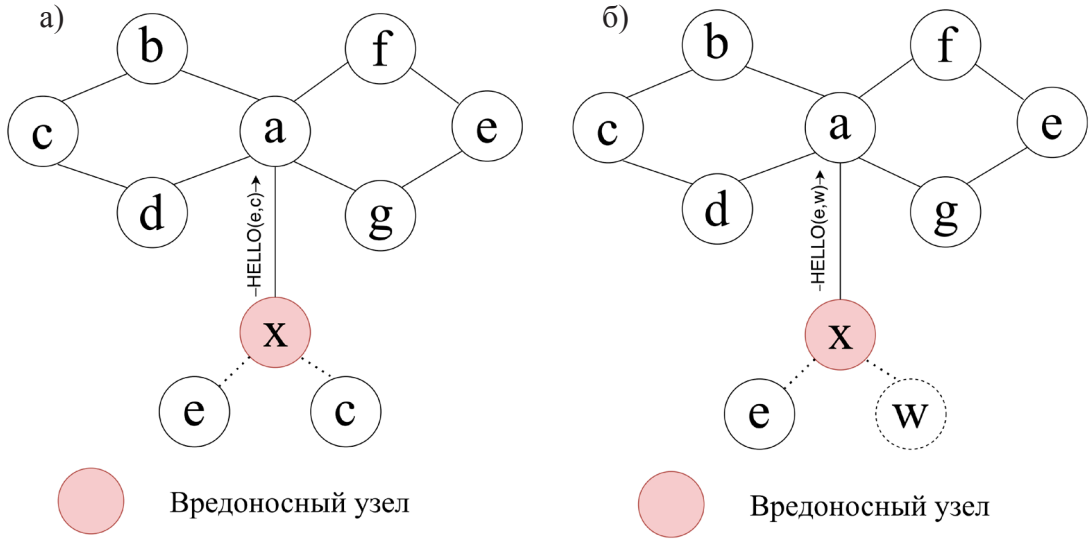

Рис. 3. Схема нарушений безопасности с подменой канала связи

за MPR узлом a. Узел a получает сообщения HELLO от узла x и неправильно вычисляет свое множество MPR, выбирая узел x как единственный узел, обеспечивающий связь с узлами e и c. В результате узел формирует ошибочный набор MPR, который может не обеспечивать покрытие всех его двушаговых соседей.

Альтернативный вариант данной атаки может быть выполнен узлом, который сообщает о канале связи с несуществующим узлом. Например, на рисунке 3(б) узел a вынужден выбрать узел x в качестве MPR, потому что это единственный узел, который обеспечивает связь с несуществующим узлом w. В этом случае вредоносный узел также получает возможность нарушить поток управляющей информации о топологии.

Причина возникновения описанных моделей атак кроется в отсутствии мер безопасности для классического протокола OLSR, где выбор множества шлюзов MPR производится без анализа достоверности полученной информации, а также без учета уровня риска для отдельно взятых узлов сети и каналов связи.

Альтернативные подходы к выбору шлюзов MPR

Для повышения доступности узлов и характеристик сетевого взаимодействия в рам-

ках протокола маршрутизации OLSR был предложен и реализован ряд альтернативных подходов к решению задачи выбора оптимального множества шлюзов MPR.

BW-OLSR

В рамках данного проекта предложен улучшенный алгоритм выбора шлюзов MPR. Особенность модификации заключается в использовании оценки пропускной способности каналов связи в качестве основной маршрутной метрики. Выбор шлюзов MPR осуществляется с помощью графов конфликтов. Согласно результатам тестирования [4], данный подход увеличивает количество шлюзов MPR в сети по сравнению со стандартной реализацией протокола, но при этом увеличивается пропускная способность всей сети.

DF-OLSR

Особенность указанной модификации протокола OLSR [5] заключается в обнаружении вредоносных узлов и их последующей изоляции от выбора в качестве шлюзов MPR. В предложенной версии протокола, узлы обмениваются как стандартными HELLO и TC сообщениями, так и сообщениями новых типов. Авторы работы предложили использовать два новых типа сообщений: VOTEFOR и VOTERPL. Сообщения VOTEFOR отправляются всем соседям на расстоянии одного шага, которые в свою очередь, пересылают эти сообщения далее своим одношаговым соседям. После получения сообщений VOTEFOR, двухшаговые соседи отправляют в ответ сообщения VOTERPL. Данные сообщения предотвращают возможность вредоносных узлов предоставлять ложную информацию о стандартных узлах, т.к. каждый узел записывает информацию, полученную с помощью количества повторов для дальнейшего сравнения, тем самым избегая выбора вредоносного узла в качестве шлюза.

TUE-OLSR

В рамках данной версии OLSR [6] предложен механизм безопасности, основанный на системе доверия между узлами. Представленный алгоритм анализирует поведение устройств и присваивает им рейтинг доверия. Рейтинг напрямую влияет на выбор узла в качестве шлюза MPR. Наиболее надежные узлы становятся шлюзами MPR. Моделирование показало, что данная модификация OLSR позволяет снизить среднюю задержку и повышает коэффициент доставки пакетов по сравнению с классическим протоколом OLSR.

PB-OLSR

Заявленная цель указанного протокола [7] заключается в повышении общей эффективности и живучести сети за счет выбора шлюзов MPR по критериям производительности и динамического уровня доверия.

Для достижения данной цели реализован следующий механизм оценки узлов. Во-первых, оценка производительности узла осуществляется с помощью метода многокритериального анализа принятия решений. Весами являются такие параметры как размер доступной оперативной памяти, уровень загрузки процессора и т.д., тем самым определяется производительность узла. Во-вторых, осуществляется проверка обработки сообщений HELLO и TC узлами сети, при этом используется метод оценки ROC на основе взвешивания критериев.

По результатам моделирования в сетевом симуляторе NS-3, применение указанного подхода позволяет уменьшить влияние вредоносных узлов, поскольку они выбираются в качестве MPR значительно реже. Кроме того, увеличивается длительность жизни маршрутов, поскольку в качестве шлюзов MPR выбираются узлы с высокой производительностью.

EM-OLSR

В данной версии протокола OLSR [8] предложена дополнительная оптимизация для классического алгоритма выбора шлюзов MPR на базе расчёта дополнительного динамического параметра узлов сети, именуемого willingness (готовность к ретрансляции, за счет оценки остаточной энергии узла и его скорости перемещения). Для оценки скорости используется GPS.

Авторы предложили три возможных значения данной характеристики:

1. willingness_high – для узлов с большим запасом энергии и малой скоростью перемещения (данные узлы считаются предпочтительными для выбора в качестве шлюзов MPR);

2. willingness_low – для узлов с высокой мобильностью и низким запасом энергии;

3. willingness_default – для типовых узлов, без выраженных отклонений.

Применение указанного критерия позволило увеличить пропускную способность соединений, уменьшить количество потерь, уменьшить энергопотребление.

