Binary Neural Network Classifier in Election Forensics: A Russian Case Study *

Kirill Kalinin†

September 5, 2024

*Prepared for the Annual Meeting of the American Political Science Association, Philadelphia, PA, September 5-8, 2024. The author is grateful to Walter Mebane for sharing his data and providing suggestions at the initial stage of this project, and to Sergey Sanovich for his support of this project.

†Researcher at the Hoover Institution, Stanford University (E-mail: kkalinin@stanford.edu)

Abstract

This paper addresses the need to integrate estimates from election forensics methods with election observation data to enhance the accuracy and reliability of election fraud detection. It proposes utilizing neural networks for fraud prediction tasks. The study leverages data from the Russian federal elections (2012-2024) and election observation data from the *Karta Narusheniy* website. The paper explores the construction and optimization of neural networks for election forensics research, experimenting with various hyperparameters. The findings demonstrate that neural networks can significantly improve election fraud prediction by integrating diverse data sources and reducing false negatives in election observation. This research underscores the potential of machine learning to refine the precision and interpretability of election fraud detection methods.

Keywords: election fraud, neural networks, machine learning, eforensics, nonparametric method, election observation.

Introduction

Modern political science, particularly the emerging field of electoral forensics, has developed several methods to effectively detect and measure election fraud. These new approaches offer valuable opportunities for scholars and practitioners to explore electoral anomalies across different electoral contexts. Among the most popular methods are digit tests (Cantu and Saiegh 2011; Pericchi and Torres 2011; Mebane 2011; Beber and Scacco 2012; Kalinin and Mebane 2013), which focus on the distribution of digits in electoral data; various 1D methods guided by assumptions of normality or unimodality in detecting anomalies in turnout or vote shares (Myagkov, Ordeshook and Shaikin 2009; Shpilkin 2011; Kobak, Shpilkin and Pshenichnikov 2016; Kalinin and Mebane 2017); 2D methods based on correlation or bivariate regression analysis of turnout and vote shares (Sobyanin and Sukhovolsky 1995; Buzin and Lubarev 2008); and parametric methods relying on statistical modeling of election fraud (Klimek et al. 2012; Mebane 2016; Mebane et al. 2022). The methods vary considerably in terms of the measurement levels (precincts or higher levels of aggregation), underlying assumptions (unimodality assumption vs. normality assumption). At last, methodological differences between methods are overshadowed by the general problem of election forensics: the fundamental ambiguity of attributing the origin of anomalies to the results of normal politics (e.g., strategic behavior) or election fraud (Hicken and Mebane 2015; Mebane 2015).

Besides election forensics, election observation has become crucial in promoting clean and fair elections globally, emphasizing democratic rights and fostering external validation of election results (Bjornlund 2004). It allows autocrats to signal adherence to democratic norms while discouraging opposition by exposing corrupt activities (Simpser 2006). Studies show that the presence of observers can not only help monitor the occurrence of election fraud but also significantly reduce it (Hyde 2007, 2011; Kelley 2012; Sjoberg 2012; Enikolopov et al. 2013). However, it may also prompt strategic adaptations, such as shifting fraud to less detectable forms or neighboring areas (Ichino and Schundeln 2012; Sjoberg 2014).

While some data on election observation is available, it has not been systematically

integrated with electoral forensics for the purpose of fraud detection. This paper seeks to bridge this gap by combining the analytical rigor of electoral forensics with the detailed empirical observations provided by election monitors. By aligning these two approaches, we aim to enhance both the accuracy and reliability of fraud detection across various electoral contexts, ultimately yielding more robust findings and practical insights.

Historically, much of the research has focused on validating election forensics methods with electoral observation. For instance, Kalinin (2019) utilizes data from election observers, voting equipment, and geographical sources to validate the finite mixture model's results for the 2011 and 2012 elections. Similarly, Mebane et al. (2022) examines 32 real-world elections to validate electronic forensics measures derived from the eforensics model. The first attempt to transition from validation to integration within the machine learning framework was implemented in Kalinin (2024). This study applies supervised machine learning algorithms to predict election fraud reported by observers, utilizing various election forensics measures based on data from the 2018 Russian presidential election, collected by activists from the For Fair Elections movement. The study compares five supervised machine learning algorithms: Decision Trees, Neural Networks, Boosted Trees, Support Vector Machines (SVMs), and k-Nearest Neighbors (k-NN), with SVMs demonstrating the best performance on the dataset. Independent observers were able to download footage from 8,000 out of 46,000 polling stations equipped with webcams. A total of 271 reports and observations were analyzed using different machine learning methods.

Hence, the present study builds upon Kalinin (2024) but takes a different perspective by focusing on neural networks and utilizing election observation data from the *Karta Narushenyy* (*Election Violations Map*) website. This platform, operated by the Movement for Voters' Rights *Golos*, covers all Russian federal elections held between 2012 and 2024. The website collects and publishes information on potential violations of electoral standards and laws in Russia (see Appendix B for more details). The service operates on a crowdsourcing model, where users contribute content, while the project organizers handle initial

moderation and technical support. Consequently, the election observation data constitutes a convenience sample, as observers self-select into the sample, unlike the election observation data from the 2011 Moscow parliamentary elections collected by *Citizen-Observer* (Enikolopov et al. 2013). This self-selection introduces potential biases that may affect the ability to make broad generalizations. Despite this limitation, this paper presents an algorithm that integrates election forensics with election observation, offering a novel approach to analyzing electoral integrity.

The structure of this paper is as follows. Section 1 provides an overview of election forensics methodology, focusing on digit tests and three precinct-level estimation approaches for election fraud: *Shpilkin's* nonparametric method, univariate finite mixture models (both precinct-based and histogram-based), and Mebane's multivariate finite mixture model (*BFMM* or *eforensics*). Section 2 details the empirical strategy, neural network architecture, and the training data. Section 3 presents the results of the machine learning analysis. The final section offers conclusions and discusses prospects for future research.

Measuring Election Fraud

Election fraud is an inherently opaque phenomenon. It involves clandestine efforts on the part of the perpetrators to shape election results in a desired direction (Lehoucq 2003). It can also be viewed as "a conduct intended to corrupt the process by which ballots are obtained, marked, or tabulated; the process by which election results are canvassed and certified" (Donsanto 2008). Although the hidden origins of fraud make it difficult to study, election forensics methodology suggests that election fraud may leave distinct traces in the electoral data that researchers intend to uncover. From a practical perspective, the difficulty of this task is compounded by data availability issues related to the lack of fine-grained data and suitable covariates to build complex explanatory models of election fraud. Despite these challenges, election forensics methods can provide accurate information about election viola-

tions, designed to separate false accusations from true evidence of election malpractice, and thereby help election observers assess the quality of elections and understand the geography of election fraud (Hicken and Mebane 2015, 4).

Digital Tests of Election Forensics

Digit tests analyze the distribution of digits in vote counts as indicators of anomalies. These tests compare empirical distributions with pre-specified theoretical distributions. Among the most popular methods are those analyzing the first digits of aggregate vote totals (Cantu and Saiegh 2011), second significant digits (Pericchi and Torres 2011; Mebane 2011), the last digits in vote counts (Beber and Scacco 2008), or the last digits in percentages (Kalinin and Mebane 2013). Different digit tests focus on specific digits in vote counts or percentages, capturing various types of election fraud.

Second-Digit Test Second-digit methods are grounded in the principle that non-anomalous vote counts should conform to the second-digit Benford's Law (2BL) distribution. According to Benford's Law, the expected relative frequencies of the second digit are as follows: $q_0, \ldots, q_9 = (0.120, 0.114, 0.109, 0.104, 0.100, 0.097, 0.093, 0.090, 0.088, 0.085)$. This approach has been elaborated in works by Pericchi and Torres (2011), Mebane (2011), and Mebane (2006). The 2BL test involves comparing the arithmetic mean of the second digits of vote counts to the theoretical mean value expected under the 2BL distribution.

However, the second-digit test has faced criticism as a tool for election forensics. For instance, Deckert, Myagkov and Ordeshook (2011) argues that the 2BL test is prone to false positives and lacks a robust theoretical foundation to account for variations due to election laws, strategic voting patterns, or the number of candidates. Further critiques by Mebane (2012) and Mebane and Klaver (2015) highlight the test's sensitivity to strategic, gerrymandered, and coerced votes, which complicates the differentiation between strategic behavior and election fraud. Consequently, the 2BL test is no longer regarded as a reliable

method for detecting electoral fraud.

Last-digit Tests Beber and Scacco (2012) propose the last-digit test based on the principle that clean vote counts should have uniformly distributed last digits from 0 to 9. The authors outline several conditions that must be met for the test to be valid: (a) vote counts should not cluster within a narrow range of numbers, and there should be minimal variation in election unit sizes, electoral support, or turnout; (b) vote returns should not include many single- and double-digit counts, meaning the method should not be applied to minor candidates with small vote counts or to small polling stations. Once these conditions are satisfied, any statistically significant deviation from the uniform distribution can be interpreted as indicative of electoral fraud. The last-digit approach can be extended to various electoral variables that meet these conditions, including counts, percentages of ballots, and electoral returns.

Additionally, the last-digit approach has been extended by introducing a new test for the last digit of percentages, supported by the concept of signaling games. This extension posits that election fraud serves as a fundamental signaling mechanism for regional leaders' loyalty and their capacity to manipulate administrative resources for the benefit of the Kremlin (Kalinin 2022*b*). During electoral signaling, data manipulation is likely to be associated with rounded percentages of electoral support, as this represents a straightforward and easily detectable method of conveying basic information to superiors.

Models of Election Forensics

In this section, I provide an overview of three primary approaches to estimating election fraud at the precinct level: the nonparametric approach, the univariate finite mixture modeling approach, and the multivariate finite mixture modeling approach. Each of these methods is based on the core assumption of multimodality and the concept of a *clean* mode. These approaches yield precinct-level quantities of electoral anomalies, which are crucial for this

paper. A detailed description of each method can be found in Kalinin (2022*a*).

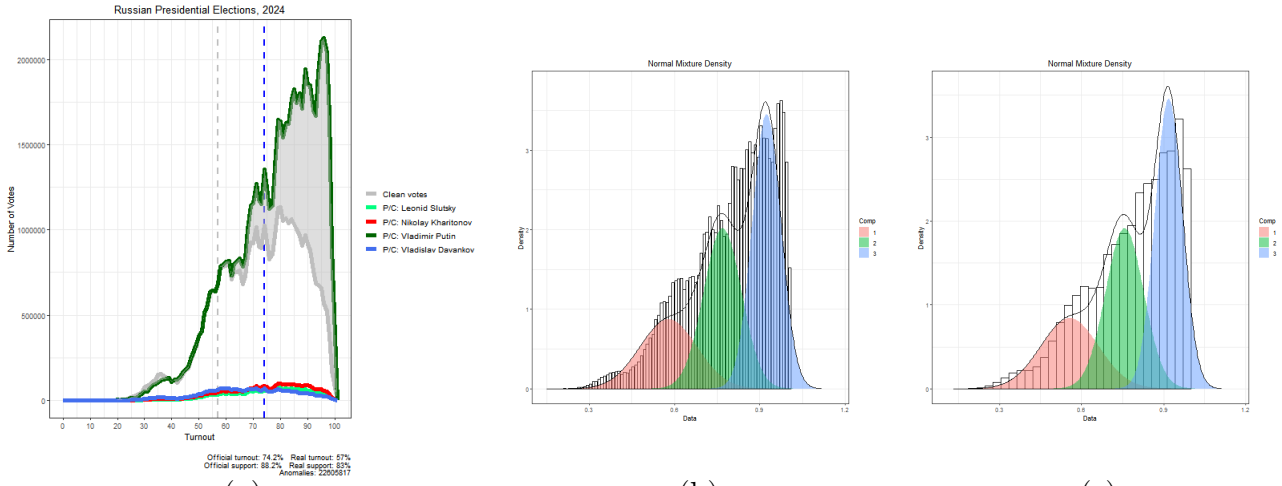
Nonparametric Method In 2007, Sergey Shpilkin introduced a nonparametric method based on vote-turnout histograms. This method estimates the number of votes allegedly stolen by the winning candidate and has been used to assess election fraud at both national and regional levels in all Russian federal elections since 2000. Due to the lack of a fully documented algorithm and replication code, this paper builds upon the approach developed by Kalinin and Mebane (2019) to present a replication algorithm. The R code for this algorithm is available on GitHub at https://github.com/kkalininMI/EFToolkit.

The nonparametric method models the number of ballots received by each party as a function of turnout and the corresponding vote share at each polling station. It constructs a turnout-vote count histogram, where turnout (on the x-axis) is partitioned into 100 bins, and the support for each party or candidate is computed within each bin (on the y-axis). This approach presumes the existence of a *clean* mode and uses the highest left-side mode to estimate instances of fraud, relying on the assumptions of normality or unimodality. A primary challenge of this method is the precise identification of the clean mode, particularly in complex, multimodal distributions.

A significant drawback of the nonparametric method is that, while it provides aggregate measures of election fraud associated with the winner, these measures are not available at the precinct level, making the method unsuitable for fine-grained precinct-level analysis. However, this issue has been addressed by Kalinin (2022*a*) through post-stratification, which adjusts the precinct-level data to align the distribution of the winner's vote counts with the known histogram-based distribution of clean votes.

Univariate Finite Mixture Models A straightforward alternative to the nonparametric approach for deriving precinct-level measures is the estimation of a finite mixture model for a univariate electoral variable (e.g., turnout) using the expectation-maximization (EM) algorithm (Kalinin 2022*a*). Univariate finite mixture models serve as an intermediary between the

Figure 1: An Example of Nonparametric Approach



(a) (b) (c)

Notes: (a) replication of *Shpilkin's* method for 2024 presidential elections; (b) univariate finite mixture model (histogram-based) for 2024 presidential elections; (c) univariate finite mixture model (precinct-based) for 2024 presidential elections.

nonparametric method and more complex multivariate finite mixture models. These models effectively represent latent group structures in the data and model intricate distributions by estimating components that capture local variations driven by different data-generating processes. Consequently, mixture models can clarify the distinct mechanisms underlying observed multimodality. The expectation-maximization (EM) algorithm is the most commonly used technique for fitting mixture distributions and estimating model parameters. There are two variants of univariate finite mixture models: (a) a univariate density based on precinct-level turnout (*EMprecinct*) and (b) a univariate density based on the histogram's electoral matrix (*EMhistogram*). Both approaches are employed in the current analysis.

Multivariate Finite Mixture Models The first parametric model for election forensics, based on a goodness-of-fit test, was proposed by Klimek et al. (2012). This model rests on two key assumptions: first, that a winning party or candidate with the most votes benefits from votes transferred from other parties or candidates, as well as from nonvoters; and second, that turnout is correlated with the extent of election fraud. The model has been

tested across a range of autocracies and democracies and has demonstrated effectiveness at various levels of data aggregation.

The Bayesian implementation of the finite mixture model (*eforensics* or *BFMM*) represents a generalization of the model introduced by Klimek et al. (2012) and Mebane (2016). The work of Mebane et al. (2022) extends these concepts by differentiating between *incremental fraud*, which involves moderate vote transfers (ballot switching), and *extreme fraud*, characterized by extreme cases of vote transfer (ballot stuffing). Unlike the nonparametric method, which is based on the aggregation principle by first estimating precinct-level fraud and then aggregating to the election level, the parametric model directly incorporates aggregation. Additionally, while nonparametric methods and univariate finite mixture models rely on bootstrapping to derive observation-level measures of uncertainty, the Bayesian framework provides credible intervals for observation-level quantities directly from the model.