W-OLSR

Авторы проекта W-OLSR (Weighted OLSR) [9] в рамках стандартного алгоритма выбора шлюзов MPR предложили использовать но-

вый критерий оценки – Weighted-MPR. Значение указанной метрики зависит от трех характеристик узла – уровень остаточной энергии, уровень сигнала, уровень задержки. Задаваемые коэффициенты определяют вклад каждой характеристики в значение Weighted-MPR. Если рассчитанное значение не превышает заданный порог, то узел может быть выбран в качестве MPR. В ходе моделирования было продемонстрировано увеличение пропускной способности соединений и снижение потерь пакетов.

EOLSR, EOLSR-EC, EOLSR-RE

Цель разработки и применения указанных протоколов [10] заключается в продлении времени функционирования беспроводной сети в условиях разряда аккумуляторов устройств. Для реализации протоколов осуществляется модификация служебных сообщений TC и HELLO. В данные сообщения, в зависимости от реализации добавляются следующие метрики – остаточная энергия (RE) и потраченная энергия (EC).

В случае с EOLSR-RE решение о назначении узла в качестве MPR принимается на основе уровня остаточной энергии. Если значение ниже заданного порога, то узел не будет выбран в качестве MPR. В модификации EOLSR-EC в качестве MPR выбирается узел с наименьшим потреблением энергии. Результаты моделирования показывают, что подход, использованный для протокола EOLSR-RE, является оптимальным, и наблюдается увеличение энергоэффективности сети.

M-OLSR

Протокол M-OLSR [11] предоставляет возможность каждому узлу самостоятельно решить, в какой момент ему обновлять служебные сообщения HELLO и TC. Данный способ позволяет минимизировать стоимость маршрута по критерию количества переходов и энергозатрат. В рамках предложенного протокола осуществляется контроль остаточной энергии узла, и когда он опускается ниже определенного порога, выбирается другой маршрут. Таким образом, для анализа и выбора маршрутов, учитываются сквозная задержка и остаточная энергия узлов.

Результаты моделирования показывают, что при использовании протокола наблюдается уменьшение объема служебного трафика и снижение энергопотребления, что также сопровождается снижением средней пропускной способности относительно классического протокола OLSR.

OLSR-ETX-ML-MD

В исследовании [12] представлен сравнительный анализ трех протоколов, в каждом из которых используется своя метрика:

1. OLSR-ETX предусматривает оценку качества каналов связи на основе успешного обмена сообщениями HELLO. В качестве шлюзов MPR выбираются узлы с наибольшим количеством надежных соседей.

2. OLSR-ML – качество каналов связи оценивается по критерию потерь пакетов.

3. OLSR-MD – в качестве основной характеристики для оценки каналов связи используется задержка.

Моделирование показало, применение протокола OLSR-ETX, из предложенных вариантов, позволяет оптимизировать среднюю задержку и пропускную способность соединений.

MOB-2-OLSR

Целью модификации MOB-2-OLSR [13] является продление времени функционирования сети. При этом ключевым параметром для оценки является мобильность узлов. Предпочтение в выборе в качестве шлюза MPR отдается узлам с наименьшей мобильностью (скоростью перемещения), благодаря чему, увеличивается время жизни сети.

Результаты моделирования показывают, что применение данного протокола вместо OLSR позволяет повысить коэффициент доставки пакетов (PDR), а также увеличить пропускную способность соединений и снизить среднюю задержку.

EDCR-OLSR

В данной работе [14] предложен новый подход к выбору шлюзов MPR. Авторы предложили использовать распределение нагрузки по аналогии с многоядерными процессорами, где нагрузка разделяется на несколько ядер. В данном случае предлагается выбирать некоторое число шлюзов MPR, которые должны функционировать совместно. То есть, в качестве шлюзов MPR выбирается несколько узлов, которые способны разделить нагрузку между собой, что должно значительно повысить отказоустойчивость всей сети.

Результаты моделирования показали, что данный подход уменьшает общее энергопотребление сети, а также увеличивает коэффициент доставки пакетов.

OLSR-AAD

В рамках протокола OLSR-AAD [15] предложено использовать новую метрику при выборе шлюзов MPR – «средний возраст смер-

Таблица 1

Сравнительный анализ модификаций протокола OLSR

Протокол	Основная метрика при выборе MPR	Особенности выбора шлюзов MPR	Новые типы сообщений	Противо-действие вредонос-ным узлам	Ключевая цель модификации
BW-OLSR	Пропускная способность	Граф конфликтов	Нет	Нет	Максимизация пропускной способности соединений
DF-OLSR	Уровень репута-ции	Изоляция ненадёжных узлов, учет задержки	Да (VOTEFOR, VOTERPL)	Да	Повышение безопасности
TUE-OLSR	Комбинированная репутационная метрика	Стандартный по метрике, с предварительной изоляцией ненадёжных узлов	Нет	Да	Повышение доступности узлов
PB-OLSR	Производитель-ность (RAM, CPU)	Многокрите-ри-альная оптимиза-ция	Нет	Да	Повышение эффективности маршрутизации
EM-OLSR	Потребление энергии	Стандартный, с расчётом willingness	Нет	Нет	Повышение энергоэффек-тив-ности
W-OLSR	Комбинированная метрика (энергия, сигнал, задержка)	Стандартный по метрике	Нет	Нет	Повышение доступности и эффективности
EOLSR-RE/ EC	Потребление энергии	Пороговые значения	Нет, но изменен формат сообще-ний	Нет	Увеличение времени жизни сети
M-OLSR	Потребление энергии	Адаптивная стратегия	Нет	Нет	Снижение нагрузки и энергопотребле-ния
OLSR-ETX/ ML/MD	Качество связи (ETX) / Задержка (MD)	Стандартный по метрике	Нет	Нет	Повышение качества обслуживания (QoS)
MOB-2-OLSR	Мобильность соседей	Приоритет менее мобильным	Нет	Нет	Снижение потерь пакетов в условиях мобильности
EDCR-OLSR	Комбинированная метрика (энергети-ческий статус, задержка, стабильность)	Многокритериаль-ная оптимизация, распределение нагрузки	Нет	Нет	Повышение энергоэффектив-ности
OLSR-AAD	Прогнозируемое время жизни узла (AAD)	Стандартный по метрике	Нет	Нет	Повышение доступности узлов
DCFM-OLSR	Стандартная	Активное продиводействие атакам	Нет	Да	Повышение безопасности
OPE-OLSR	Энергетический вес (остаточный заряд, стоимость передачи)	Фильтрация неэффективных узлов	Нет	Нет	Увеличение времени жизни сети

ти» (Average Age of Death, AAD). Данная метрика представляет прогнозное время, в течение которого узел сможет выполнять свою роль в качестве шлюза MPR.

Особенность указанного подхода заключается в том, что он позволяет оценить не мгновенное состояние узла, а прогнозируемое. Соответственно, в качестве шлюза MPR выбирается узел, позволяющий обеспечить наибольшее время жизни сетевых соединений.

Результаты моделирования показывают, что применение данного протокола вместо OLSR приводит к увеличению коэффициента доставки пакетов и уменьшению средней задержки.

DCFM-OLSR

Для проекта [16] авторы предложили активный механизм защиты от сетевых атак. Механизм DCFM основан на создании виртуальных узлов, которые имитируют поведение легитимных узлов. Указанные узлы используются для перенаправления или блокировки действий вредоносного узла, что позволяет обеспечить защиту реальных устройств.