Empirical Strategy: Data and Methods

The empirical strategy employs a neural network classifier to predict precinct-level election fraud by analyzing electoral data alongside election forensics measures. The model's input consists of this combined dataset, while the output is a binary classifier that categorizes each precinct as either fraudulent or non-fraudulent. This approach facilitates a data-driven assessment of election integrity, integrating both raw electoral data and specialized forensic indicators.

Data

Target variable: election observation The target variable is a binary indicator derived from data obtained from the *Karta Narushenyy* website, which documents various types of electoral violations. The coding schemes for election violations differ from year to year (see Appendix B). For this study, precincts were included in the dataset if an observer reported

any of the following violations: *violation of election results tabulation rules*, *distortion of results*, *illegal voting*, or *violations during vote counting*. All other precincts were coded as 0.

The data presented in Table C1 in the Appendix C provides a comprehensive overview of the proportion of precincts with observed election fraud across various Russian regions from 2012 to 2024. The figures reveal significant variability in reported fraud rates over time and across regions, highlighting both consistent patterns and fluctuations in electoral integrity.

In general, electoral observation data indicate that larger cities, such as Moscow and St.Petersburg, exhibit notably higher proportions of reported fraud at the precinct level compared to more rural regions. For instance, Moscow consistently records some of the highest detected fraud rates over the years, peaking at 0.140 in 2021 and demonstrating significant levels in other years as well. St. Petersburg follows a similar trend, with a peak fraud rate of 0.136 in 2012, though it exhibits some variability in subsequent years. These elevated figures likely reflect enhanced electoral monitoring capabilities in these major cities rather than an inherently contentious political climate. Emphasizing these regions is crucial, as they contribute significantly to neural network training for election fraud detection, while also presenting challenges for extrapolating findings to the rest of the country.

Conversely, several regions consistently show low levels of reported fraud. For example, areas such as Gorod Baykonur and the Republic of Kalmykia exhibit relatively minimal fraud rates over the years. The Republic of Kalmykia, in particular, shows minimal variation, with a peak of 0.079 in 2012 but generally low figures in subsequent years. This may suggest either a lack of reported incidents or the presence of effective electoral practices in these regions. Some regions, however, have displayed significant fluctuations in fraud rates over time. For instance, the Republic of Chechnya shows a substantial drop from 0.048 in 2012 to 0.000 in later years. This decline is likely due not to improvements in monitoring but rather to the absence of election observation, a factor that must be considered when training our models.

The electoral observation data highlights the intricate challenges of detecting and report-

ing electoral fraud. The variability observed across different regions and years suggests that a range of factors – including local political dynamics, the effectiveness of election monitoring, and regional differences in reporting practices—significantly influence these outcomes. The data also reflects the impact of varying regional governance regimes, which can shape the extent and visibility of electoral anomalies.

Input features: official electoral data (vote tallies) The input features for the neural network consist of precinct-level electoral data, including vote counts and vote shares, as well as election forensics estimates derived from various methods, such as digit tests, and parametric and nonparametric election forensics approaches previously discussed.

For a clearer understanding of the election forensics component among the input features, refer to Table 1, which presents the proportion of precincts with observed election fraud across different years, analyzed using these methods. The primary data source for this analysis is the precinct-level official electoral data from Russian federal elections and a referendum.

Notably, extreme values are observed in 2024, with *Shpilkin's* method indicating an unusually high fraud proportion of 0.964, and the $EM_{precinct}$ method reaching a perfect 1.000. These high proportions suggest a substantial detection of fraud in 2024, which could reflect either an increase in actual fraud or a heightened sensitivity of the methods employed.

Table 1: Proportion of Precincts with Election Fraud Across Different Election Forensics Methods, by Year

Year	Shpilkin's	$\text{EM}_{precinct}$	$\text{EM}_{histogram}$	BFMM	Average
2012	0.411	0.596	0.313	0.224	0.386
2016	0.457	0.683	0.277	0.191	0.402
2018	0.436	0.414	0.326	0.294	0.367
2020	0.697	0.523	0.721	0.531	0.618
2021	0.502	0.721	0.312	0.183	0.429
2024	0.964	1.000	0.943	0.672	0.895

Notes: Shpilkin's – *Shpilkin's* estimates; (b) $EM_{precinct}$ – univariate finite mixture model (precinct-based); (c) $EM_{histogram}$ – univariate finite mixture model (histogram-based); (d) *BFMM* – Bayesian finite mixture model's estimates.

Conversely, the *BFMM* method consistently reports the lowest proportions, particularly

in 2024 with a value of 0.672, indicating a potentially more conservative detection threshold. The dynamics across years show variability in fraud detection, with some methods like *Shpilkin's* and $EM_{precinct}$ exhibiting significant fluctuations, suggesting either evolving patterns of fraud or differing methodological sensitivities over time. These extreme cases and their variations underscore the impact of the chosen forensic methods on observed fraud proportions and highlight the need for careful interpretation of these estimates in different electoral contexts.

Methods

In this section, I will explore the theoretical foundation of the neural network implementation designed for election fraud prediction. The discussion will focus on three key areas: the core principles of neural networks, the application of the focal loss function to address the class imbalance inherent in fraud detection, and the necessity of oversampling techniques to ensure the model remains well-calibrated and robust when handling imbalanced data.

Neural Networks Architecture A neural network consists of interconnected units called neurons that work together to solve complex problems. In a feedforward neural network, the information moves in only one direction—from the input layer through the hidden layers to the output layer. Each layer is composed of several neurons, and each neuron in a layer is connected to every neuron in the subsequent layer.

Mathematically, the output y of a neural network can be expressed as:

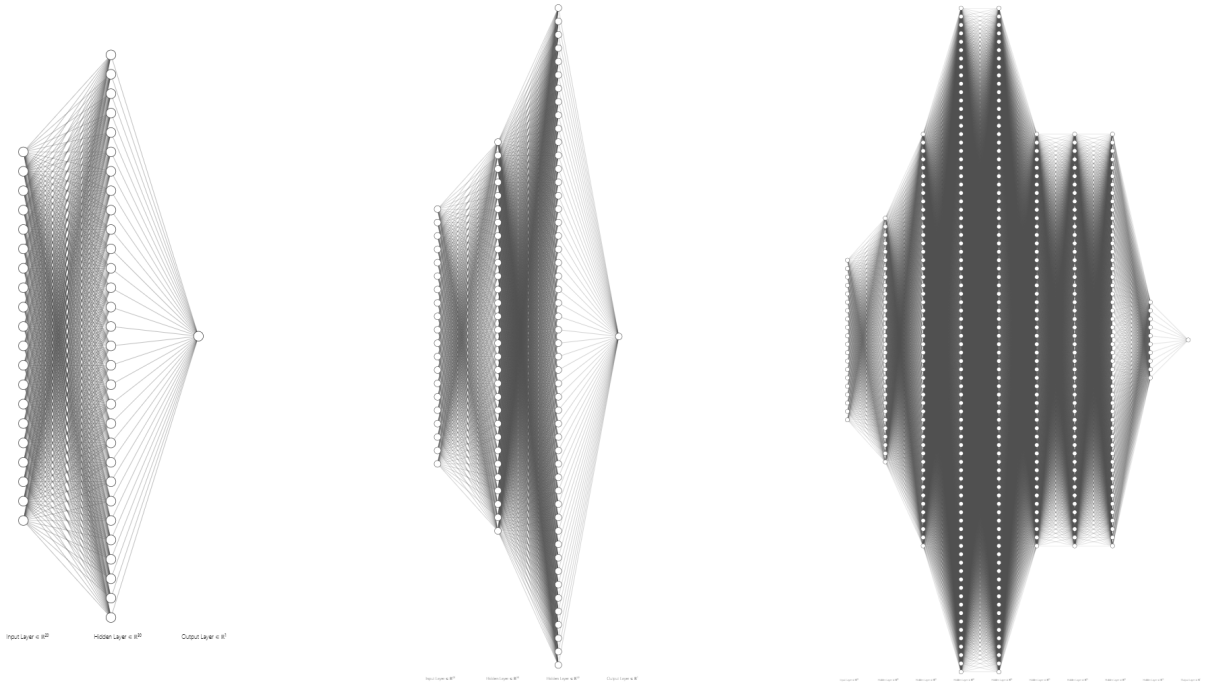
$$y = \sigma(W_3 \cdot \sigma(W_2 \cdot \sigma(W_1 \cdot x + b_1) + b_2) + b_3) \tag{1}$$

where:

- x is the input vector,
- W_1, W_2, W_3 are the weight matrices for each layer,

- b_1, b_2, b_3 are the bias vectors,
- σ is the activation function (e.g., ReLU, Sigmoid).

Figure 2: Fully Connected Neural Network (FCNN) Architectures



(a) (b) (c)

Notes: The FCNN architectures utilized in this paper are as follows: (a) *SmallNN*, (b) *AverageNN*, and (c) *LargeNN*.

The objective of the neural network is to learn from input features and predict whether a specific voting precinct or region is likely to have experienced fraud. During training, the network adjusts its internal parameters (weights and biases) to minimize the discrepancy between its predictions and the actual outcomes in the training data. The input layer processes the voting statistics, which are fed into the network. The architecture of the network, including the number of layers and neurons per layer, significantly impacts its performance. While a deeper network can capture more intricate patterns, it may also demand more computational resources and risk overfitting if not appropriately regularized.

In my election fraud prediction model, I have implemented three neural network architectures: *SmallNN*, *AverageNN*, and *LargeNN*. Each model varies in complexity, with an

increasing number of layers and nodes, tailored for binary classification tasks.

The *SmallNN* model is the simplest of the three, consisting of three fully connected layers (See Table 2(a)). The first layer takes the input data and maps it to 20 nodes, followed by a second layer with 30 nodes. The final layer outputs a single value, which is passed through a sigmoid activation function to produce a binary classification. The two hidden layers use the $ReLU$ activation function to introduce non-linearity, making this model suitable for tasks where a smaller network is sufficient.

The *AverageNN* model builds upon the *SmallNN* by adding an additional fully connected layer (See Table 2(b)). It starts similarly with 20 nodes in the first layer, followed by 30 nodes in the second layer, and then a third layer with 50 nodes. The final layer still outputs a single value, processed by the sigmoid function for binary classification. This architecture allows the network to capture more complex relationships in the data while still remaining relatively lightweight.

The *LargeNN model* is the most complex, with a total of 10 fully connected layers (See Table 2(c)). Starting with 20 nodes in the first layer, it gradually increases to 100 nodes by the fourth and fifth layers, then decreases back to 10 nodes before the final output layer. Each hidden layer is followed by a $ReLU$ activation function, enabling the model to learn intricate patterns in the data. The final output is passed through a sigmoid activation function for binary classification. This deep architecture is designed for scenarios where the data is highly complex and requires a large capacity to accurately model the underlying patterns.

Loss function The loss function is a critical component in training a neural network. It measures how well the network's predictions match the actual outcomes. The training process aims to minimize this loss, thereby improving the model's accuracy. For binary classification tasks, the most commonly used loss function is the Binary Cross-Entropy (BCE) loss. The BCE loss for a single prediction is defined as:

$$\text{BCE}(y, \hat{y}) = -\left[y \cdot \log(\hat{y}) + (1 - y) \cdot \log(1 - \hat{y})\right] \tag{2}$$

where:

- y is the actual label (0 or 1),
- $\hat{y}$ is the predicted probability.

However, when dealing with highly imbalanced data, such as predicting election fraud (where fraudulent cases are much rarer than non-fraudulent cases), the BCE loss may not be sufficient. In such cases, the model might become biased towards the majority class, leading to poor performance on the minority class. To address the issue of class imbalance, the Focal Loss function was introduced by Lin et al. (2018). Focal Loss is a modification of the BCE loss that down-weights the loss for well-classified examples and focuses more on hard-to-classify examples.

The Focal Loss is defined as:

$$\text{FL}(y, \hat{y}) = -\alpha \cdot (1 - \hat{y})^{\gamma} \cdot y \cdot \log(\hat{y}) - (1 - \alpha) \cdot \hat{y}^{\gamma} \cdot (1 - y) \cdot \log(1 - \hat{y}) \tag{3}$$

where:

- α is a weighting factor for the minority class,
- γ is a focusing parameter that adjusts the rate at which easy examples are down-weighted.

The Focal Loss reduces the loss contribution from easy examples, allowing the model to focus more on difficult examples, which are often the minority class in an imbalanced dataset. In my specific application, some regions are overrepresented in the dataset, which

could lead to biased predictions. To counteract this, the loss function can be weighted by region. Regions with more fraudulent observed cases are assigned lower weights, while those with fewer fraudulent cases are assigned higher weights. This ensures that the model does not become biased towards regions with more data, thereby providing a fairer and more accurate prediction across all regions.

This expression incorporates both the focal loss component and the application of weights:

$$\text{FL}(y, \hat{y})_w = \alpha \cdot (1 - \sigma(\text{inputs}))^\gamma \cdot [-y \log(\sigma(\text{inputs})) - (1 - y) \log(1 - \sigma(\text{inputs}))] \cdot \text{weights} \quad (4)$$

Where:

- $\sigma(\text{inputs})$ denotes the sigmoid function applied to the inputs to obtain p_t.
- α is a weighting factor for the class.
- γ is the focusing parameter.
- weights are applied to the focal loss:

$$\text{weights} = \frac{1.0}{\text{region\_fraud\_counts\_from\_el.observation} + 1 \times 10^{-2}}$$

.

Class imbalance is a prevalent challenge in machine learning, particularly in binary classification tasks such as fraud detection, where the minority class (fraud) is significantly underrepresented compared to the majority class (non-fraud). Without appropriate mitigation, this imbalance can lead to models that are biased towards the majority class, resulting in suboptimal performance on the minority class. A common technique to address class imbalance is oversampling the minority class. Simple oversampling involves duplicating existing minority class samples to equalize the size of the majority class, which can result in

overfitting, as the model may become overly attuned to the duplicated patterns of the minority class. Alternatively, SMOTE (Synthetic Minority Over-sampling Technique) improves the dataset by generating synthetic samples through interpolation between existing minority class instances (Chawla et al. 2002). This approach not only balances the class distribution but also introduces variability into the training data, enhancing model generalization. By creating new, synthetic examples that reflect the underlying distribution of the minority class, SMOTE helps to prevent overfitting and boosts the model's ability to generalize to unseen data. Therefore, SMOTE is often preferred over simple oversampling for its ability to offer a more nuanced and robust solution to class imbalance. In the current implementation, however, simple oversampling is used.

For more details on the technical description, see Appendix A.

In summary, the neural network for election fraud prediction is an advanced binary classification model specifically engineered to handle imbalanced datasets through the application of customized loss functions and region-based weighting strategies. The choice of loss function, the approach to class imbalance via oversampling, and the careful design of the network architecture are pivotal in enhancing the classifier's performance in detecting election fraud. By targeting difficult cases and adjusting the influence of different regions, the classifier aims to deliver accurate and balanced predictions across the entire dataset.

I tested all three models—*SmallNN*, *AverageNN*, and *LargeNN*– using both Binary Cross-Entropy (BCE) loss and Focal Loss, with region-based weighting to address data imbalance. A learning rate of 0.005 was consistently applied across all cases. Model performance was primarily evaluated using F1 scores, a metric that balances precision and recall, making it particularly suitable for imbalanced datasets. By focusing on F1 scores, the model's ability to accurately identify positive cases (fraud) is appropriately weighed against minimizing false positives, providing a comprehensive assessment of model effectiveness in election fraud detection. Additional technical details of the model are provided in the Appendix A.