Моделирование продемонстрировало, что данный подход позволяет эффективно противодействовать широкому спектру известных атак, что увеличивает безопасность сети.

OPE-OLSR

Разработанный протокол OPE-OLSR [17] направлен на увеличение срока функционирования сети, за счет выбора в качестве шлюзов MPR энергоэффективных узлов. В рамках данного подхода производится оценка остаточной энергии узла у одношаговых соседей. В случае, если несколько одношаговых соседей имеют одинаковый уровень остаточной энергии, то в качестве шлюза MPR выбирается узел с наибольшим количеством двухшаговых соседей. Результаты имитационного моделирования подтверждают достижение целей, заявленных авторами проекта.

Заключение

Сравнительный анализ различных модификаций протокола OLSR (таблица 1) позволил сформулировать следующие выводы:

1. Модификация стандартного эвристического алгоритма для задачи выбора шлюзов MPR, связанной с задачей о покрытии множества, в большинстве случаев действительно позволяет обеспечить более эффективный выбор шлюзов MPR и повысить показатели характеристик сетевого взаимодействия.

2. В настоящее время основные усилия исследователей сосредоточены на оптимизации энергопотребления и увеличении времени жизни сети за счет повышения энергоэффективности. В значительном количестве работ предложены новые метрики для процесса выбора шлюзов MPR, учитывающие остаточный уровень заряда, качество каналов связи и мобильность узлов. При этом, следует отметить, что, как правило, указанные характеристики являются взаимозависимыми, но оценка их взаимного влияния друг на друга не учитывается и не приводится.

3. Проблема безопасного выбора шлюзов MPR в рамках протокола маршрутизации OLSR в условиях наличия вредоносных узлов остаётся актуальной. Определяя и учитывая уровень репутации узлов в процессе выбора шлюзов MPR, можно снизить вероятность выбора вредоносных узлов в качестве шлюзов MPR и, тем самым, повысить безопасность сетевого взаимодействия. При этом, ключевые задачи заключаются в поиске подходящей репутационной модели и разработке эффективного алгоритма выбора шлюзов MPR с учетом репутации узлов (каналов связи).

Литература

1. RFC3626: Optimized Link State Routing Protocol (OLSR)/ T. Clausen, P. Jacquet, 2003. URL: https://tools.ietf.org/html/rfc3626 (дата обращения: 15.02.2026).

2. Еремеев А.В., Заозерская Л.А., Колоколов А.А. Задача о покрытии множества: сложность, алгоритмы, экспериментальные исследования / А.В. Еремеев, Л.А. Заозерская, А.А. Колоколов // Дискретный анализ и исследование операций, сер. 2, 2000. Т. 7, № 2. С. 22–46.

3. Сергин Д.А., Васильев А.А. Моделирование атаки на множество шлюзов пересылки в рамках протокола маршрутизации OLSR // ПЕРСПЕКТИВА-2024: Сборник трудов одиннадцатой всероссийской молодежной школы-семинара по проблемам информационной безопасности. Таганрог, ЮФУ, 2024. С. 140–146.

4. Moad D., Djahel S., Nait-Abdesselam F. Improving the quality of service routing in OLSR protocol // 2012 International Conference on Communications and Information Technology (ICCIT). – IEEE, 2012. – С. 314–319.

5. Malik D., Mahajan K., Rizvi M. A. Security for node isolation attack on OLSR by modifying MPR selection process // 2014 First International Conference on Networks & Soft Computing (ICNSC2014). – IEEE, 2014. – С. 102–106.

6. Wang X. et al. Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network // IEEE Access. – 2020. – Т. 8. – С. 47675–47693.

7. Dyabi M., Hajami A., Allali H. PB-OLSR: Performance Based OLSR // IJCSNS International Journal of Computer Science and Network Security. – 2015. – Т. 15.

8. Fatima L., Najib E. Energy and mobility in OLSR routing protocol // Journal of Selected Areas in Telecommunications (JSAT). – 2012. – Т. 2012. – № 3. – С. 1–6.

9. Anandrao L. S., Amey J. Y. Comparison of OLSR and Energy Conserved OLSR // International Journal of Technical Research and Applications. – 2014. – Т. 2. – № 4.

10. Mohit M., Pal S. Stable MPR selection in OLSR for mobile ad-hoc networks // Int. J. Comp. Sci. Inf. Technol. – 2015. – Т. 6. – № 6. – С. 5121–5125.

11. Jaiswal A. K., Tiwari S. Modified OLSR (MOLSR) Protocol for improving optimal route selection with Dynamic MPR selection in Mobile Adhoc Network // International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). – 2015. – Т. 1. – № 6. – С. 535–541.

12. Pandey A., Baliyan M. Performance Analysis of OLSR and Modified Version of OLSR-ETX/MD/ML in Mesh Networks // International Journal of Computer Science & Communication Networks. – 2012. – Т. 2. – № 2. – С. 268–271.

13. Ouacha A. et al. OLSR protocol enhancement through mobility integration // 2013 10th IEEE International Conference on Networking, Sensing And Control (ICNSC). – IEEE, 2013. – С. 17–22.

14. Ouacha A. et al. Proactive routing based distributed energy consumption // 2013 8th International Conference on Intelligent Systems: Theories and Applications (SITA). – IEEE, 2013. – С. 1–5.

15. Ouacha A. et al. New Mobility Metric based on MultiPoint Relay Life Duration // SIGMAP. – 2012. – С. 305–309.

16. Rani V. I. U., Reddy K. T. To Improve the Security of OLSR Routing Protocol Based on Local Detection of Link Spoofing // International Journal of Science Engineering Technology, IJSEAT. – 2017. – Т. 5.

17. Prajapati S., Patel N., Patel R. Optimizing performance of OLSR protocol using energy based MPR selection in MANET // 2015 Fifth International Conference on Communication Systems and Network Technologies. – IEEE, 2015. – С. 268–272.

References

1. RFC3626: Optimized Link State Routing Protocol (OLSR)/ T. Clausen, P. Jacquet, 2003. URL: https://tools.ietf.org/html/rfc3626

2. Eremeev A.V., Zaozerskaya L.A., Kolokolov A.A. Zadacha o pokrytii mnozhestva: slozhnost', algoritmy, eksperimental'nye issledovaniya / A.V. Eremeev, L.A. Zaozerskaya, A.A. Kolokolov // Diskretnyy analiz i issledovanie operatsiy, ser. 2, 2000. T. 7, № 2. S. 22–46.

3. Sergin D.A., Vasil'ev A.A. Modelirovanie ataki na mnozhestvo shlyuzov peresylki v ramkakh protokola marshrutizatsii OLSR // PERSPEKTIVA-2024: Sbornik trudov odinnadtsatoy vserossiyskoy molodezhnoy shkoly-seminara po problemam informatsionnoy bezopasnosti. Taganrog, YuFU, 2024. S. 140–146.

4. Moad D., Djahel S., Nait-Abdesselam F. Improving the quality of service routing in OLSR protocol // 2012 International Conference on Communications and Information Technology (ICCIT). – IEEE, 2012. – S. 314–319.