Findings

Performance Evaluation Table 2 presents the F1 scores for three neural network models (*SmallNN*, *AverageNN*, and *LargeNN*) across the years (2012 to 2024), comparing their performance using both Cross-Entropy and Focal Loss. For the *SmallNN* model, the F1 scores are generally higher when using Cross-Entropy loss, with a peak of 0.956 in 2016, indicating effective handling of imbalanced data in that year. However, the performance with Focal Loss is consistently lower, suggesting that while Focal Loss aims to address class imbalance by down-weighting easy-to-classify examples, it may not be as effective for this model size across the dataset, particularly in 2012, 2018, and 2020.

For the *AverageNN* model, Cross-Entropy loss consistently outperforms Focal Loss in most years, with a notable exception in 2016, where both loss functions yield similar high F1 scores around 0.93-0.94. However, Focal Loss shows a significant drop in F1 scores to 0.333 in 2012, 2020, and 2021, indicating challenges in generalizing during those years. The *LargeNN* model exhibits similar trends, with Cross-Entropy loss performing well in 2012 and 2016 but encountering severe performance issues from 2020 onward. Focal Loss results for the *LargeNN* model are particularly poor, consistently returning the minimum score of 0.333 across all years except 2016. Part of the reason for Cross-Entropy loss's superior performance is its ability to more effectively focus on clean precincts and regions with higher observed election fraud, while Focal Loss struggles in this regard. These results suggest that while Cross-Entropy remains robust across models and years, Focal Loss, particularly in deeper networks, may require further tuning or adjustments to achieve comparable performance.

According to Table 3, which presents a series of figures, Cross-Entropy loss consistently demonstrates higher learning rates across all epochs for each year, particularly for the small and average models. This trend is evident as both model sizes exhibit decreasing training and test losses, indicating effective learning and minimal overfitting. Despite training for 50 epochs, there is potential for further improvement; extending the number of epochs could enhance model performance. The increasing F1 scores underscore the models' improved

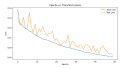
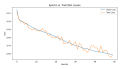
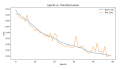
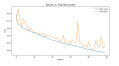
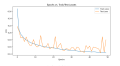
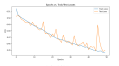
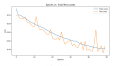
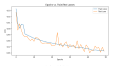
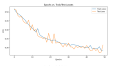
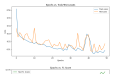
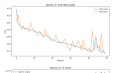
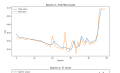
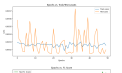
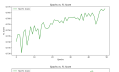
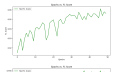
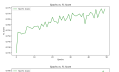
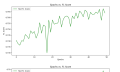
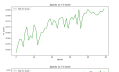
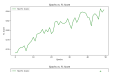
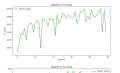
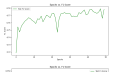
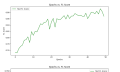
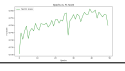
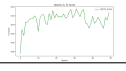
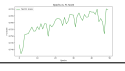
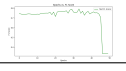
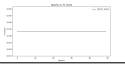
Table 2: F1 Score Performance Comparison Across Models and Years

Year	*SmallNN*		*AverageNN*		*LargeNN*	
	CE	FL	CE	FL	CE	FL
2012	0.768	0.713	0.764	0.333	0.750	0.333
2016	0.956	0.941	0.930	0.940	0.944	0.333
2018	0.774	0.738	0.777	0.748	0.770	0.333
2020	0.764	0.735	0.766	0.333	0.333	0.333
2021	0.786	0.752	0.778	0.333	0.333	0.333
2024	0.843	0.770	0.868	0.772	0.333	0.333

Notes: CE – Cross-Entropy, FC – Focal Loss, weighted.

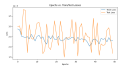
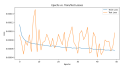
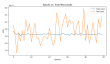
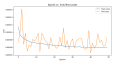
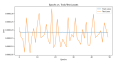
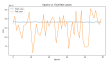
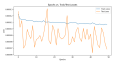
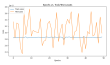
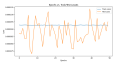
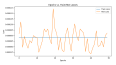
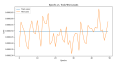
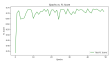
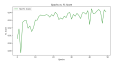
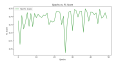
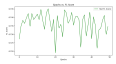
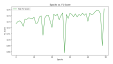
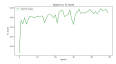
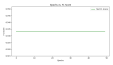
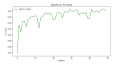
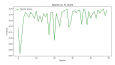
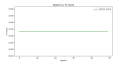
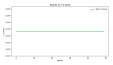
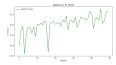
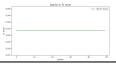
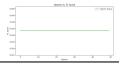
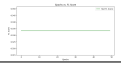
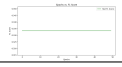
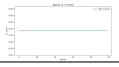
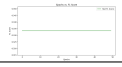
accuracy on imbalanced data. In contrast, the large model shows significantly poorer performance, with stagnant F1 scores indicating ineffective learning. This underperformance may be due to the model's increased complexity, leading to overfitting where the model captures noise rather than meaningful patterns in the data.

Table 3: Learning Curves and F1 Scores Across Epochs for Cross-Entropy Loss

Years	2012	2016	2018	2020	2021	2024
SmallNN, learning curves						
AverageNN, learning curves						
LargeNN, learning curves						
SmallNN, F1 scores						
AverageNN, F1 scores						
LargeNN, F1 scores						

The results for Focal Loss, as presented in Table 3, demonstrate considerable learning challenges across all model sizes – small, average, and large. These models struggle to effectively learn from the data, with particular difficulties observed during the 2012-2016 and 2021-2024 periods. Although some learning is evident, the training and test losses are characterized by significant noise, indicating poor generalization to unseen data – a critical issue in machine learning. Contrary to expectations, the larger model, which was presumed to handle data complexity more effectively, fails to resolve these issues. In fact, the smaller and average models frequently outperform the larger model. These findings suggest the need

Table 4: Learning Curves and F1 Scores Across Epochs for Focal Loss

Years	2012	2016	2018	2020	2021	2024
SmallNN, learning curves						
AverageNN, learning curves						
LargeNN, learning curves						
SmallNN, F1 scores						
AverageNN, F1 scores						
LargeNN, F1 scores						

for further hyperparameter tuning, particularly in terms of learning rates and the number of epochs.

The F1 scores, a valuable metric for summarizing accuracy improvements, provide key insights into the models' performance. Both the small and large models achieve relatively high F1 scores on the test set within the first 10-20 epochs. However, beyond this initial improvement, there is no significant gain in performance with further training. This plateau suggests that the models are not effectively learning beyond a certain point, potentially due to overfitting or an inability to capture more nuanced patterns in the data. The average model, while showing a more gradual improvement, still faces similar limitations, highlighting a broader challenge in using focal loss for this task.

In summary, the focal loss approach, although intended to address imbalanced data, proves insufficient in this context. The models, irrespective of size, struggle with generalization and show limited learning progression after the initial stages of training. This underscores the need for further refinement of the model architecture or loss function, potentially incorporating additional techniques such as regularization or alternative loss formulations to enhance the models' robustness and generalization capabilities.

Election Fraud Analysis Table 5 presents a comparative analysis of the proportion of precincts with observed election fraud for various models and loss functions across different

Table 5: Predicted Proportions of Fraudulent Precincts Based on Observation Data for Different Models and Loss Functions, by Year

Year	*SmallNN*		*AverageNN*		*LargeNN*	
	CE	FC	CE	FC	CE	FC
2012	0.302	0.224	0.276	1.000	0.283	0.000
2016	0.068	0.114	0.071	0.111	0.084	1.000
2018	0.329	0.427	0.352	0.308	0.361	1.000
2020	0.350	0.420	0.384	0.000	1.000	0.000
2021	0.281	0.284	0.288	1.000	0.000	1.000
2024	0.176	0.247	0.226	0.216	1.000	1.000

Notes: CE – Cross-Entropy, FC – Focal Loss, weighted.

election years. The data reveal that the *SmallNN* model, when using Cross-Entropy loss, often identifies a higher proportion of fraud in earlier years compared to Focal Loss. However, in 2016 and 2020, the Focal Loss shows extreme results, achieving a maximum value of 1.000 for the *AverageNN* model in 2020 and 2021, while the Cross-Entropy loss does not exhibit such high values. For the *LargeNN* model, Focal Loss consistently results in a proportion of 1.000, indicating a potential issue with generalization or overfitting, as the model appears to classify nearly all precincts as having fraud. This contrasts with the Cross-Entropy loss, which shows more variability and often lower proportions. These patterns suggest that while Focal Loss aims to address class imbalance, it may lead to overfitting or extreme predictions in certain contexts, highlighting the need for careful evaluation and potential adjustments in its application.

The key takeaway is that the choice of method or model has a significant impact on the predicted proportions of fraudulent precincts. Different models and loss functions with varying sensitivities can report divergent levels of detected fraud, reflecting differences in detection capabilities and potentially differing interpretations of fraud. For the small model, the Focal Loss function consistently yields higher fraud proportions compared to the Cross-Entropy function across all years. This suggests that the Focal Loss function, designed to address class imbalance and enhance learning about fraudulent precincts, may be more effective in detecting fraud in specific contexts, particularly where fraud is less prevalent or more

challenging to identify. In the average and large models, results exhibit more pronounced variability. The average model using Focal Loss reports a perfect score of 1.000 for fraud detection in 2012 and 2021 but identifies no fraud in 2020, indicating possible overfitting or instability in the model's generalization across different years. Similarly, the large model using Cross-Entropy shows extreme results, detecting fraud with a proportion of 1.000 in 2020 and 2024 but none in 2021. The large model's performance with Focal Loss is equally polarized, demonstrating that while the model may capture specific patterns, it fails to generalize consistently, leading to either extreme sensitivity or complete insensitivity to fraud detection in certain years.

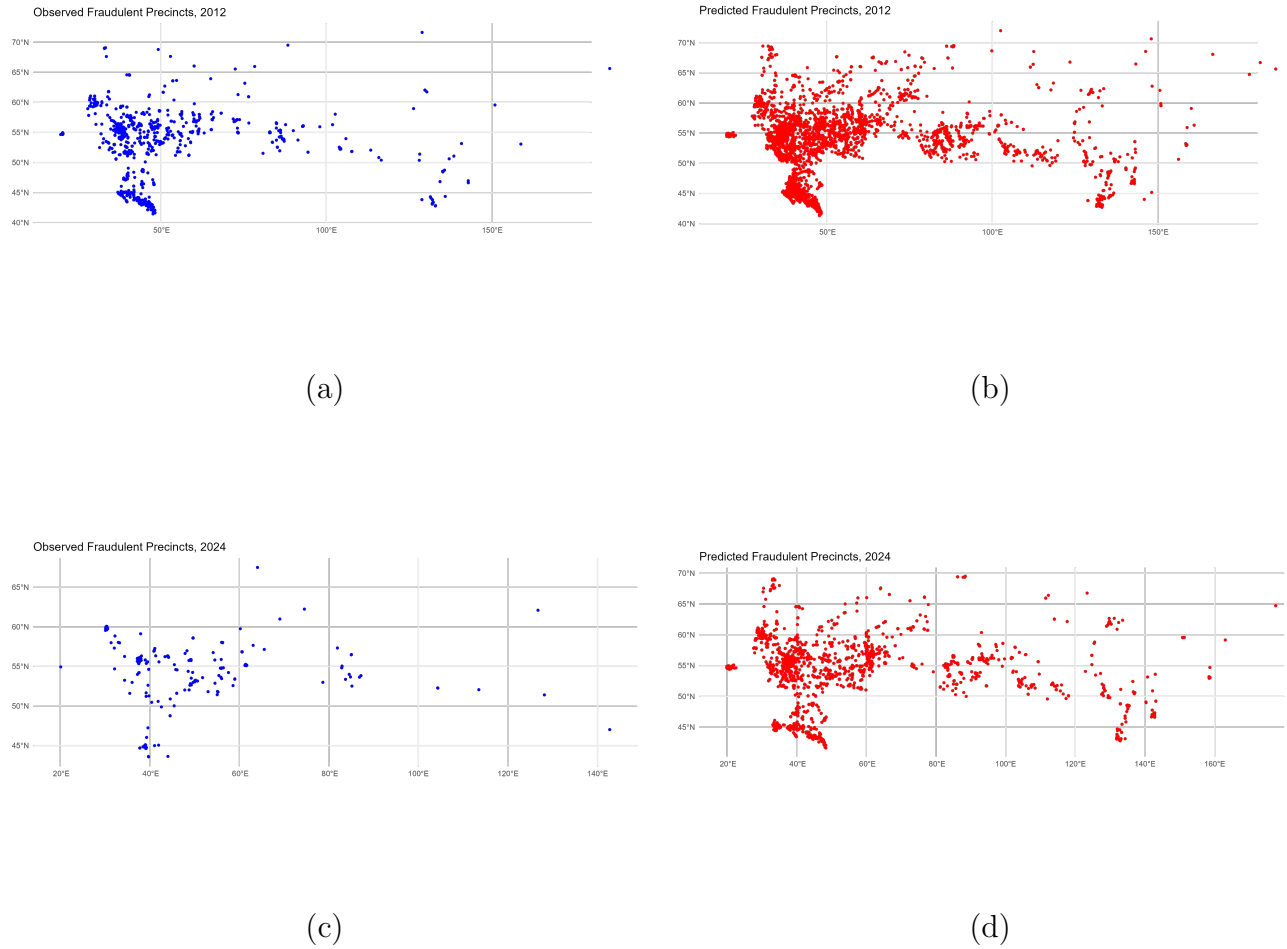
In Table C2 of the Appendix, which presents the proportion of predicted precincts with election fraud across various regions from 2012 to 2024 using the small model and cross-entropy loss, several notable patterns and extreme cases emerge when comparing oblasts and republics. Chechnya is particularly noteworthy for its exceptionally high proportion of fraudulent precincts in 2012 (0.515), which is significantly higher than most other regions. This trend indicates persistent issues within the region over the years; however, the proportion of fraud drops markedly in 2020 and 2024, suggesting possible changes in data reporting or model performance. In contrast, Moscow and St. Petersburg consistently report high proportions of fraud across multiple years, with values exceeding 0.90. This sustained high level of predicted fraud is likely due to a high volume of election observer reports rather than an increase in actual election fraud. Regions such as Ingushetiya and Dagestan exhibit considerable variation in fraud proportions. For example, Dagestan shows a notable decrease in predicted fraud proportions over the years, declining from 0.236 in 2012 to 0.066 in 2024. Conversely, Yevreyskaya AO consistently reports low fraud proportions throughout the years (ranging from 0.139 to 0.060), marking it as an outlier with persistently minimal predicted fraud. This may be attributable to effective controls or lower incidence rates of fraud in this region.

Table C3, based on data generated for the small model using Focal Loss, highlights signif-

icant variability in the predicted proportions of fraudulent precincts across different regions and years. For instance, Chechnya, despite showing high fraud predictions in 2012 (0.423), experiences a sharp decline to 0.000 in 2024, suggesting potential data inconsistencies. Regions such as Moscow and St.Petersburg exhibit consistently high values over several years, while Sakhalin oblast shows lower and more stable values over time, indicating less fluctuation in perceived fraud levels. Regions with low fraud predictions, such as Yevreyskaya AO and Zabaykalsky krai, display more consistent results. Yevreyskaya AO's fraud rates range from 0.117 to 0.281 across years, while Zabaykalsky krai maintains consistently low values (0.025 to 0.180). This stability may reflect either lower actual fraud or more consistent reporting. Conversely, regions like Ingushetia and Tatarstan show substantial fluctuations, with Ingushetia ranging from 0.234 to 0.847 and Tatarstan from 0.152 to 0.658, which might indicate varying levels of election integrity or differences in data reporting practices. Certain regions display upward trends over time. For example, Kaliningrad oblast shows a gradual increase in fraud prediction from 0.267 in 2012 to 0.447 in 2024. Similarly, Dagestan (Respublika Dagestan) exhibits a high value of 0.452 in 2016 but drops to 0.038 by 2024, suggesting either significant improvements or potential changes in fraud reporting or detection methods. These trends underscore the need for further investigation into the factors influencing regional variations.

In Figure B6, the geographic distribution of election fraud illustrates that neural network-based extrapolation can effectively project observation-like results across precincts. The model significantly expands the number of precincts identified with counting process violations compared to the data found in *Karta Narusheniy*. For example, while *Karta Narusheniy* reported 2,512 precincts with such violations, the machine learning-based extrapolation increased this number to 30,727. Similarly, in 2024, 574 precincts were documented for counting-related violations, but the ML algorithm expanded this figure to 16,431. This capability to extrapolate beyond observed data highlights the model's potential to fill gaps in observational coverage, particularly in regions where manual reporting is sparse or in-

Figure 3: Geographic Distribution of Observation-based Election 2012 and 2024, precinct-level



(a) (b)

(c) (d)

Notes: (a) Observed fraud from *Karta Narusheniy* for the 2012 election; (b) Predicted fraudulent precincts for the 2012 election (*SmallNN*, focal loss); (c) Observed fraud from *Karta Narusheniy* for the 2024 election; (d) Predicted fraudulent precincts for the 2024 election (*SmallNN*, focal loss)

complete. By leveraging neural networks, the model can infer likely instances of fraud in precincts that were not directly observed, thus providing a more comprehensive overview of electoral integrity.

Discussion

In this section, we will examine how to interpret discrepancies between forensic estimates and observer-based forensic estimates in the context of Type I and Type II errors. Both methods are differently susceptible to false positives and false negatives, which have varying implications for election fraud detection.

Beyond measurement errors, election forensics estimates are prone to Type I errors – false positives – due to the large volume of data and the inherent heterogeneity in electoral processes, which may stem from normal political variations. The vast amount of data can lead to the detection of patterns that appear suspicious but are actually non-fraudulent, such as legitimate regional variations in voter turnout. Additionally, significant differences in electoral practices across regions can create anomalies in the data that may be misinterpreted as fraud.

In contrast, observation-based election forensics estimates, which rely on human observers to detect fraud at polling stations and predict fraud occurrences using paired data, are susceptible to Type II errors—false negatives. Observers can only identify fraud that is visible within their monitoring scope, potentially missing fraudulent activities that occur outside their view, such as during result tabulation. Furthermore, election administrators might strategically relocate fraudulent activities to unobserved areas, further increasing the likelihood of Type II errors. Observer biases and limitations, along with the possibility that the presence of observers may deter visible fraud, can also contribute to the underreporting of actual fraudulent activities. In this context, *power* refers to the ability of observation-based methods to correctly identify actual cases of fraud (i.e., avoiding Type II errors). Given the limited scope and visibility of observers, while the power to detect visible fraud may be reasonable, the risk of false negatives (Type II errors) remains considerable.

Since both types of estimates contain inherent errors, neither can be considered definitive ground truth, which complicates our analysis. Consequently, this discussion emphasizes the discrepancies between the two types of estimates, each subject to different types of errors,

rather than focusing on biases that imply a ground truth. It is crucial to acknowledge that we are dealing not only with observation-based data but also with synthetic or predicted data derived from election forensics estimates. From a technical perspective, the synthetic generation of observational data has the potential to reduce Type I errors associated with election forensics methods. However, Type II errors related to our target variable cannot be entirely resolved within the machine learning framework.

When comparing the power of election forensics to observation-based methods, it is important to recognize that each method has its own strengths and weaknesses. Election forensics might have higher power in detecting fraud across a broad spectrum of data due to its comprehensive analysis, allowing for the detection of subtle and widespread irregularities. However, this comes at the cost of a higher risk of Type I errors, where fingerprints of normal politics might be misinterpreted as fraud. Conversely, observation-based methods, which rely on human observers to detect fraud at polling stations, might have lower overall power due to their limited scope and the potential for observers to miss fraudulent activities outside their view. This limitation increases the risk of Type II errors, where actual fraud may go undetected. Additionally, the strategic behavior of election administrators and observer biases can further impact the effectiveness of observation-based methods. Combining these approaches may offer a more balanced perspective, leveraging the broad analytical power of forensics with the on-the-ground insights of observation to reduce both Type I and Type II errors.

Thus the observed difference besides possible measurement errors can be explained by the presence of both types of errors in the estimates of interest. Table 6 presents an overview of Type I and Type II errors in election fraud detection, highlighting the discrepancies between election forensics and observation-based methods. When election forensics detects fraud, it is considered a correct detection (True Positive), but there is a risk of Type I errors, where non-fraudulent anomalies may be falsely identified as fraud. This risk is attributed to data heterogeneity and the vast volume of data analyzed, which can lead to overestimation of

fraud. Conversely, when election forensics does not detect fraud, it can result in Type II errors, where actual fraud is missed, potentially due to less obvious cases being overlooked. This scenario also includes correct rejections (True Negatives) and potential underestimation of fraud.

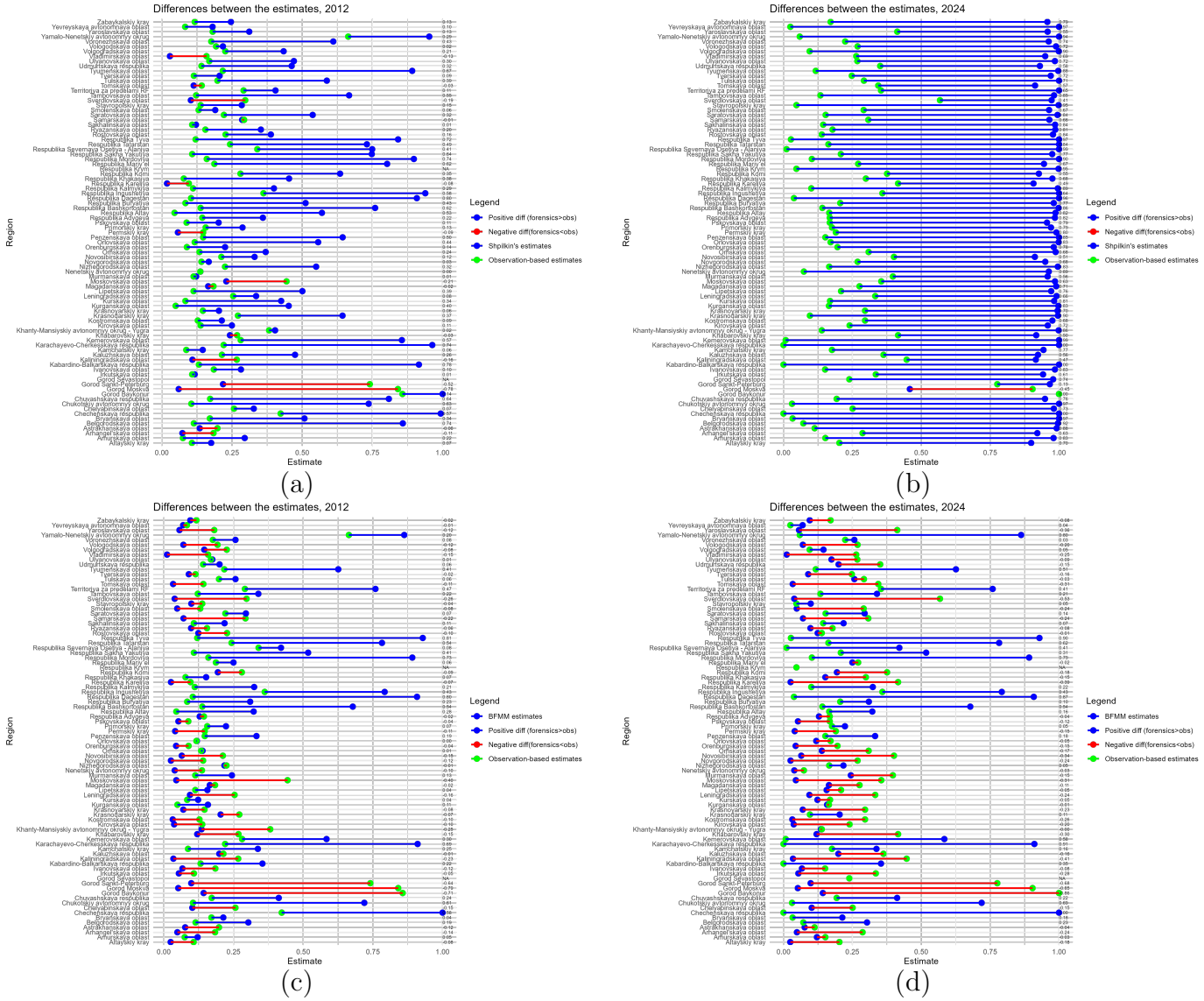
Table 6: Type I and Type II Errors in Election Fraud Detection with Methodological Discrepancies

Scenarios	**Election Fraud Present**	**No Election Fraud**
Election Forensics Detects Fraud	Correct Detection (True Positive)	False Positive (Type I Error): Possible overestimation of fraud due to data heterogeneity
Election Forensics Does Not Detect Fraud	False Negative (Type II Error): Potential underestimation of fraud in less obvious cases	Correct Rejection (True Negative)
Observers Detect Fraud	Correct Detection (True Positive)	False Positive (Type I Error): Possible overestimation of election fraud
Observers Do Not Detect Fraud	False Negative (Type II Error): Potential underestimation in unobserved precincts, where fraud is shifted	Correct Rejection (True Negative)

Discrepancies between forensic estimates and observer-based estimates can provide insights into potential errors in each method. When forensic estimates are higher than observer-based estimates, it may suggest a Type I error in the forensic analysis. This could occur if the forensic methods are identifying anomalies that are not truly indicative of fraud, possibly due to the high sensitivity of detection algorithms or the natural variability in the data. Alternatively, this discrepancy might indicate that the observers missed some instances of fraud (Type II error) because the fraudulent activities were either not visible to them or occurred in precincts not under observation.

Conversely, if election forensic estimates are lower than observer-based estimates, this might point to a Type II error in the forensic analysis. In this case, the forensic methods may have failed to detect fraud that was observed by human monitors, perhaps because the fraud was subtle, localized, or did not produce clear statistical signals. On the other hand, this discrepancy could also reflect a Type I error in the observer-based estimates if observers

Figure 4: Discrepancy Analysis



Notes: (a) *Shpilkin's* estimates vs. observation-based estimates for the 2012 elections; (b) *Shpilkin's* estimates vs. observation-based estimates for the 2024 elections; (c) *BFMM*'s estimates vs. observation-based estimates for the 2012 elections; (d) *BFMM*'s estimates vs. observation-based estimates for the 2024 elections.

reported fraud where none actually occurred. Understanding these discrepancies can help refine both methods and improve the overall accuracy of fraud detection in elections.

There are several limitations to the logic discussed. The accuracy of forensic methods and observer-based estimates can vary by electoral context, with methods effective in one system potentially failing in another. Observer bias and coverage also play a role, as reports may

be skewed based on observer training, biases, and the locations monitored. Additionally, nonrandom assignment of election observers will most certainly undermine the analysis and bias our estimates.

In Table 4 the discrepancy analysis for the years 2012 and 2024 reveals notable variations in election forensics accuracy across different methods. Using *Shpilkin's* method and *Bayesian Finite Mixture* model, we observe significant disparities in proportions of precincts affected by fraud among Russian regions. The mean discrepancy across the regions for *Shpilkin's* method was 0.23 (SD = 0.29) in 2012 and 0.74 (SD = 0.22) in 2024. For the *BFMM*, the mean discrepancy was 0.05 (SD = 0.29) in 2012 and 0.442 (SD = 0.36) in 2024

Specifically, for 2012, *Shpilkin's* method reveals a broad range of discrepancies, from positive values such as 0.74 in Belgorodskaya oblast to negative values, such as -0.78 in Moscow and -0.52 in St. Petersburg. The negative values suggest that observation-based fraud significantly exceeds election forensics fraud, likely due to the high concentration of monitoring efforts in Moscow. This concentration may have biased the neural network's analysis, leading it to inaccurately classify Moscow and St. Petersburg as having disproportionately high levels of observation-based fraud. For 2012, the *BFMM* generally exhibits a lower mean proportion of fraudulent precincts, resulting in a wider range of discrepancy scores, including more frequent negative biases where forensic scores are lower than observation-based scores. This presents a challenge for interpretation, as observation-based scores are expected to be lower due to Type II errors, while forensic scores might be inflated by Type I errors. However, it is also possible that *BFMM* is better equipped to manage Type I errors, thus providing a closer approximation to the true levels of fraud.

By 2024, the data indicates an overall increase in discrepancy levels compared to 2012 using *Shpilkin's* method. Most regions now exhibit higher positive biases, suggesting the detection of larger-scale anomalies by *Shpilkin's* method. In contrast, observation-based fraud levels have remained relatively stable, with mean values of 0.23 in 2012 and 0.20 in 2024. Since the *BFMM* model typically identifies smaller proportions of fraudulent precincts,

it results in more consistent negative or near-zero biases. One contributing factor is that the *BFMM* model has reached its reached its boundary for the 2024 election. The increases in the probability of *eforensics* fraud are not monotonic but are steady and substantial, eventually nearing the model's upper bounds, with $\pi_2 + \pi_3 = 0.615$ in 2024, just below the maximum possible total of 0.667. Comparatively, the more than doubled number of *eforensics*-fraudulent votes in 2024 compared to 2018 is primarily due to the significant rise in the proportion of polling stations exhibiting fraud, increasing from 0.29 to 0.67 of polling stations.

The significant differences between the two methods suggest that the choice of measurement technique can greatly influence the interpretation of forensic findings. This dichotomy underscores the need for a multi-faceted approach to measuring and analyzing regional biases. Advanced algorithms and models may offer more nuanced and accurate assessments, thereby reducing the likelihood of Type I and Type II errors. Ongoing research and development in measurement techniques are essential to adapt to changing regional contexts and enhance the precision of bias analysis.

Conclusion

This study offers a comprehensive evaluation of integrating machine learning techniques with traditional election forensics methods to enhance fraud detection across various elections. By focusing on Russian federal elections from 2012 to 2024, and utilizing data from the *Karta Narusheniy* website along with extensive electoral datasets, we investigated the efficacy of various neural network models and loss functions in predicting fraudulent precincts. The study employed various election forensics techniques, including digit tests and both parametric and non-parametric models.

The findings suggest that while neural networks exhibit strong generalization capabilities with well-tuned hyperparameters, the Cross-Entropy loss function consistently delivered

superior performance. Nonetheless, Focal Loss holds promise for better handling class imbalances and should be further refined to address the observed limitations. Future research should focus on optimizing loss functions and exploring a broader range of machine learning classifiers, including ensemble methods, to enhance fraud detection accuracy and robustness.

The analysis demonstrated significant variability in fraud detection across different regions and years, reflecting both the effectiveness of election monitoring and variations in regional political regimes. This variability highlights the complexity of electoral fraud detection and the necessity for models capable of adapting to diverse and evolving contexts. Furthermore, the discrepancies observed between forensic estimates and observer-based estimates can be attributed to false positives and false negatives, each impacting fraud detection differently. While the machine learning approach is effective in reducing false positives, false negatives related to the target variable *fraud* remain largely unresolved within the machine learning framework and require additional research.