5. Malik D., Mahajan K., Rizvi M. A. Security for node isolation attack on OLSR by modifying MPR selection process // 2014 First International Conference on Networks & Soft Computing (ICNSC2014). – IEEE, 2014. – S. 102–106.

6. Wang X. et al. Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network // IEEE Access. – 2020. – T. 8. – S. 47675–47693.

7. Dyabi M., Hajami A., Allali H. PB-OLSR: Performance Based OLSR // IJCSNS International Journal of Computer Science and Network Security. – 2015. – T. 15.

8. Fatima L., Najib E. Energy and mobility in OLSR routing protocol // Journal of Selected Areas in Telecommunications (JSAT). – 2012. – T. 2012. – №. 3. – S. 1–6.

9. Anandrao L. S., Amey J. Y. Comparison of OLSR and Energy Conserved OLSR // International Journal of Technical Research and Applications. – 2014. – T. 2. – № 4.

10. Mohit M., Pal S. Stable MPR selection in OLSR for mobile ad-hoc networks // Int. J. Comp. Sci. Inf. Technol. – 2015. – T. 6. – №. 6. – S. 5121–5125.

11. Jaiswal A. K., Tiwari S. Modified OLSR (MOLSR) Protocol for improving optimal route selection with Dynamic MPR selection in Mobile Adhoc Network // International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). – 2015. – T. 1. – № 6. – S. 535–541.

12. Pandey A., Baliyan M. Performance Analysis of OLSR and Modified Version of OLSR-ETX/MD/ML in Mesh Networks //International Journal of Computer Science & Communication Networks. – 2012. – T. 2. – № 2. – S. 268–271.

13. Ouacha A. et al. OLSR protocol enhancement through mobility integration // 2013 10th IEEE International Conference on Networking, Sensing And Control (ICNSC). – IEEE, 2013. – S. 17–22.

14. Ouacha A. et al. Proactive routing based distributed energy consumption // 2013 8th International Conference on Intelligent Systems: Theories and Applications (SITA). – IEEE, 2013. – S. 1–5.

15. Ouacha A. et al. New Mobility Metric based on MultiPoint Relay Life Duration // SIGMAP. – 2012. – S. 305–309.

16. Rani V. I. U., Reddy K. T. To Improve the Security of OLSR Routing Protocol Based on Local Detection of Link Spoofing // International Journal of Science Engineering Technology, IJSEAT. – 2017. – T. 5.

17. Prajapati S., Patel N., Patel R. Optimizing performance of OLSR protocol using energy based MPR selection in MANET // 2015 Fifth International Conference on Communication Systems and Network Technologies. – IEEE, 2015. – S. 268–272.

СЕРГИН Даниил Альбертович, аспирант федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: daniil0808_98@mail.ru

ЩЕРБА Евгений Викторович, кандидат технических наук, доцент, доцент кафедры «Комплексная защита информации» федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: evscherba@gmail.com

SERGIN Daniil Albertovich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "Omsk State Technical University". 644050, Omsk, pr. Mira, 11. E-mail: daniil0808_98@mail.ru

SHCHERBA Evgeny Victorovich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Complex Information Protection, at the Federal State Autonomous Educational Institution of Higher Education "Omsk State Technical University". 644050, Omsk, pr. Mira, 11. E-mail: evscherba@gmail.com

УДК 004.056.55:343.149 Вестник УрФО № 1(59) / 2026, с. 68–77

Титов Е. С., Зырянова Т. Ю

DOI: 10.14529/secur260107

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ДЛЯ ВЕРИФИКАЦИИ КОНФИДЕНЦИАЛЬНЫХ ДОКАЗАТЕЛЬСТВ В СУДОПРОИЗВОДСТВЕ

Рассматривается актуальная проблема совмещения принципов прозрачности и конфиденциальности в современном судопроизводстве. Подчеркивается ключевая роль протоколов с нулевым разглашением (Zero-Knowledge Proofs, ZKP) как инструмента, позволяющего проводить верификацию фактов без раскрытия конфиденциальных данных. Анализируются технические и правовые аспекты применения ZKP в российских судах, выявляется необходимость гармонизации нормативных актов и технического оснащения судебной системы. Рассматриваются перспективы интеграции криптографических протоколов в судопроизводство, приводятся примеры успешных зарубежных практик и разрабатываются рекомендации по совершенствованию отечественного законодательства. Приводится концепт модели применения ZKP, детально описано устройство предлагаемой системы, этапы верификации и инфраструктура, необходимая для успешного внедрения. Проводится сравнительный анализ традиционной и новой парадигмы судопроизводства, оцениваются преимущества и недостатки обоих подходов. Делается вывод о том, что внедрение ZKP способно радикально повысить качество и безопасность судебных процессов, укрепить принципы верховенства права и минимизировать коррупционные риски, вызванные распространением конфиденциальной информации. Формулируются рекомендации по дальнейшему развитию и внедрению ZKP в российскую судебную систему.

Ключевые слова: *доказательство с нулевым разглашением, адвокатская тайна, верификация доказательств, блокчейн, конфиденциальность доказательств, судопроизводство, цифровые доказательства, электронное правосудие, безопасность юридического документооборота.*

APPLICATION OF CRYPTOGRAPHIC WITH ZERO KNOWLEDGE PROTOCOLS FOR VERIFICATION OF CONFIDENTIAL EVIDENCE IN COURT PROCEEDINGS

The article discusses the current problem of combining the principles of transparency and confidentiality in modern legal proceedings. It emphasizes the key role of zero-knowledge protocols (Zero-Knowledge Proofs, ZKP) as a tool that allows for verification of facts without disclosing confidential data. The article analyzes the technical and legal aspects of using ZKP in Russian courts, highlighting the need for harmonization of regulations and the technical equipment of the judicial system. The article also explores the prospects for integrating cryptographic protocols into legal proceedings, provides examples of successful foreign practices, and develops recommendations for improving domestic legislation. The article presents a concept of the ZKP application model, describes in detail the structure of the proposed system, the stages of verification, and the infrastructure required for successful implementation. The article provides a comparative analysis of the traditional and new paradigms of legal proceedings, and evaluates the advantages and disadvantages of both.

Keywords: *zero-knowledge proof, attorney-client privilege, evidence verification, blockchain, evidence confidentiality, legal proceedings, digital evidence, e-justice, and legal document security.*

Введение

Современные судебные системы сталкиваются с нарастающим конфликтом между необходимостью обеспечения прозрачности доказательств и соблюдением конфиденциальности личных и коммерческих данных участников процесса. Протоколы с нулевым разглашением (Zero-Knowledge Proofs, ZKP) представляют собой криптографический инструмент, способный принципиально изменить подход к данной проблеме. Они позволяют верифицировать факты, такие как подлинность подписи или соответствие данных определенным критериям без раскрытия самой информации. Таким образом, ZKP открывают новые возможности для баланса между требованиями правосудия и обеспечением конфиденциальности в судопроизводстве.