In conclusion, this study highlights the potential of combining machine learning with election forensics to improve the precision and reliability of fraud detection. The results support continued development and refinement of both methodologies and models to advance the field of election forensics and ensure more accurate and fair electoral processes.

References

Beber, Bernd and Alexandra Scacco. 2008. "What the Numbers Say: A Digit-Based Test for Election Fraud Using New Data from Nigeria.".

Beber, Bernd and Alexandra Scacco. 2012. "What the Numbers Say: A Digit-Based Test for Election Fraud." *Political Analysis* 20(2):211–234.

Bjornlund, Eric C. 2004. *Beyond Free and Fair: Monitoring Elections and Building Democracy.* Woodrow Wilson Center Press.

Buzin, Andrei and Arkadiy Lubarev. 2008. *Crime without Punishment: administrative electoral technologies in Russian federal elections 2007-2008.* NIKKOLO M.

Cantu, Francisco and Sebastian M. Saiegh. 2011. "Fraudulent Democracy? An Analysis of Argentina's Infamous Decade Using Supervised Machine Learning." *Political Analysis* 19(4):409–433.

Chawla, N. V., K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer. 2002. "SMOTE: Synthetic Minority Over-sampling Technique." *Journal of Artificial Intelligence Research* 16:321357. **URL:** *http://dx.doi.org/10.1613/jair.953*

Deckert, Joseph, Mikhail Myagkov and Peter C. Ordeshook. 2011. "Benford's Law and the Detection of Election Fraud." *Political Analysis* 19(3):245–268.

Donsanto, Craig C. 2008. *Election Fraud: Detecting and Deterring Electoral Manipulation.* Washington, DC: Brookings Institution Press chapter Corruption of the Election Process under U.S. Federal Law, pp. 21–36.

Enikolopov, Ruben, Vasily Korovkin, Maria Petrova, Konstantin Sonin and Alexei Zakharov. 2013. "Field Experiment Estimate of Electoral Fraud in Russian Parliamentary Elections." *Proceedings of the National Academy of Sciences of the United States of America* 110(2):448–452.

Hicken, Allen and Walter R. Mebane, Jr. 2015. "A Guide to Election Forensics." Working paper for IIE/USAID subaward #DFG-10-APS-UM, "Development of an Election Forensics Toolkit: Using Subnational Data to Detect Anomalies".

Hyde, Susan D. 2007. "The Observer Effect in International Politics: Evidence from a Natural Experiment." *World Politics* 60:37–63.

Hyde, Susan D. 2011. *The Pseudo-Democrats Dilemma: Why Election Monitoring Became an International Norm*. Cornell University Press.

Ichino, Nahomi and Matthias Schundeln. 2012. "Deterring or Displacing Electoral Irregularities? Spillover Effects of Observers in a Randomized Field Experiment in Ghana." *The Journal of Politics* 74(1):292–307.

Kalinin, Kirill. 2019. "Validation of the Finite Mixture Model Using Quasi-Experimental Data and Geography. . 2019. No. 1. P. 6." (1):6.

Kalinin, Kirill. 2022*a*. "An Empirical Comparison of Parametric and Nonparametric Methods Applied to the Measurement of Election Fraud." (7).

Kalinin, Kirill. 2022*b*. "Signaling Games of Election Fraud: A Case of Russia." *Russian Politics* 7(2):210 – 236.
URL: *https://brill.com/view/journals/rupo/7/2/article-p210*$_3$*.xml*

Kalinin, Kirill. 2024. "Applying Machine Learning to Election Forensics Research: A Case of Russia.".

Kalinin, Kirill and Walter R. Mebane, Jr. 2013. "Understanding Electoral Frauds through Evolution of Russian Federalism: the Emergence of Signaling Loyalty." Paper prepared for the Annual Meeting of Midwest Political Science Association, Chicago.

Kalinin, Kirill and Walter R. Mebane, Jr. 2017. "Worst Election Ever in Russia?" Prepared

for presentation at the 2017 Annual Meeting of the Midwest Political Science Association, Chicago, IL.

Kalinin, Kirill and Walter R. Mebane, Jr. 2019. "EFToolkit: Election Forensics Toolkit.". **URL:** *https://github.com/kkalininMI/EFToolkit*

Kelley, Judith. 2012. *Monitoring Democracy: When International Election Observation Works and Why it Often Fails*. Princeton: Princeton University Press.

Klimek, Peter, Yuri Yegorov, Rudolf Hanel and Stefan Thurner. 2012. "Statistical Detection of Systematic Election Irregularities." *Proceedings of the National Academy of Sciences of the United States of America* 109(41):16469–16473.

Kobak, Dmitry, Sergey Shpilkin and Maxim S. Pshenichnikov. 2016. "Integer Percentages as Electoral Falsification Fingerprints." *The Annals of Applied Statistics* 10:54–73.

Lehoucq, Fabrice. 2003. "Electoral Fraud: Causes, Types, and Consequences." *Annual Review of Political Science* 6:233–256.

Lin, Tsung-Yi, Priya Goyal, Ross Girshick, Kaiming He and Piotr Doll 2018. "Focal Loss for Dense Object Detection.". **URL:** *https://arxiv.org/abs/1708.02002*

Mebane, Jr., Walter R. 2006. "Election Forensics: Vote Counts and Benfords Law." Paper prepared for the 2006 Summer Meeting of the Political Methodology Society, UC-Davis, July 20-22.

Mebane, Jr., Walter R. 2011. "Comment on "Benford's Law and the Detection of Election Fraud"." *Political Analysis* 19(3):269–272.

Mebane, Jr., Walter R. 2012. "Second-digit Tests for Voters Election Strategies and Election Fraud." Prepared for presentation at the 2012 Annual Meeting of the Midwest Political Science Association, Chicago, April 1215, 2010.

Mebane, Jr., Walter R. 2015. "Election Forensics: Latent Dimensions of Election Frauds and Strategic Voting." Paper presented at the 2015 Summer Meeting of the Political Methodology Society, Rochester, July 23–25.

Mebane, Jr., Walter R. 2016. "Election Forensics: Frauds Tests and Observation-level Frauds Probabilities." Prepared for presentation at the 2016 Annual Meeting of the Midwest Political Science Association, Chicago, IL, April 7–10.

Mebane, Jr., Walter R. and Joseph Klaver. 2015. "Election Forensics: Strategies versus Election Frauds in Germany." Prepared for presentation at the 2015 Annual Conference of the European Political Science Association, Vienna, Austria.

Mebane, Walter R. Jr., Diogo Ferrari, Kevin McAlister and Patrick Y. Wu. 2022. "Measuring Election Frauds.".

Myagkov, Mikhail, Peter C. Ordeshook and Dimitry Shaikin. 2009. *The Forensics of Election Fraud: With Applications to Russia and Ukraine*. New York: Cambridge University Press.

Pericchi, Luis Raul and David Torres. 2011. "Quick Anomaly Detection by the Newcomb-Benford Law, with Applications to Electoral Processes Data from the USA, Puerto Rico and Venezuela." *Statistical Science* 26(4):502–516.

Shpilkin, Sergei. 2011. "Statistika issledovala vybory: Statisticheskij analiz vyborov v Gosdumu 2011 goda pokazyvaet vozmozhnye fal'sifikacii (Statistics examined elections: Statistical analysis of elections to the State Duma in 2011 indicates possible fraud)." gazeta.ru (in Russian).
URL: *http://bit.ly/2q4Jdgc*

Simpser, Alberto. 2006. "A Theory of Corrupt Elections." Working paper.

Sjoberg, Fredrik M. 2012. "Making Vote Count: Evidence from Field Experiments about the Efficacy of Domestic Election Observation." Harriman Institute Working Paper No 1.

Sjoberg, Fredrik M. 2014. "Autocratic Adaptation: The Strategic Use of Transparency and the Persistence of Election Fraud." *Electoral Studies* 33:233–245.

Sobyanin, Alexander and Vladislav Sukhovolsky. 1995. *Demokratiya, ogranichennaya fal'sifikatsiyami: vybory i referendumy v Rossii v 1991-1993 gg.* Moscow: .

A Appendix. Technical Description

Code The replication code for the neural network binary classifiers used in this paper can be found in the GitHub repository:

https://github.com/kkalininMI/NeuralNets4ElectionForensics

Dataset The dataset used for training and evaluation consists of features and target labels. Features are represented as a matrix $\mathbf{X}$, where each row corresponds to a sample and each column corresponds to a feature. The target labels are represented as a vector $\mathbf{y}$, where each entry corresponds to the label of the corresponding sample.

Handling Imbalanced Data To address class imbalance, the following techniques are employed:

- **Oversampling**: The minority class is oversampled to balance the class distribution. This is achieved using techniques like SMOTE (Synthetic Minority Over-sampling Technique) or simple resampling.
- **Weighted Loss Function**: Weights are assigned to different samples or classes to address imbalances during model training.

Generating Region Weights Weights are computed based on fraud occurrences in different regions. The weights are inversely proportional to the fraud counts:

$$\text{weights}_i = \frac{1}{\text{fraud\_count}_i + \epsilon} \tag{5}$$

where ϵ is a small constant to avoid division by zero.

Standardization, Feature Scaling To improve convergence and performance, features are standardized:

$$\mathbf{X}_{\text{scaled}} = \frac{\mathbf{X} - \mu}{\sigma} \tag{6}$$

where μ and σ are the mean and standard deviation of the features, respectively.

Hyperparameters

Learning Rate The learning rate (lr) determines the step size during gradient descent. A typical range is 0.001 to 0.01; lr=0.005 is used in this paper.

Number of Epochs The number of epochs (num_epochs) defines how many times the entire dataset is processed. Common values range from 10 to 100; num_epochs = 50 in this paper.

Batch Size The batch size determines the number of samples processed before updating the model parameters. Typical values are 32 or 64; batch_size = 32 in this paper.

Loss Functions

Binary Cross-Entropy Loss Binary Cross-Entropy Loss is used for binary classification tasks and is defined as:

$$\text{BCE}(\mathbf{y}, \hat{\mathbf{y}}) = -\frac{1}{N} \sum_{i=1}^{N} [y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)] \tag{7}$$

where $\mathbf{y}$ is the vector of true labels, $\hat{\mathbf{y}}$ is the vector of predicted probabilities, and N is the number of samples.

Focal Loss Focal Loss is designed to address class imbalance by down-weighting easy examples and focusing on hard examples. It is defined as:

$$\text{FL}(\mathbf{y}, \hat{\mathbf{y}}) = \alpha(1 - \hat{y})^{\gamma}\text{BCE}(\mathbf{y}, \hat{\mathbf{y}}) \tag{8}$$

where α is a weighting factor, and γ is the focusing parameter. $\hat{y}$ is the predicted probability and BCE is the binary cross-entropy loss.

Weighted Loss Function Incorporating weights into the loss function adjusts the importance of each sample:

$$\text{Weighted Loss} = \sum_{i=1}^{N} w_i \cdot \text{FL}_i \tag{9}$$

where w_i is the weight for sample i, and Loss_i is the loss for sample i. Weighted Loss function is used in this paper.

Model Architecture

Small Neural Network The *SmallNN* class is defined with the following architecture:

- Input layer: 20 nodes
- Hidden layer 1: 30 nodes
- Output layer: 1 node with sigmoid activation

Average Neural Network The *AverageNN* class has the following architecture:

- Input layer: 20 nodes
- Hidden layer 1: 30 nodes
- Hidden layer 2: 50 nodes

- Output layer: 1 node with sigmoid activation

Large Neural Network The *LargeNN* class features a more complex architecture:

- Input layer: 20 nodes
- Hidden layers: 30, 50, 100, 100, 50, 50, 50, 10 nodes
- Output layer: 1 node with sigmoid activation

Training Procedure The training procedure involves:

- **Initialization**: Model, optimizer (Adam), and loss function are initialized.
- **Forward Pass**: Compute predictions and loss.
- **Backward Pass**: Compute gradients and update model parameters.
- **Evaluation**: Calculate average loss and F1 score for each epoch.

Plotting Losses Training and testing losses, as well as F1 scores, are plotted to visualize model performance over epochs.

The implementation of neural networks involves various stages from data preparation to model training. Understanding each component, including data handling, standardization, hyperparameters, and loss functions, is crucial for building effective models.

On Focal Loss

Formula 1: Simplified Form

$$\mathrm{FL}(\mathbf{y}, \hat{\mathbf{y}}) = \alpha(1-\hat{y})^{\gamma}\mathrm{BCE}(\mathbf{y}, \hat{\mathbf{y}})$$

Formula 2: Expanded Form

$$\mathrm{FL}(y, \hat{y}) = -\alpha \cdot (1-\hat{y})^{\gamma} \cdot y \cdot \log(\hat{y}) - (1-\alpha) \cdot \hat{y}^{\gamma} \cdot (1-y) \cdot \log(1-\hat{y})$$

Connection Between the Formulas 1. **Base Component (BCE Loss)**:

$$\mathrm{BCE}(y, \hat{y}) = -y \cdot \log(\hat{y}) - (1-y) \cdot \log(1-\hat{y})$$

The focal loss modifies the binary cross-entropy (BCE) loss by applying a scaling factor.

2. **Scaling Factor**: The focal loss formula introduces a scaling factor $\alpha(1-\hat{y})^{\gamma}$ for positive samples and $(1-\alpha) \cdot \hat{y}^{\gamma}$ for negative samples.

3. **Detailed Breakdown**:

- **Positive Samples** ($y = 1$):

  $$\mathrm{FL}(1, \hat{y}) = -\alpha \cdot (1-\hat{y})^{\gamma} \cdot \log(\hat{y})$$

  This represents the contribution for the positive class.

- **Negative Samples** ($y = 0$):

  $$\mathrm{FL}(0, \hat{y}) = -(1-\alpha) \cdot \hat{y}^{\gamma} \cdot \log(1-\hat{y})$$

  This represents the contribution for the negative class.

4. **Combining Terms**: Combining both terms gives:

$$\text{FL}(y, \hat{y}) = -\alpha \cdot (1 - \hat{y})^{\gamma} \cdot y \cdot \log(\hat{y}) - (1 - \alpha) \cdot \hat{y}^{\gamma} \cdot (1 - y) \cdot \log(1 - \hat{y})$$

5. **Simplified Expression**: The first formula is a more compact representation:

$$\text{FL}(\mathbf{y}, \hat{\mathbf{y}}) = \alpha(1 - \hat{y})^{\gamma}\text{BCE}(\mathbf{y}, \hat{\mathbf{y}})$$

In summary, both formulas express the same concept of focal loss: emphasizing hard-to-classify examples and reducing the relative loss for well-classified examples. The first formula is a compact form, while the second explicitly details the contributions from positive and negative samples.

On Focal Loss with Weighted Adjustment for Election Forensics

Focal loss is an adaptation of the standard binary cross-entropy loss that seeks to address the issue of class imbalance by down-weighting well-classified examples and focusing the loss on hard-to-classify instances. The introduction of weights to focal loss is particularly useful in election forensics, where the distribution of fraudulent activity across regions is uneven, necessitating a more nuanced approach to model training.

Why Weighted Loss by the Proportion of Observed Fraud? In election forensics, the distribution of fraudulent activity is not uniform across regions. Some regions may have a higher number of observed fraud cases, while others may have few or none. This disparity introduces the need for a weighted loss function to ensure that regions with fewer observed fraud cases are not overshadowed by those with higher counts.

The need for weighted loss arises from the necessity to prevent the model from being

biased towards regions with more data. The inclusion of weights allows us to proportionally adjust the contribution of each region to the loss function, ensuring that regions with fewer observed fraud cases are still adequately represented in the model's learning process.

The weighted focal loss can be mathematically expressed as follows:

$$\text{FL}(y, \hat{y})_w = \alpha \cdot (1 - \sigma(\text{inputs}))^\gamma \cdot [-y \log(\sigma(\text{inputs})) - (1 - y) \log(1 - \sigma(\text{inputs}))] \cdot \text{weights}$$

Where:

- $\sigma(\text{inputs})$ denotes the sigmoid function applied to the inputs to obtain p_t.
- α is a class weighting factor, which helps to balance the importance of positive and negative classes.
- γ is the focusing parameter, which modulates the degree of down-weighting for easy examples.
- weights are defined as:

$$\text{weights} = \frac{1.0}{\text{region\_fraud\_counts\_from\_el.observation} + 1 \times 10^{-2}}$$

Importance of Multiple Weights (α, γ, and weights) in Election Forensics In the context of election forensics, the three types of weights play critical roles in refining the model's sensitivity to the distribution of fraud across regions:

1. α**:** This weight compensates for the imbalance between the positive (fraudulent) and negative (non-fraudulent) classes, ensuring that the model does not become biased towards the majority class.
2. γ**:** The focusing parameter γ adjusts the focal loss such that the model emphasizes

learning from hard-to-classify examples. In election forensics, this is particularly useful for identifying subtle or less obvious cases of fraud that might otherwise be overlooked.

3. **weights:** The additional weights, based on the proportion of observed fraud in each region, ensure that regions with fewer observed cases of fraud still contribute meaningfully to the loss function. This adjustment is crucial for achieving a balanced model that performs well across all regions, not just those with abundant data.

Why Additional Oversampling is Necessary Despite the introduction of focal loss, without additional oversampling of the minority class (fraud cases), the model tends to classify nearly all instances as non-fraudulent. This occurs because the focal loss, while effective at emphasizing harder-to-classify examples, still relies on a sufficient number of positive examples (fraud cases) to adjust the model's decision boundary.

In highly imbalanced datasets, where fraud cases are significantly outnumbered, the model may fail to learn meaningful patterns related to fraud detection, resulting in a default prediction of the majority class (no fraud). Oversampling the minority class artificially increases the number of fraud cases in the training set, providing the model with more opportunities to learn the distinguishing features of fraud. This, in turn, enhances the effectiveness of focal loss, allowing the model to better differentiate between fraudulent and non-fraudulent instances.

By combining focal loss with oversampling, we can create a more robust model that not only accounts for class imbalance but also effectively extrapolates the detection of fraud to underrepresented precincts.

B Appendix. Electoral Violations from *Karta Narusheniy*

Table B1: Electoral Violations from *Karta Narusheniy*, 2012

	Counts
Administrative Resource	972
Influence of Law Enforcement	16
Pressure from Management on Voters	561
Complaints	839
Other Violations	703
Other Violations on Voting Day	1431
Use of Government Power to Create Advantages	395
Violation in Polling Station Setup	462
Violation of Candidate Rights	155
Violation of Rights of Observers, Commission Members, Media Representatives	953
Violation of Campaign Rules in the Media	102
Violation of Election Result Tabulation Rules, Result Distortion	**675**
Violation of Street and Outdoor Campaign Rules	121
Violations on Voting Day	5160
Violations During Election Campaign	1183
Violations in Absentee, At-Home, or Illegal Voting	**834**
Exclusion from Voter Lists, Denial of Voting Rights	478
Illegal Campaigning	123
Complaint Filed	728
Voter Bribery	102
Official Reaction Received	111
Voter Coercion, Violation of Voting Secrecy	204

Table B2: Electoral Violations from *Karta Narusheniy*, 2016

	Counts
Administrative Resource	1589
Influence of Law Enforcement	106
Pressure from Management on Voters	299
Other	157
Complaints	882
Other Violations	337
Other Violations on Voting Day	447
Use of Government Power to Create Advantages	1184
Crime	157
Violation in Polling Station Setup	158
Violation of Candidate Rights	324
Violation of Rights of Observers, Commission Members, Media Representatives	383
Violation of Rights of Observers, Commission Members, Media	99
Violation of Campaign Rules in the Media	388
Violation of Election Result Tabulation Rules, Result Distortion	**275**
Violation of Street and Outdoor Campaign Rules	531
Violations on Voting Day	2136
Violations During Election Campaign	1871
Violations in Absentee, At-Home, or Illegal Voting	**350**
Violations in Early Voting	4
Exclusion from Voter Lists, Denial of Voting Rights	130
Illegal Campaigning	197
Complaint Filed	729
Voter Bribery	188
Official Reaction Received	153
Voter Coercion, Violation of Voting Secrecy	196

Table B3: Electoral Violations from *Karta Narusheniy*, 2018

	Counts
Administrative Resource	1372
Influence of Law Enforcement	46
Pressure from Management on Voters	559
Other	47
Complaints	649
Other Violations	446
Other Violations on Voting Day	476
Use of Budgetary Resources	264
Use of Government Power to Create Advantages	503
Crime	47
Violation in Polling Station Setup	360
Violation of Candidate Rights	82
Violation of Rights of Observers, Commission Members, Media Representatives	472
Violation of Rights of Observers, Commission Members, Media	90
Violation of Campaign Rules in the Media	144
Violation of Election Result Tabulation Rules, Result Distortion	**445**
Violation of Street and Outdoor Campaign Rules	80
Violation in Signature Collection	44
Violations on Voting Day	2517
Violations During Election Campaign	945
Violations in Absentee, At-Home, or Illegal Voting	**335**
Violations in Early Voting	11
Exclusion from Voter Lists, Denial of Voting Rights	186
Illegal Campaigning	48
Complaint Filed	519
Voter Bribery	48
Official Reaction Received	130
Voter Coercion, Violation of Voting Secrecy	195

Table B4: Electoral Violations from *Karta Narusheniy*, 2020

	Counts
Campaigning in State and Municipal Media	130
Campaigning by Election Commissions, Authorities, Municipal Officials	395
Influence of Law Enforcement	37
Obstruction of Campaigning and Information	35
Pressure from Management on Voters	475
Complaints	1
Abuse of Administrative Resource	1
Other Violations on Voting Day	219
Other Violations Before Voting Day	282
Other Violations in Vote Counting and Finalization	57
Violation of Rights of Observers, Commission Members, Media Representatives: Restricted Movement, Ban on Photography, etc.	123
Violation of Rights of Commission Members, Observers, Media	177
Violation of the Right of Observers and Commission Members to Access Voter Lists and Acts	95
Violations in Vote Counting: Combining Stages, Failure to Announce and Record Data in the Enlarged Protocol Form, Lack of Voter List Count, Failure to Announce Post-Count Voter Data, etc.	**69**
Violations on the Day of National Voting	**763**
Violations Before Voting Day	2
Violations Before National Voting Day	1957
Violations Before Voting: Sealing Boxes, Storing Ballots, Failure to Announce Data, etc.	61
Violations of Early Voting Procedures	1
Violations in At-Home Voting	38
Violations in Voting: Ballot Stuffing, Voting for Others, Illegal Inclusion in Voter Lists, Bribery, etc.	**144**
Violations in Early At-Home Voting	143
Violations in Early Voting, Including Sealing and Storing Voting Documentation	112
Violations in Processing and Finalizing Results in Higher Commissions	11
Violations in National Voting Count	**215**
Violations Related to Mobile Voting	54
Violations Related to Electronic and Digital Voting	80
Covert Sorting of Ballots, Simultaneous Counting in Two Batches, Counting by Corners	26
Covert Protocol Compilation, Improper Document Packaging, Failure to Certify Protocol Copies, etc.	17
Non-Acceptance or Non-Consideration of Complaints	25
Complaint Filed	1
Voter Bribery	38
Voter Coercion, Transport or Violation of Voting Secrecy	58
Obvious Distortion of Results: Ballot Stuffing, Transferring from One Batch to Another, Rewriting Results, etc.	**35**

Table B5: Electoral Violations from *Karta Narusheniy*, 2021

	Counts
Ballot Stuffing, "Carousels", etc.	**286**
Influence of Law Enforcement	66
Pressure from Management, Coercion, Voter Bribery	212
Complaints	1842
Abuse of Administrative Resource	580
Other Violations on Voting Day	836
Other Violations Before Voting Day	357
Other Violations in Vote Counting and Finalization	**326**
Distortion of Voting Results During Counting	**206**
Violation in Voter List Management, Refusal to Vote	685
Violation of Rights of Commission Members, Observers, Media	132
Violation of Rules for Printed and Outdoor Campaigning	246
Violations on Voting Day	2101
Violations in Vote Counting, Result Finalization	**879**
Violations in At-Home Voting	194
Violations in Voter List Compilation, Disputes over Identity Verification	270
Complaint Filed	720
Violations of Early Voting Procedures	139
Voter Bribery	103
Obvious Distortion of Results: Ballot Stuffing, Rewriting Results, etc.	**139**
Use of Budgetary Resources	455
Use of Government Power to Create Advantages	472

Table B6: Electoral Violations from *Karta Narusheniy*, 2024

	Counts
Abuse of administrative resources	568
Violations before the start of voting: problems with safe packages, non-compliance with procedures, etc.	37
Violations of the sequence and procedure of counting	**117**
Complaint filed	218
Encroachment on life, health, property	31
Falsification of voting results during counting	**91**
Violations in polling station equipment	110
Unlawful refusals of registration and violation of candidate rights	3
Official response received	57
Violations of observer, commission member, media rights	249
Violations in protocol drafting, copy preparation	50
Ballot stuffing, "carousel voting", etc.	**47**
Violations in higher commissions	15
Violations of campaigning rules in media	179
Other violations during counting and result establishment	62
Violations of printed and outdoor campaigning rules	29
Violations in home voting	77
Pressure from superiors, coercion, voter bribery	238
Violations in voter list management, refusal to vote	118
Violations of early voting procedure	2
Coercion, transportation of voters, voting control	**144**
Violations of commission member, observer, media rights	33
Illegal campaigning, lotteries, bribery	156
Influence of law enforcement agencies	12
Other violations on voting day	222
Other violations before voting day	139
Violations during signature collection	155
Complaints	298
Violations on voting day	1194
Violations before voting day	1358
Violations during remote electronic voting	34
Violations during vote counting	**335**
Dissenting opinion	23
Encroachments on personal safety	31

C Appendix. Tables and Figures

Table C1: Proportion of Precincts with Observed Election Fraud Based on Data from the Election Violations Map (*Karta Narusheniy*)

Region	2012	2016	2018	2020	2021	2024
Altayskiy kray	0.005	0.000	0.008	0.007	0.014	0.003
Amurskaya oblast	0.003	0.000	0.001	0.000	0.001	0.001
Arhangel'skaya oblast	0.007	0.000	0.004	0.002	0.004	0.000
Astrakhanskaya oblast	0.034	0.000	0.003	0.003	0.007	0.000
Belgorodskaya oblast	0.009	0.000	0.006	0.001	0.002	0.001
Bryanskaya oblast	0.012	0.000	0.012	0.004	0.008	0.001
Chechenskaya respublika	0.048	0.000	0.029	0.000	0.000	0.000
Chelyabinskaya oblast	0.020	0.000	0.010	0.006	0.019	0.009
Chukotskiy avtonomnyy okrug	0.018	0.000	0.055	0.000	0.000	0.000
Chuvashskaya respublika	0.017	0.000	0.008	0.003	0.013	0.000
Gorod Baykonur	0.000	–	0.000	–	–	0.000
Gorod Moskva	0.113	0.000	0.069	0.076	0.140	0.057
Gorod Sankt-Peterburg	0.136	0.000	0.076	0.045	0.134	0.043
Gorod Sevastopol	–	0.000	0.000	0.000	0.000	0.000
Irkutskaya oblast	0.012	0.000	0.003	0.002	0.005	0.002
Ivanovskaya oblast	0.025	0.000	0.031	0.012	0.035	0.008
Kabardino-Balkarskaya respublika	0.048	0.000	0.017	0.003	0.003	0.003
Kaliningradskaya oblast	0.051	0.000	0.016	0.010	0.027	0.002
Kaluzhskaya oblast	0.008	0.000	0.019	0.001	0.014	0.000
Kamchatskiy kray	0.003	0.000	0.120	0.000	0.010	0.000
Karachayevo-Cherkesskaya respublika	0.008	0.000	0.116	0.000	0.000	0.000
Kemerovskaya oblast	0.015	1.000	0.023	0.006	0.030	0.002
Khabarovskiy kray	0.016	0.000	0.016	0.001	0.010	0.000
Khanty-Mansiyskiy avtonomnyy okrug - Yugra	0.006	0.000	0.007	0.001	0.028	0.003
Kirovskaya oblast	0.017	0.000	0.009	0.007	0.043	0.008
Kostromskaya oblast	0.035	0.000	0.010	0.005	0.022	0.000
Krasnodarskiy kray	0.043	0.000	0.035	0.010	0.048	0.014
Krasnoyarskiy kray	0.005	0.000	0.010	0.004	0.011	0.000
Kurganskaya oblast	0.004	0.000	0.005	0.008	0.003	0.000
Kurskaya oblast	0.003	0.000	0.003	0.002	0.004	0.001
Leningradskaya oblast	0.043	0.000	0.022	0.003	0.028	0.008
Lipetskaya oblast	0.013	0.000	0.000	0.000	0.008	0.001
Magadanskaya oblast	0.010	0.000	0.019	0.000	0.019	0.000
Moskovskaya oblast	0.076	0.000	0.031	0.015	0.079	0.024
Murmanskaya oblast	0.014	0.000	0.008	0.002	0.005	0.000
Nenetskiy avtonomnyy okrug	0.039	0.000	0.000	0.018	0.000	0.000
Nizhegorodskaya oblast	0.028	0.000	0.009	0.004	0.023	0.008
Novgorodskaya oblast	0.002	0.000	0.009	0.006	0.006	0.010

Table C1: (Continued)