Традиционные судебные процедуры требуют полного раскрытия доказательств для их проверки, что неизбежно приводит к рискам утечки конфиденциальной информации. Особенно остро эта проблема проявляется в делах, связанных с коммерческой тайной, медицинскими данными или адвокатской тайной. Государственная тайна в рамках данной статьи не рассматривается. Участники процесса вынуждены идти на компромисс между необходимостью доказать свою позицию и сохранением конфиденциальности чувствительных сведений. Следствием такого противоречия становится снижение доверия к судебной системе, затягивание процессов и потенциальные злоупотребления их участников. Даже при наличии правовых механизмов обеспечения конфиденциальности практическая реализация часто оказывается неэффективной. Это создает потребность в инноваци-

онных решениях, способных обеспечить верификацию доказательств без их раскрытия, сохраняя при этом юридическую силу и процессуальную корректность.

Актуальность внедрения ZKP в судопроизводство усиливается на фоне экспоненциального роста использования блокчейн-технологий и цифровых активов. Одновременно ужесточаются российские и международные регуляторные требования к защите данных, такие как Федеральный закон №152-ФЗ «О персональных данных» в России или Общий регламент по защите данных (General Data Protection Regulation, GDPR) в Европе. Эти факторы создают благоприятную почву для междисциплинарных исследований на стыке криптографии и юриспруденции. Недавние научные публикации (2022-2025 гг.) демонстрируют растущий интерес к применению криптографических инноваций в правоприменении. Однако комплексное исследование интеграции ZKP именно в судебные процедуры с учетом специфики процессуального законодательства остается актуальной научной и практической задачей. Настоящая работа призвана восполнить этот пробел, предложив модель, сочетающую технологические возможности с юридической практикой.

Целью данной работы является разработка концептуальной модели применения протоколов с нулевым разглашением (преимущественно zk-SNARKs и zk-STARKs) для верификации конфиденциальных доказательств в гражданском и уголовном судопроизводстве. Модель должна обеспечивать сохранение юридической силы доказательств и соответствие действующему процессуальному законодательству при одновременной защите конфиденциальных, или просто избыточных данных от несанкционированного раскрытия.

Для достижения поставленной цели определен ряд задач. Первая задача включает криптографический анализ ZKP-протоколов, оценку их применимости к судебным доказательствам с учетом математических основ и практических реализаций. Вторая задача посвящена изучению правовых аспектов конфиденциальности доказательств, выявлению пробелов в законодательстве и определению точек интеграции ZKP. Третья задача заключается в проектировании архитектуры системы верификации на основе ZKP, моделируя ее работу на примере типичного гражданского дела. Четвертая задача предусматривает оценку преимуществ и ограничений предложенной модели, включая вычислительную сложность, юридические риски и этические последствия, с последующей разработкой рекомендаций для пилотного внедрения.

Криптографические примитивы и их роль в защите данных

Криптографические примитивы служат фундаментальными компонентами систем защиты информации. Они обеспечивают базовые функции конфиденциальности, целостности и аутентификации данных. Эти элементы позволяют создавать защищенные системы обработки и передачи сведений. Их корректное применение гарантирует безопасность информации на всех этапах работы. В исследовании освещаются ключевые механизмы блокчейна, такие как хеширование, цифровые подписи и консенсусные протоколы, и объясняется, как они в совокупности способствуют обеспечению целостности данных и безопасному контролю доступа [3]. Данные примитивы формируют основу для построения доверенных сред обмена информацией. Их комбинированное использование позволяет решать комплексные задачи защиты.

Асимметричное шифрование использует пару ключей – открытый и закрытый – для обеспечения конфиденциальности передаваемых данных. Электронные подписи на основе асимметричной криптографии позволяют подтверждать подлинность и авторство документов. Эти технологии создают основу для формирования доверенных каналов передачи судебных доказательств. Они обеспечивают защиту информации от несанкционированного доступа при её перемещении.

Хеш-функции преобразуют произвольные данные в уникальные фиксированной длины значения. Протоколы обязательств позволяют зафиксировать информацию без её немедленного раскрытия. В совокупности эти примитивы гарантируют неизменяемость и верифицируемость цифровых доказательств. Они обеспечивают возможность последующей проверки целостности представленных материалов.

Принципы функционирования протоколов с нулевым разглашением

Протоколы с нулевым разглашением представляют криптографический метод, позволяющий одной стороне доказать истинность утверждения другой стороне без раскрытия какой-либо информации, кроме

самого факта истинности. Данная концепция основана на идее, что верификатор может убедиться в корректности утверждения, не получая доступа к конфиденциальным данным. Такой подход обеспечивает сохранение секретности исходной информации при подтверждении её достоверности. Применение этой технологии особенно актуально в ситуациях, требующих доказательства владения данными без их демонстрации. Основная задача протоколов с нулевым разглашением заключается в предоставлении строгого криптографического доказательства, исключающего необходимость передачи самих сведений. Это достигается за счёт специальных математических конструкций, которые преобразуют исходные данные в доказательство, не раскрывающее их содержание. Подобные механизмы позволяют, например, подтвердить знание пароля или наличие определённого атрибута, не разглашая сам пароль или атрибут. Таким образом, концепция нулевого разглашения создаёт фундамент для безопасной верификации в контексте конфиденциальных доказательств.

К протоколам с нулевым разглашением предъявляются три фундаментальных требования: полнота, корректность и нулевое разглашение. Полнота гарантирует, что честный доказывающий сможет убедить проверяющего в истинности корректного утверждения. Корректность обеспечивает невозможность обмана со стороны доказывающего при ложном утверждении. Нулевое разглашение означает, что верификатор не получает никакой дополнительной информации, кроме факта истинности утверждения. «Совершенность означает, что если бесконечное число нелегитимных абонентов не имеет возможности извлечь информацию о секрете, то такая схема – совершенная. Идеальность означает, что если размер доли секрета равен размеру секрета, то такая схема идеальна» [5].

Протоколы с нулевым разглашением могут быть реализованы как в интерактивных, так и в неинтерактивных схемах. Интерактивные схемы предполагают обмен несколькими сообщениями между доказывающей и проверяющей сторонами для достижения консенсуса относительно истинности утверждения. Неинтерактивные схемы позволяют сгенерировать одноразовое доказательство, которое может быть проверено без дальнейшего взаимодействия сторон.

Обзор основных типов ZKP: zk-SNARKs, zk-STARKs и их применимость

zk-SNARKs представляют собой компактные неинтерактивные доказательства с нулевым разглашением. Для их функционирования требуется этап доверенной настройки, в ходе которого генерируются общие параметры. Данный этап создает риски утечки критической информации, так как требует надёжного уничтожения использованных данных после настройки. Несмотря на этот недостаток, zk-SNARKs обеспечивают высокую эффективность проверки и минимальный размер доказательств.

zk-STARKs предлагают альтернативу без необходимости доверенной настройки, обеспечивая прозрачность процесса. Они обладают квантовой устойчивостью благодаря использованию хеш-функций вместо криптографии с открытым ключом. Это делает их перспективными для долгосрочной безопасности в условиях развития квантовых вычислений. Кроме того, zk-STARKs демонстрируют высокую масштабируемость при увеличении сложности вычислений. Важным аспектом zk-STARKs является оптимизация производительности. Третий приём — оптимизация модели с помощью порождающей функции. Данная оптимизация связана с особенностью работы инструмента проверки модели TLC и позволяет повысить его производительность (снизить время верификации). После оптимизации спецификация TLA+ остаётся информативной и удобочитаемой, так как ограничения, накладываемые протоколом на сообщения, сконцентрированы в определении порождающей функции [4]. Это подчеркивает значимость эффективных методов верификации в контексте судебных систем.