Region	2012	2016	2018	2020	2021	2024
Novosibirskaya oblast	0.009	0.000	0.007	0.003	0.010	0.002
Omskaya oblast	0.016	0.000	0.003	0.003	0.005	0.000
Orenburgskaya oblast	0.027	0.000	0.001	0.003	0.005	0.003
Orlovskaya oblast	0.015	0.000	0.026	0.000	0.043	0.001
Penzenskaya oblast	0.007	0.000	0.003	0.002	0.005	0.000
Permskiy kray	0.006	0.000	0.007	0.007	0.013	0.003
Primorskiy kray	0.015	0.000	0.004	0.002	0.016	0.000
Pskovskaya oblast	0.006	0.000	0.006	0.002	0.008	0.000
Respublika Adygeya	0.049	0.000	0.045	0.000	0.008	0.000
Respublika Altay	0.008	0.000	0.000	0.000	0.000	0.000
Respublika Bashkortostan	0.018	0.000	0.015	0.001	0.016	0.004
Respublika Buryatiya	0.005	0.000	0.001	0.001	0.006	0.000
Respublika Dagestan	0.019	0.000	0.019	0.001	0.002	0.000
Respublika Ingushetiya	0.023	0.000	0.000	0.000	0.000	0.000
Respublika Kalmykiya	0.079	0.000	0.008	0.000	0.009	0.000
Respublika Kareliya	0.029	0.000	0.011	0.000	0.015	0.000
Respublika Khakasiya	0.003	0.000	0.003	0.000	0.000	0.000
Respublika Komi	0.017	0.000	0.003	0.009	0.009	0.002
Respublika Krym	–	0.000	0.000	0.000	0.000	0.000
Respublika Mariy El	0.016	0.000	0.011	0.000	0.006	0.004
Respublika Mordoviya	0.012	0.000	0.008	0.000	0.003	0.003
Respublika Sakha Yakutiya	0.011	0.000	0.005	0.001	0.001	0.001
Respublika Severnaya Osetiya - Alaniya	0.027	0.000	0.014	0.003	0.003	0.000
Respublika Tatarstan	0.021	0.000	0.027	0.004	0.017	0.005
Respublika Tyva	0.011	0.000	0.011	0.000	0.000	0.000
Rostovskaya oblast	0.021	0.000	0.007	0.001	0.005	0.000
Ryazanskaya oblast	0.037	0.000	0.034	0.017	0.037	0.002
Sakhalinskaya oblast	0.007	0.000	0.008	0.000	0.002	0.002
Samarskaya oblast	0.082	0.000	0.017	0.006	0.039	0.014
Saratovskaya oblast	0.049	0.000	0.019	0.003	0.015	0.002
Smolenskaya oblast	0.006	0.000	0.005	0.006	0.008	0.001
Stavropolskiy kray	0.044	0.000	0.039	0.000	0.044	0.001
Sverdlovskaya oblast	0.017	0.000	0.006	0.008	0.018	0.003
Tambovskaya oblast	0.015	0.000	0.010	0.015	0.038	0.000
Territoriya za predelami RF	0.013	–	0.044	–	–	0.059
Tomskaya oblast	0.012	0.000	0.019	0.013	0.009	0.004
Tulskaya oblast	0.021	0.000	0.011	0.010	0.000	0.004
Tverskaya oblast	0.009	0.000	0.008	0.001	0.013	0.001
Tyumenskaya oblast	0.009	0.000	0.045	0.004	0.006	0.001
Udmurtskaya respublika	0.003	0.000	0.003	0.000	0.005	0.004
Ulyanovskaya oblast	0.008	0.000	0.002	0.002	0.005	0.002

Table C1: (Continued)

Region	2012	2016	2018	2020	2021	2024
Vladimirskaya oblast	0.015	0.000	0.012	0.005	0.012	0.002
Volgogradskaya oblast	0.021	0.000	0.010	0.001	0.023	0.006
Vologodskaya oblast	0.013	0.000	0.005	0.006	0.016	0.001
Voronezhskaya oblast	0.016	0.000	0.008	0.004	0.005	0.002
Yamalo-Nenetskiy avtonomnyy okrug	0.019	0.000	0.009	0.004	0.052	0.000
Yaroslavskaya oblast	0.010	0.000	0.006	0.005	0.002	0.000
Yevreyskaya avtonomnaya oblast	0.000	0.000	0.005	0.000	0.000	0.000
Zabaykalskiy kray	0.003	0.000	0.002	0.000	0.004	0.001

Table C2: Predicted Proportions of Fraudulent Precincts Based on Observation Data for the *NNSmall* Model Using Cross-Entropy Loss, by Region and Year

Region	2012	2016	2018	2020	2021	2024
Altayskiy kray	0.127	0.001	0.161	0.285	0.148	0.131
Amurskaya oblast	0.109	0.016	0.104	0.245	0.051	0.101
Arhangel'skaya oblast	0.230	0.004	0.282	0.348	0.378	0.098
Astrakhanskaya oblast	0.319	0.005	0.245	0.383	0.294	0.101
Belgorodskaya oblast	0.173	0.149	0.216	0.257	0.082	0.061
Bryanskaya oblast	0.116	0.055	0.198	0.109	0.149	0.051
Chechenskaya respublika	0.515	0.019	0.419	0.085	0.002	0.019
Chelyabinskaya oblast	0.404	0.013	0.379	0.401	0.290	0.161
Chukotskiy avtonomnyy okrug	0.158	0.145	0.164	0.145	0.066	0.016
Chuvashskaya respublika	0.236	0.073	0.173	0.218	0.159	0.082
Gorod Baykonur	1.000	–	0.571	–	–	0.714
Gorod Moskva	0.934	0.003	0.936	0.868	0.928	0.869
Gorod Sankt-Peterburg	0.912	0.001	0.892	0.826	0.934	0.647
Gorod Sevastopol	–	0.000	0.319	0.642	0.522	0.181
Irkutskaya oblast	0.167	0.004	0.181	0.364	0.142	0.194
Ivanovskaya oblast	0.360	0.011	0.282	0.387	0.311	0.117
Kabardino-Balkarskaya respublika	0.247	0.028	0.444	0.513	0.006	0.039
Kaliningradskaya oblast	0.441	0.007	0.510	0.484	0.469	0.313
Kaluzhskaya oblast	0.311	0.018	0.313	0.389	0.280	0.197
Kamchatskiy kray	0.111	0.083	0.170	0.357	0.056	0.056
Karachayevo-Cherkesskaya respublika	0.293	0.000	0.414	0.308	0.016	0.040
Kemerovskaya oblast	0.250	0.969	0.355	0.184	0.193	0.034
Khabarovskiy kray	0.239	0.013	0.299	0.491	0.269	0.195
Khanty-Mansiyskiy avtonomnyy okrug - Yugra	0.492	0.028	0.386	0.679	0.389	0.151
Kirovskaya oblast	0.204	0.005	0.211	0.269	0.173	0.120
Kostromskaya oblast	0.173	0.002	0.210	0.319	0.156	0.132
Krasnodarskiy kray	0.332	0.045	0.413	0.296	0.342	0.130
Krasnoyarskiy kray	0.204	0.009	0.226	0.329	0.304	0.157
Kurganskaya oblast	0.100	0.007	0.100	0.184	0.061	0.097
Kurskaya oblast	0.125	0.003	0.132	0.220	0.078	0.081
Leningradskaya oblast	0.496	0.004	0.508	0.430	0.484	0.251
Lipetskaya oblast	0.198	0.059	0.235	0.285	0.104	0.117
Magadanskaya oblast	0.146	0.037	0.221	0.402	0.189	0.153
Moskovskaya oblast	0.687	0.002	0.629	0.510	0.652	0.287
Murmanskaya oblast	0.305	0.010	0.403	0.404	0.184	0.181
Nenetskiy avtonomnyy okrug	0.176	0.000	0.059	0.436	0.073	0.037
Nizhegorodskaya oblast	0.299	0.046	0.347	0.348	0.251	0.119
Novgorodskaya oblast	0.191	0.002	0.256	0.247	0.287	0.159
Novosibirskaya oblast	0.270	0.006	0.286	0.408	0.276	0.311
Omskaya oblast	0.180	0.013	0.187	0.334	0.123	0.177

Table C2: (Continued)

Region	2012	2016	2018	2020	2021	2024
Orenburgskaya oblast	0.114	0.011	0.176	0.280	0.122	0.127
Orlovskaya oblast	0.085	0.024	0.212	0.235	0.186	0.127
Penzenskaya oblast	0.158	0.119	0.232	0.270	0.197	0.100
Permskiy kray	0.357	0.002	0.368	0.346	0.312	0.147
Primorskiy kray	0.248	0.021	0.226	0.336	0.215	0.118
Pskovskaya oblast	0.151	0.006	0.279	0.216	0.391	0.101
Respublika Adygeya	0.208	0.114	0.352	0.292	0.218	0.123
Respublika Altay	0.083	0.004	0.054	0.186	0.089	0.102
Respublika Bashkortostan	0.189	0.116	0.247	0.122	0.163	0.089
Respublika Buryatiya	0.200	0.005	0.185	0.245	0.101	0.124
Respublika Dagestan	0.236	0.145	0.215	0.097	0.066	0.063
Respublika Ingushetiya	0.385	0.044	0.774	0.489	0.270	0.282
Respublika Kalmykiya	0.233	0.120	0.199	0.180	0.115	0.106
Respublika Kareliya	0.269	0.000	0.411	0.307	0.573	0.190
Respublika Khakasiya	0.190	0.008	0.171	0.344	0.115	0.168
Respublika Komi	0.382	0.006	0.312	0.406	0.111	0.143
Respublika Krym	–	0.027	0.204	0.281	0.464	0.076
Respublika Mariy El	0.332	0.004	0.200	0.280	0.035	0.146
Respublika Mordoviya	0.107	0.438	0.159	0.184	0.140	0.070
Respublika Sakha Yakutiya	0.183	0.012	0.166	0.291	0.078	0.158
Respublika Severnaya Osetiya - Alaniya	0.213	0.045	0.365	0.482	0.101	0.051
Respublika Tatarstan	0.246	0.390	0.341	0.285	0.139	0.117
Respublika Tyva	0.104	0.115	0.246	0.115	0.075	0.021
Rostovskaya oblast	0.317	0.042	0.319	0.296	0.287	0.103
Ryazanskaya oblast	0.183	0.010	0.189	0.252	0.214	0.087
Sakhalinskaya oblast	0.187	0.047	0.164	0.286	0.136	0.099
Samarskaya oblast	0.342	0.075	0.467	0.472	0.404	0.220
Saratovskaya oblast	0.283	0.125	0.244	0.285	0.261	0.100
Smolenskaya oblast	0.165	0.020	0.208	0.310	0.156	0.191
Stavropolskiy kray	0.278	0.016	0.389	0.389	0.285	0.097
Sverdlovskaya oblast	0.487	0.002	0.408	0.492	0.380	0.369
Tambovskaya oblast	0.152	0.042	0.198	0.210	0.194	0.096
Territoriya za predelami RF	0.127	–	0.227	–	–	0.392
Tomskaya oblast	0.263	0.001	0.317	0.338	0.283	0.277
Tulskaya oblast	0.274	0.011	0.313	0.340	0.308	0.188
Tverskaya oblast	0.226	0.019	0.212	0.247	0.161	0.167
Tyumenskaya oblast	0.253	0.417	0.251	0.324	0.236	0.159
Udmurtskaya respublika	0.266	0.015	0.242	0.312	0.133	0.167
Ulyanovskaya oblast	0.241	0.088	0.213	0.338	0.109	0.131
Vladimirskaya oblast	0.245	0.001	0.297	0.372	0.274	0.137
Volgogradskaya oblast	0.269	0.009	0.279	0.345	0.258	0.097

Table C2: (Continued)

Region	2012	2016	2018	2020	2021	2024
Vologodskaya oblast	0.241	0.003	0.269	0.287	0.191	0.155
Voronezhskaya oblast	0.255	0.148	0.252	0.308	0.208	0.144
Yamalo-Nenetskiy avtonomnyy okrug	0.265	0.053	0.509	0.498	0.443	0.054
Yaroslavskaya oblast	0.342	0.001	0.483	0.415	0.313	0.207
Yevreyskaya avtonomnaya oblast	0.139	0.006	0.060	0.142	0.065	0.037
Zabaykalskiy kray	0.115	0.007	0.108	0.240	0.063	0.088

Table C3: Predicted Proportions of Fraudulent Precincts Based on Observation Data for the *NNSmall* Model Using Focal Loss, by Region and Year

Region	2012	2016	2018	2020	2021	2024
Altayskiy kray	0.107	0.003	0.307	0.380	0.161	0.203
Amurskaya oblast	0.075	0.030	0.238	0.308	0.092	0.152
Arhangel'skaya oblast	0.184	0.017	0.345	0.414	0.331	0.287
Astrakhanskaya oblast	0.198	0.010	0.423	0.406	0.313	0.113
Belgorodskaya oblast	0.114	0.253	0.344	0.339	0.116	0.072
Bryanskaya oblast	0.171	0.096	0.298	0.243	0.158	0.033
Chechenskaya respublika	0.423	0.175	0.688	0.067	0.037	0.000
Chelyabinskaya oblast	0.257	0.020	0.472	0.513	0.287	0.251
Chukotskiy avtonomnyy okrug	0.105	0.109	0.236	0.164	0.066	0.031
Chuvashskaya respublika	0.172	0.102	0.252	0.273	0.134	0.193
Gorod Baykonur	0.857	–	1.000	–	–	1.000
Gorod Moskva	0.841	0.007	0.944	0.904	0.881	0.904
Gorod Sankt-Peterburg	0.741	0.002	0.913	0.897	0.930	0.776
Gorod Sevastopol	–	0.010	0.747	0.749	0.500	0.239
Irkutskaya oblast	0.108	0.005	0.285	0.389	0.209	0.335
Ivanovskaya oblast	0.185	0.015	0.379	0.427	0.200	0.151
Kabardino-Balkarskaya respublika	0.132	0.121	0.669	0.617	0.039	0.000
Kaliningradskaya oblast	0.267	0.019	0.570	0.578	0.489	0.447
Kaluzhskaya oblast	0.214	0.036	0.423	0.458	0.299	0.363
Kamchatskiy kray	0.087	0.150	0.293	0.364	0.175	0.176
Karachayevo-Cherkesskaya respublika	0.220	0.032	0.474	0.452	0.047	0.000
Kemerovskaya oblast	0.281	0.982	0.455	0.317	0.232	0.008
Khabarovskiy kray	0.268	0.023	0.448	0.497	0.389	0.416
Khanty-Mansiyskiy avtonomnyy okrug - Yugra	0.382	0.054	0.755	0.768	0.462	0.139
Kirovskaya oblast	0.138	0.017	0.284	0.343	0.136	0.240
Kostromskaya oblast	0.128	0.000	0.280	0.371	0.199	0.296
Krasnodarskiy kray	0.271	0.106	0.606	0.373	0.366	0.096
Krasnoyarskiy kray	0.146	0.026	0.341	0.386	0.282	0.296
Kurganskaya oblast	0.049	0.010	0.159	0.242	0.093	0.165
Kurskaya oblast	0.084	0.031	0.212	0.279	0.099	0.169
Leningradskaya oblast	0.254	0.020	0.579	0.544	0.458	0.333
Lipetskaya oblast	0.113	0.107	0.346	0.339	0.205	0.209
Magadanskaya oblast	0.184	0.065	0.356	0.412	0.217	0.276
Moskovskaya oblast	0.444	0.006	0.702	0.625	0.498	0.355
Murmanskaya oblast	0.113	0.040	0.498	0.489	0.180	0.397
Nenetskiy avtonomnyy okrug	0.137	0.000	0.216	0.400	0.018	0.074
Nizhegorodskaya oblast	0.225	0.091	0.447	0.395	0.234	0.166
Novgorodskaya oblast	0.141	0.002	0.305	0.328	0.233	0.269
Novosibirskaya oblast	0.212	0.015	0.381	0.451	0.320	0.401
Omskaya oblast	0.134	0.021	0.272	0.367	0.179	0.309

Table C3: (Continued)