Выбор между zk-SNARKs и zk-STARKs для судебных систем определяется балансом требований к производительности, безопасности и юридической допустимости. Zk-SNARKs предпочтительны при ограниченных вычислительных ресурсах и необходимости минимального размера доказательств. zk-STARKs более применимы в сценариях, требующих долгосрочной безопасности и отсутствия доверенных третьих сторон. Юридические аспекты включают соответствие стандартам доказывания и допустимость электронных доказательств в судопроизводстве. Для обеспечения большего доверия, можно комбинировать эти подходы с системами электронной подписи, и загрузкой в блокчейны, например, используя OpenTimeStamps.

Конфиденциальность доказательств в российском судопроизводстве: текущее состояние

Российское законодательство устанавливает комплекс норм, регулирующих защиту конфиденциальных доказательств в уголовном и гражданском процессах. Уголовно-процессуальный кодекс Российской Федерации содержит положения о неразглашении данных предварительного расследования, а также о защите сведений о частной жизни участников процесса. Гражданский процессуальный кодекс Российской Федерации предусматривает возможность проведения закрытых судебных заседаний и ограничения доступа к материалам дела для защиты охраняемой законом тайны. Статья 8 Федерального закона №63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» закрепляет понятие адвокатской тайны и устанавливает жесткие гарантии её сохранения.

Эти нормативные правовые акты формируют правовую основу для обеспечения конфиденциальности в судопроизводстве.

Судебная практика демонстрирует ограниченное применение механизмов защиты конфиденциальных доказательств. Ходатайства о проведении закрытых заседаний удовлетворяются преимущественно по уголовным делам, связанным с государственной тайной или преступлениями против половой неприкосновенности. В гражданском процессе такие меры применяются реже, преимущественно при рассмотрении споров, связанных с коммерческой тайной или семейными отношениями. Анализ конкретных кейсов выявляет непоследовательность судов в оценке необходимости защиты конфиденциальной информации. Существует опасность формирования целого нового направления – инициации процессов с единственной целью получения доступа к конфиденциальной информации или легитимизации данных.

Доказательства, требующие конфиденциальной защиты в судопроизводстве, подразделяются на несколько категорий. К ним относятся сведения, составляющие государственную тайну, доступ к которой ограничен федеральным законом. Отдельную группу образуют доказательства, содержащие коммерческую тайну, охраняемую в соответствии с Гражданским кодексом Российской Федерации. Отдельную категорию составляют персональные данные участников процесса, защита которых обеспечивается Федеральным законом №152-ФЗ «О персональных данных», применимую, практически к любым процессам. Все эти данные могут в совокупности составлять различные виды профессиональных тайн, например, адвокатской, врачебной и другими, урегулированными специальными законами.

Традиционные механизмы обеспечения конфиденциальности имеют существенные ограничения на разных стадиях процесса. В досудебном производстве защита доказательств осуществляется преимущественно через институт следственной тайны, что не всегда предотвращает утечки информации. В судебном разбирательстве основными инструментами остаются закрытые заседания и ограниченный доступ к материалам дела, однако эти меры не гарантируют полной защиты при передаче и исследовании доказательств. Системной проблемой является отсутствие технических средств, позволяющих верифицировать доказательства без их полного раскрытия.

Проблемы баланса между раскрытием и защитой данных в судебных процессах

В судопроизводстве возникает фундаментальная коллизия между правом стороны защиты на ознакомление с доказательствами и необходимостью сохранения конфиденциальности определенной информации. Данная проблема особенно остро проявляется при работе с чувствительными данными, такими как медицинские записи (врачебная тайна), данные о личной жизни граждан, или коммерческая тайна. Существует противоречие между принципом состязательности сторон и требованиями законодательства о защите конфиденциальных данных. Разрешение этой коллизии требует поиска компромиссных решений, обеспечивающих как справедливость судебного разбирательства, так и защиту конфиденциальных сведений.

Традиционные процедуры раскрытия доказательств несут значительные риски несанкционированного распространения конфиденциальной информации. Передача документов сторонам процесса и суду создает множество точек уязвимости для утечек данных. Особую опасность представляет возможность злоупотребления полученной информацией участниками судебного разбирательства в личных или корыстных целях. Эти риски подрывают доверие к судебной системе и могут препятствовать предоставлению

важных доказательств из-за опасений за сохранность данных.

Существенная проблема заключается в верификации доказательств без их полного раскрытия сторонам процесса. Традиционные методы требуют предоставления полного содержания документов для установления их достоверности и допустимости. Однако это противоречит потребности в защите конфиденциальных сведений, составляющих суть доказательства. Необходимы инновационные подходы, позволяющие подтверждать подлинность и релевантность доказательств, не раскрывая при этом их содержательную часть.

Доступ судей и участников процесса к конфиденциальным данным создает серьезные этические дилеммы. С одной стороны, судьи должны иметь достаточно информации для принятия обоснованного решения. С другой стороны, даже ограниченный доступ к чувствительной информации может нарушать права граждан на неприкосновенность частной жизни. Возникает вопрос о том, как обеспечить необходимый уровень информированности суда, минимизируя при этом этические риски, связанные с обработкой конфиденциальных данных в ходе судебного разбирательства.

Архитектура системы верификации на основе ZKP для судебных доказательств

Предлагаемая архитектура системы верификации судебных доказательств на основе ZKP имеет многоуровневую структуру, состоящую из трех основных модулей. Модуль генерации доказательств отвечает за создание криптографических утверждений о конфиденциальных данных без их раскрытия. Модуль верификации позволяет проверять корректность этих утверждений с использованием протоколов с нулевым разглашением. Модуль арбитража обеспечивает разрешение спорных ситуаций и финальное подтверждение результатов верификации. Такое разделение функций гарантирует четкое распределение ролей между участниками судебного процесса. Сторона, представляющая доказательства, взаимодействует исключительно с модулем генерации, что минимизирует риск несанкционированного доступа к данным. Судья или уполномоченные эксперты получают доступ к модулю верификации для подтверждения обоснованности утверждений. Модуль арбитража активируется только при возникновении конфликтных ситуаций, обеспечивая дополнительный уровень доверия к системе.

Криптографическая защита данных в системе реализуется через комбинированное применение протоколов zk-SNARKs и алгоритмов цифровой подписи. Протоколы zk-SNARKs обеспечивают возможность верификации утверждений о конфиденциальных доказательствах без раскрытия их содержания. Цифровые подписи используются для аутентификации участников процесса и подтверждения целостности передаваемых данных на каждом этапе обработки. Гибридный подход гарантирует сохранение конфиденциальности исходных доказательств на протяжении всей цепочки обработки. Применение zk-SNARKs исключает необходимость раскрытия информации в ходе верификации. Одновременно цифровые подписи предотвращают несанкционированные модификации данных и обеспечивают неотказуемость действий участников. Это создает надежную основу для судебного процесса, где соблюдается баланс между проверяемостью и конфиденциальностью.

Этапы интеграции ZKP в судебный процесс: от представления до верификации

Процедура представления доказательств в системе верификации на основе ZKP начинается с их преобразования в верифицируемую форму. Конфиденциальные данные подвергаются криптографической обработке для создания математических представлений, сохраняющих исходную информацию в скрытом виде. Данный этап обеспечивает защиту содержательных аспектов доказательств при последующей обработке. Ключевым требованием является гарантия корректности преобразования без ущерба для конфиденциальности. Преобразование включает генерацию доказательства с нулевым разглашением, которое подтверждает истинность утверждения о доказательстве, не раскрывая его содержание. Для этого используются специализированные алгоритмы, такие как zk-SNARKs или zk-STARKs, адаптированные под требования судебного процесса. Полученное доказательство в зашифрованной форме подготавливается для передачи в судебную систему. Таким образом, обеспечивается начальный этап интеграции ZKP, сохраняющий секретность исходных материалов.

Этап судебной проверки предполагает интерактивное взаимодействие между сто-

ронами процесса через протоколы с нулевым разглашением. Участники обмениваются криптографическими доказательствами без раскрытия содержательной информации, что соответствует принципам конфиденциальности. «Когда требуется проверка (например, во время проверки соответствия требованиям, судебного спора или запроса на доступ), система не извлекает и не раскрывает персональные данные. Вместо этого она повторно обрабатывает представленные данные и сравнивает полученный хеш с хешем, хранящимся в блокчейне» [3]. Данный механизм позволяет проверить соответствие доказательств установленным критериям без доступа к их содержанию.

Финальная верификация осуществляется арбитром, который использует открытые параметры системы для подтверждения корректности доказательств. Судья или уполномоченный эксперт проверяет математическую достоверность представленных ZKP-доказательств, опираясь на публично доступные криптографические ключи. Процесс не требует раскрытия конфиденциальных данных, поскольку основан на проверке формальных свойств доказательства. Результатом является юридически значимое подтверждение обоснованности доказательства при сохранении его секретности.

Моделирование применения ZKP на примере гражданского дела

В рамках моделирования рассматривается гипотетическое гражданское дело о нарушении договорных обязательств между контрагентами. Истец утверждает, что ответчик не выполнил условия контракта, что привело к финансовым потерям. Для подтверждения факта нарушения требуется предъявить доказательства, содержащие коммерческую тайну. Использование протоколов с нулевым разглашением позволяет верифицировать истинность утверждения без раскрытия конфиденциальных данных. В данном сценарии применяется методика, аналогичная описанной в научной литературе: «Применение результатов демонстрируется на примере простого протокола — протокола Нидхема-Шредера для аутентификации с открытым ключом» [4]. Адаптированный подход обеспечивает доказательство нарушения обязательств, сохраняя в тайне конкретные условия договора и финансовые показатели. Это соответствует требованиям защиты коммерческой информации в судебном процессе.

Проведенный анализ вычислительной эффективности сравнивает традиционные методы верификации с использованием оптимизированных протоколов zk-STARKs. Результаты показывают значительное сокращение времени обработки доказательств. В смоделированном кейсе применение zk-STARKs позволило уменьшить продолжительность верификации на 40% по сравнению с классическими криптографическими методами. Ускорение процесса достигается за счет оптимизации алгоритмов доказательства и верификации, характерной для zk-STARKs. Данный протокол исключает необходимость сложных вычислений на стороне доказывающего, перераспределяя нагрузку. Эффективность решения подтверждает его практическую применимость в условиях ограниченных временных ресурсов судопроизводства.

Технические требования и инфраструктурные аспекты реализации модели

Минимальные системные требования для реализации модели верификации на основе протоколов с нулевым разглашением включают поддержку криптографических алгоритмов высокой стойкости. Особое внимание уделяется использованию эллиптических кривых, обеспечивающих уровень безопасности не менее 128 бит. Данный подход гарантирует защиту от современных криптоаналитических атак. Интеграция таких кривых требует специализированных математических библиотек. Дополнительным требованием является применение специализированных криптопроцессоров, оптимизированных для выполнения ресурсоемких операций ZKP. Эти аппаратные компоненты ускоряют вычисления, связанные с генерацией и верификацией доказательств, что критично для соблюдения процессуальных сроков. Использование аппаратного ускорения позволяет снизить общую вычислительную нагрузку на систему. Внедрение подобных процессоров должно соответствовать международным стандартам безопасности.

Развертывание инфраструктуры для предложенной модели предусматривает создание доверенной среды исполнения (TEE) на защищенных серверах. TEE обеспечивает изолированное выполнение криптографических операций, предотвращая несанкционированный доступ к конфиденциальным данным доказательств. Данная среда должна соответствовать требованиям стандартов

Trusted Computing Group. Реализация TEE включает аппаратные и программные механизмы защиты. Важным инфраструктурным аспектом является использование распределенных реестров для аудита операций верификации без раскрытия содержательной части доказательств. Блокчейн-технологии позволяют фиксировать факт выполнения проверки и обеспечивают неизменяемость журналов событий. Это создает прозрачную и проверяемую систему контроля. Применение распределенных реестров повышает доверие к результатам верификации со стороны всех участников процесса.

Преимущества и ограничения предложенной модели ZKP в судопроизводстве

Предложенная модель применения протоколов с нулевым разглашением (ZKP) обеспечивает криптографически подтверждённую конфиденциальность данных участников судебного процесса. Данный подход минимизирует риски несанкционированного доступа к конфиденциальным доказательствам. Одновременно сохраняется возможность независимой верификации представленных материалов. «Ключевые преимущества применения ZKP включают обеспечение криптографически подтверждённой конфиденциальности данных участников процесса, минимизацию рисков несанкционированного доступа к доказательствам и защиту уязвимых категорий лиц (свидетелей, потерпевших) без компромисса верифицируемости представленных материалов» [2]. Особую значимость модель приобретает при защите уязвимых категорий лиц, таких как свидетели и потерпевшие. Их персональные данные и показания могут быть верифицированы без раскрытия самой информации. Это позволяет соблюсти баланс между требованиями конфиденциальности и необходимостью процессуальной проверки доказательств. Таким образом, внедрение ZKP способствует повышению доверия к судебной системе при работе с конфиденциальными материалами.

Основные ограничения предложенной модели обусловлены высокими вычислительными затратами на генерацию доказательств для сложных судебных кейсов. Данный фактор может существенно замедлить судебные процессы, особенно при рассмотрении дел с большим объемом доказательств. «Основные ограничения модели связаны с высокими вычислительными затратами на генерацию доказательств для сложных кейсов, необходимостью адаптации судебной инфраструктуры и специализированной подготовки юридического персонала для работы с криптографическими протоколами» [1]. Дополнительным барьером внедрения выступает необходимость адаптации существующей судебной инфраструктуры и специализированной подготовки юридического персонала. Судебные работники должны обладать достаточными знаниями для корректной работы с криптографическими протоколами. Эти требования создают практические сложности при масштабировании модели на всю судебную систему.

Юридические и этические аспекты внедрения ZKP: риски и перспективы

Внедрение ZKP в судопроизводство сталкивается с юридическими вызовами, связанными с процессуальной легитимностью доказательств. Использование ZKP требует модификации существующих норм доказывания, поскольку традиционные стандарты допустимости основаны на полном раскрытии информации. Необходимо обеспечить соответствие криптографических доказательств требованиям проверяемости и достоверности, установленным процессуальным законодательством. Это предполагает разработку новых критериев оценки доказательств, учитывающих специфику ZKP. Ограниченный доступ к исходным данным при верификации доказательств посредством ZKP создает риски конфликта с принципами состязательности судебного процесса. Стороны могут быть лишены возможности полноценно оспаривать доказательства из-за отсутствия доступа к первичной информации. Такая ситуация требует пересмотра баланса между конфиденциальностью и правом на защиту. Решение данных вопросов должно основываться на детальном анализе соответствия ZKP фундаментальным принципам правосудия.

Этические риски внедрения ZKP сосредоточены на обеспечении баланса между конфиденциальностью данных и прозрачностью правосудия. Применение криптографических методов не должно подрывать общественное доверие к судебной системе из-за непрозрачности процедур верификации. Необходимо предотвратить возможные злоупотребления при использовании ZKP, такие как сокрытие релевантной информации под предлогом защиты конфиденциальности. Этические нормы требуют четкого определе-

ния границ применения протоколов с нулевым разглашением. Для поддержания доверия к системе необходимы гарантии независимости криптографических методов, используемых в ZKP. Создание специализированных надзорных органов или привлечение аккредитованных экспертов может обеспечить проверку корректности реализации протоколов. Такие меры способствуют минимизации рисков технических ошибок и злоупотреблений. Перспективы внедрения ZKP зависят от решения указанных этических вопросов при сохранении эффективности судопроизводства.

Заключение

Криптографические протоколы с нулевым разглашением (ZKP) представляют собой технологически обоснованное решение для преодоления фундаментального конфликта между необходимостью верификации доказательств и защитой конфиденциальности в судопроизводстве. Они позволяют доказывать соответствие данных установленным критериям, таким как валидность подписи или соблюдение временных рамок, без раскрытия самой конфиденциальной информации. Наряду с другими методами информационной безопасности электронного документооборота это обеспечивает баланс между прозрачностью судебного процесса и защитой личных или коммерческих тайн участников дела.

Разработанная концептуальная модель интеграции ZKP в судебные процедуры демонстрирует практическую осуществимость их применения как в гражданском, так и в уголовном процессе. Архитектура системы обеспечивает сохранение целостности доказательств на всех этапах — от представления до верификации — при строгом соблюдении требований конфиденциальности. Моделирование на примере типичного гражданского дела подтвердило функциональность подхода и его соответствие процессуальным нормам.

Несмотря на значительные преимущества, включая снижение рисков утечек данных и повышение доверия к судебным решениям, внедрение ZKP сталкивается с объективными ограничениями. К ним относятся высокая вычислительная сложность протоколов и необходимость адаптации существующих правовых норм к новым технологическим реалиям. Эти вызовы требуют взвешенного подхода при интеграции криптографических инструментов в судебную практику.

Для успешной имплементации предложенной модели рекомендовано поэтапное пилотное внедрение в практику. Параллельно необходима разработка стандартов и обучение специалистов работе с ZKP-системами. Такой подход минимизирует риски и откроет путь к системной модернизации судопроизводства в условиях цифровой эпохи, отвечая на вызовы защиты данных и технологического прогресса.

Литература

1. Дьяконова В. В. Этические вопросы применения цифровых технологий в судебной и правоохранительной деятельности // Вопросы российского и международного права. – 2025. – №3. – С. 584–591.

2. Качалова О. В. Частные и публичные интересы при производстве по уголовным делам и цифровизация уголовного судопроизводства // Правовое государство: теория и практика. – 2025. – №1. – С. 69–77.

3. Нажимова Н. А., Токарев С. В. Модель гибридной базы для хранения персональных данных на основе распределенной компьютерной сети blockchain // Современные наукоемкие технологии. – 2025. – №10. – С. 58–62.

4. Нейзов М. В., Кузьмин Е. В. Применение TLA+/TLC для моделирования и верификации криптографических протоколов // Моделирование и анализ информационных систем. – 2024. – №4. – С. 446–473.

5. Шумилин А. С. Метод обеспечения защиты персональных данных в медицинской облачной системе // Вопросы кибербезопасности. – 2023. – №4. – С. 53–64.

References

1. D'yakonova V. V. Eticheskie voprosy primeneniya cifrovyh tekhnologij v sudebnoj i pravoohranitel' noj deyatel'nosti // Voprosy rossijskogo i mezhdunarodnogo prava. – 2025. – № 3. – S. 584–591.

2. Kachalova O. V. Chastnye i publichnye interesy pri proizvodstve po ugolovnym delam i cifrovizaciy a ugolovnogo sudoproizvodstva // Pravovoe gosudarstvo: teoriya i praktika. – 2025. – № 1. – S. 69–77.

3. Nazhimova N. A., Tokarev S. V. Model' gibridnoj bazy dlya hraneniya personal'nyh dannyh na osnov e raspredelennoj komp'yuternoj seti blockchain // Sovremennye naukoemkie tekhnologii. – 2025. – № 10. – S. 58–62.

4. Neyzov M. V., Kuz'min E. V. Primenenie TLA+/TLC dlya modelirovaniya i verifikacii kriptograficheskih protokolov // Modelirovanie i analiz informacionnyh sistem. – 2024. – № 4. – S. 446–473.

5. Shumilin A. S. Metod obespecheniya zashchity personal'nyh dannyh v medicinskoj oblachnoj siste me // Voprosy kiberbezopasnosti. – 2023. – № 4. – S. 53–64.

ТИТОВ Евгений Сергеевич, аспирант Федерального государственного бюджетного образовательного учреждения высшего образования Уральский государственный университет путей сообщения. 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: eugene.titov@mail.ru

ЗЫРЯНОВА Татьяна Юрьевна, кандидат технических наук, доцент, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения. 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: tzyryanova@usurt.ru

TITOV Evgenij Sergeevich, post-graduate student at the Federal State Budgetary Educational Institution of Higher Education Ural State University of Railway Transport. 66 Kolmogorova St., Yekaterinburg, 650034. E-mail: eugene.titov@mail.ru

ZYRYANOVA Tatyana Yuryevna, Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Technology and Information Security at the Ural State University of Railway Transport. 66 Kolmogorova St., Yekaterinburg, 650034. E-mail: tzyryanova@usurt.ru

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76, ЮУрГУ,
Издательский центр

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(59) / 2026
Подписано в печать 15.06.2026. Дата выхода в свет 15.06.2026.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 7,0. Тираж 50 экз.
Заказ 129/166.
Цена свободная.

Отпечатано в типографии Издательского центра ФГАОУ ВО "ЮУрГУ (НИУ)".
454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(59) / 2026
Signed to print 15.06.2026. Date of publication of the 15.06.2026.
Format 70×108 1/16. Screen printing. Conventional printed sheet 7,0. Circulation – 50 issues.
Order 129/166.
Open price.

Printed in the printing house of the Publishing Center of FGAOU VO "SUSU (NIU)".
SUSU, Publishing Center, 76, Lenina Str., Chelyabinsk, 454080