Region	2012	2016	2018	2020	2021	2024
Orenburgskaya oblast	0.089	0.024	0.281	0.344	0.122	0.196
Orlovskaya oblast	0.117	0.062	0.301	0.293	0.206	0.171
Penzenskaya oblast	0.147	0.250	0.321	0.300	0.171	0.152
Permskiy kray	0.147	0.004	0.433	0.450	0.307	0.190
Primorskiy kray	0.156	0.045	0.334	0.385	0.195	0.176
Pskovskaya oblast	0.088	0.006	0.301	0.281	0.304	0.168
Respublika Adygeya	0.144	0.202	0.485	0.462	0.256	0.168
Respublika Altay	0.045	0.004	0.145	0.203	0.123	0.166
Respublika Bashkortostan	0.138	0.236	0.317	0.206	0.107	0.141
Respublika Buryatiya	0.084	0.010	0.238	0.296	0.110	0.206
Respublika Dagestan	0.104	0.452	0.294	0.148	0.098	0.038
Respublika Ingushetiya	0.362	0.140	0.847	0.693	0.234	0.359
Respublika Kalmykiya	0.111	0.227	0.223	0.230	0.128	0.101
Respublika Kareliya	0.096	0.011	0.474	0.461	0.474	0.416
Respublika Khakasiya	0.078	0.018	0.345	0.443	0.196	0.299
Respublika Komi	0.280	0.004	0.411	0.443	0.218	0.376
Respublika Krym	–	0.076	0.510	0.405	0.368	0.047
Respublika Mariy el	0.187	0.013	0.313	0.354	0.144	0.271
Respublika Mordoviya	0.160	0.696	0.236	0.208	0.113	0.103
Respublika Sakha Yakutiya	0.108	0.025	0.256	0.293	0.125	0.208
Respublika Severnaya Osetiya - Alaniya	0.340	0.111	0.624	0.584	0.296	0.011
Respublika Tatarstan	0.243	0.658	0.387	0.340	0.152	0.163
Respublika tyva	0.120	0.355	0.333	0.137	0.118	0.027
Rostovskaya oblast	0.227	0.089	0.412	0.434	0.276	0.139
Ryazanskaya oblast	0.155	0.029	0.257	0.288	0.190	0.178
Sakhalinskaya oblast	0.108	0.112	0.299	0.331	0.201	0.144
Samarskaya oblast	0.293	0.141	0.568	0.517	0.400	0.308
Saratovskaya oblast	0.221	0.231	0.316	0.333	0.197	0.153
Smolenskaya oblast	0.131	0.033	0.333	0.367	0.207	0.291
Stavropolskiy kray	0.138	0.024	0.565	0.512	0.306	0.047
Sverdlovskaya oblast	0.297	0.005	0.542	0.595	0.405	0.568
Tambovskaya oblast	0.122	0.086	0.265	0.204	0.324	0.134
Territoriya za predelami RF	0.291	–	0.543	–	–	0.354
Tomskaya oblast	0.142	0.001	0.356	0.381	0.290	0.344
Tulskaya oblast	0.198	0.034	0.377	0.382	0.260	0.292
Tverskaya oblast	0.114	0.029	0.275	0.337	0.219	0.248
Tyumenskaya oblast	0.217	0.535	0.353	0.349	0.256	0.117
Udmurtskaya respublika	0.141	0.023	0.363	0.408	0.177	0.351
Ulyanovskaya oblast	0.169	0.152	0.334	0.391	0.206	0.268
Vladimirskaya oblast	0.159	0.003	0.433	0.447	0.287	0.264
Volgogradskaya oblast	0.226	0.021	0.375	0.431	0.277	0.095

Table C3: (Continued)

Region	2012	2016	2018	2020	2021	2024
Vologodskaya oblast	0.193	0.003	0.323	0.358	0.198	0.269
Voronezhskaya oblast	0.176	0.240	0.347	0.361	0.279	0.224
Yamalo-Nenetskiy avtonomnyy okrug	0.664	0.075	0.759	0.614	0.283	0.059
Yaroslavskaya oblast	0.181	0.002	0.541	0.529	0.317	0.413
Yevreyskaya avtonomnaya oblast	0.083	0.012	0.152	0.180	0.076	0.025
Zabaykalskiy kray	0.117	0.018	0.188	0.281	0.134	0.171

Table C4: Proportion of Predicted Precincts with Election Forensics Estimates, by Region and Year

Region	2012				2016				2018				2020				2021				2024			
	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm
Altayskiy kray	0.18	0.33	0.11	0.02	0.28	0.41	0.04	0.02	0.37	0.20	0.16	0.05	0.41	0.14	0.50	0.25	0.29	0.48	0.08	0.02	0.90	1.00	0.83	0.30
Amurskaya oblast	0.30	0.42	0.24	0.12	0.34	0.45	0.11	0.03	0.29	0.18	0.20	0.09	0.60	0.23	0.62	0.36	0.29	0.48	0.12	0.04	0.98	1.00	0.97	0.65
Arhangel'skaya oblast	0.07	0.41	0.18	0.05	0.15	0.49	0.07	0.04	0.07	0.17	0.16	0.08	0.21	0.05	0.20	0.18	0.25	0.43	0.04	0.03	0.92	1.00	0.78	0.24
Astrakhanskaya oblast	0.13	0.58	0.32	0.08	0.19	0.66	0.15	0.07	0.23	0.23	0.25	0.18	0.78	0.64	0.79	0.61	0.38	0.71	0.23	0.09	0.99	1.00	0.99	0.79
Belgorodskaya oblast	0.86	0.75	0.51	0.30	0.81	0.79	0.55	0.37	0.67	0.59	0.48	0.48	0.90	0.82	0.91	0.74	0.83	0.81	0.50	0.31	1.00	1.00	0.99	0.88
Bryanskaya oblast	0.51	0.50	0.29	0.21	0.68	0.75	0.45	0.32	0.87	0.82	0.70	0.65	0.98	0.98	0.98	0.92	0.89	0.91	0.75	0.44	1.00	1.00	1.00	0.93
Chechenskaya respublika	0.99	1.00	0.99	1.00	0.97	1.00	0.97	1.00	0.91	0.96	0.91	0.90	0.98	1.00	0.99	1.00	0.97	1.00	0.98	0.98	1.00	1.00	1.00	1.00
Chelyabinskaya oblast	0.33	0.49	0.15	0.10	0.48	0.49	0.08	0.03	0.40	0.23	0.14	0.11	0.71	0.41	0.72	0.42	0.51	0.62	0.16	0.04	0.98	1.00	0.96	0.70
Chukotskiy ao	0.74	0.98	0.61	0.72	0.67	0.80	0.55	0.56	0.76	0.95	0.56	0.84	0.62	0.73	0.60	0.75	0.59	0.72	0.38	0.31	1.00	1.00	1.00	0.95
Chuvashskaya respublika	0.81	0.81	0.56	0.41	0.87	0.82	0.59	0.30	0.77	0.76	0.61	0.62	0.68	0.63	0.69	0.63	0.83	0.80	0.48	0.13	0.95	1.00	0.90	0.63
Gorod Baykonur	1.00	1.00	0.14	0.14	–	–	–	–	0.43	0.43	0.00	0.00	–	–	–	–	–	–	–	–	1.00	1.00	0.71	0.29
Gorod Moskva	0.06	0.86	0.18	0.05	0.10	0.95	0.06	0.03	0.07	0.29	0.09	0.05	0.23	0.14	0.34	0.13	0.07	0.94	0.08	0.02	0.46	1.00	0.56	0.08
Gorod Sankt-Peterburg	0.22	0.81	0.18	0.10	0.06	0.95	0.13	0.04	0.28	0.31	0.10	0.10	0.85	0.74	0.86	0.54	0.18	0.94	0.06	0.03	0.97	1.00	0.94	0.54
Gorod Sevastopol	–	–	–	–	0.70	0.74	0.06	0.05	0.85	0.76	0.14	0.95	0.70	0.47	0.66	0.50	0.42	0.81	0.12	0.04	0.98	1.00	0.97	0.85
Irkutskaya oblast	0.12	0.41	0.25	0.05	0.14	0.55	0.14	0.04	0.06	0.10	0.23	0.06	0.24	0.06	0.33	0.18	0.15	0.52	0.08	0.03	0.94	1.00	0.86	0.43
Ivanovskaya oblast	0.28	0.52	0.22	0.07	0.28	0.67	0.19	0.05	0.19	0.11	0.21	0.04	0.71	0.38	0.75	0.44	0.20	0.61	0.07	0.01	0.99	1.00	0.98	0.78
Kabardino-balkarskaya resp.	0.92	0.81	0.42	0.35	0.97	1.00	0.96	0.73	0.99	0.99	0.99	0.99	0.99	0.89	1.00	0.76	1.00	1.00	1.00	0.57	1.00	1.00	1.00	1.00
Kaliningradskaya oblast	0.11	0.50	0.16	0.03	0.43	0.61	0.07	0.05	0.22	0.29	0.16	0.13	0.51	0.32	0.57	0.34	0.45	0.63	0.10	0.05	0.92	1.00	0.90	0.56
Kaluzhskaya oblast	0.47	0.63	0.29	0.20	0.50	0.72	0.25	0.10	0.58	0.45	0.31	0.25	0.64	0.47	0.66	0.45	0.47	0.73	0.25	0.05	0.92	1.00	0.91	0.54
Kamchatskiy kray	0.15	0.69	0.11	0.34	0.24	0.73	0.15	0.27	0.26	0.53	0.16	0.36	0.21	0.44	0.31	0.37	0.21	0.72	0.14	0.28	0.94	1.00	0.93	0.65
Karachayevo-Cherkesskaya resp.	0.96	0.99	0.95	0.91	0.98	1.00	0.97	0.86	0.90	0.90	0.86	0.84	0.99	0.98	0.99	0.84	0.97	1.00	0.97	0.73	1.00	1.00	1.00	0.99
Kemerovskaya oblast	0.86	0.91	0.70	0.58	0.91	0.99	0.90	0.74	0.85	0.89	0.78	0.79	0.98	0.98	0.98	0.88	0.93	0.97	0.86	0.49	1.00	1.00	1.00	0.99
Khabarovskiy kray	0.24	0.54	0.19	0.12	0.20	0.67	0.14	0.06	0.25	0.23	0.14	0.09	0.16	0.10	0.28	0.14	0.36	0.56	0.07	0.02	0.92	1.00	0.86	0.43
Khanty-Mansiyskiy ao	0.40	0.77	0.26	0.14	0.32	0.81	0.18	0.07	0.57	0.40	0.22	0.14	0.54	0.31	0.54	0.28	0.42	0.79	0.15	0.04	1.00	1.00	1.00	0.87
Kirovskaya oblast	0.25	0.31	0.12	0.04	0.35	0.38	0.05	0.01	0.32	0.23	0.19	0.07	0.57	0.17	0.60	0.37	0.44	0.46	0.08	0.01	0.96	1.00	0.90	0.49
Kostromskaya oblast	0.21	0.30	0.09	0.03	0.20	0.33	0.03	0.00	0.07	0.06	0.07	0.01	0.52	0.06	0.56	0.27	0.20	0.39	0.02	0.00	0.98	1.00	0.94	0.50
Krasnodarskiy kray	0.64	0.69	0.36	0.20	0.60	0.79	0.33	0.13	0.75	0.76	0.62	0.56	0.98	0.94	0.98	0.83	0.76	0.95	0.63	0.34	1.00	1.00	0.99	0.92
Krasnoyarskiy kray	0.20	0.42	0.18	0.07	0.21	0.50	0.11	0.04	0.23	0.23	0.20	0.13	0.55	0.31	0.56	0.40	0.31	0.50	0.09	0.03	0.99	1.00	0.99	0.73
Kurganskaya oblast	0.45	0.35	0.19	0.16	0.36	0.40	0.13	0.02	0.23	0.09	0.10	0.06	0.66	0.17	0.67	0.35	0.53	0.53	0.21	0.03	1.00	1.00	0.99	0.75
Kurskaya oblast	0.42	0.41	0.18	0.12	0.46	0.38	0.08	0.10	0.39	0.26	0.19	0.37	0.66	0.26	0.66	0.46	0.40	0.52	0.16	0.08	0.98	1.00	0.95	0.69
Leningradskaya oblast	0.34	0.49	0.16	0.09	0.44	0.59	0.08	0.04	0.42	0.34	0.20	0.22	0.84	0.64	0.86	0.58	0.43	0.68	0.14	0.05	0.99	1.00	0.97	0.72
Lipetskaya oblast	0.50	0.54	0.24	0.16	0.70	0.73	0.37	0.31	0.62	0.61	0.51	0.53	0.70	0.66	0.71	0.64	0.63	0.83	0.46	0.26	0.97	1.00	0.94	0.70
Magadanskaya oblast	0.17	0.53	0.13	0.17	0.22	0.69	0.15	0.19	0.54	0.52	0.23	0.32	0.42	0.36	0.45	0.34	0.33	0.82	0.25	0.22	0.99	1.00	0.96	0.67
Moskovskaya oblast	0.23	0.63	0.20	0.04	0.22	0.75	0.07	0.02	0.25	0.20	0.15	0.08	0.87	0.69	0.88	0.57	0.40	0.74	0.13	0.03	0.99	1.00	0.97	0.62

Table C4: (Continued)

Region	2012				2016				2018				2020				2021				2024			
	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm	Shp	EM_p	Em_h	Bfm
Murmanskaya oblast	0.12	0.66	0.15	0.24	0.18	0.78	0.09	0.14	0.23	0.40	0.10	0.28	0.08	0.26	0.18	0.22	0.17	0.67	0.10	0.11	0.96	1.00	0.88	0.46
Nenetskiy ao	0.14	0.22	0.18	0.04	0.12	0.31	0.02	0.00	0.14	0.12	0.08	0.04	0.13	0.02	0.13	0.02	0.22	0.20	0.02	0.00	0.96	1.00	0.78	0.15
Nizhegorodskaya oblast	0.55	0.63	0.33	0.22	0.47	0.74	0.29	0.22	0.48	0.43	0.30	0.28	0.81	0.66	0.82	0.63	0.45	0.79	0.32	0.20	1.00	1.00	0.99	0.77
Novgorodskaya oblast	0.17	0.31	0.14	0.03	0.24	0.46	0.07	0.01	0.05	0.06	0.14	0.03	0.41	0.08	0.45	0.26	0.24	0.43	0.03	0.01	0.95	1.00	0.86	0.31
Novosibirskaya oblast	0.33	0.38	0.12	0.06	0.16	0.49	0.10	0.01	0.19	0.17	0.15	0.06	0.51	0.31	0.65	0.39	0.29	0.60	0.16	0.04	0.91	1.00	0.88	0.44
Omskaya oblast	0.37	0.45	0.22	0.14	0.29	0.48	0.15	0.06	0.18	0.16	0.14	0.09	0.69	0.41	0.69	0.47	0.28	0.47	0.11	0.05	0.99	1.00	0.96	0.64
Orenburgskaya oblast	0.23	0.31	0.13	0.04	0.35	0.45	0.10	0.04	0.39	0.25	0.17	0.12	0.86	0.49	0.87	0.55	0.43	0.54	0.14	0.06	0.98	1.00	0.96	0.67
Orlovskaya oblast	0.56	0.42	0.20	0.12	0.71	0.72	0.42	0.21	0.74	0.62	0.53	0.44	0.91	0.80	0.92	0.76	0.63	0.70	0.33	0.16	1.00	1.00	0.99	0.77
Penzenskaya oblast	0.64	0.65	0.37	0.33	0.84	0.89	0.63	0.52	0.75	0.71	0.60	0.58	0.93	0.81	0.93	0.80	0.83	0.91	0.60	0.36	1.00	1.00	0.99	0.85
Permskiy kray	0.06	0.46	0.28	0.04	0.12	0.56	0.09	0.01	0.42	0.27	0.15	0.16	0.40	0.09	0.45	0.25	0.19	0.53	0.05	0.01	0.99	1.00	0.98	0.79
Primorskiy kray	0.29	0.53	0.26	0.22	0.21	0.60	0.16	0.09	0.16	0.25	0.19	0.14	0.60	0.42	0.65	0.45	0.26	0.58	0.13	0.10	0.97	1.00	0.95	0.66
Pskovskaya oblast	0.20	0.29	0.15	0.05	0.31	0.39	0.06	0.02	0.42	0.25	0.18	0.14	0.66	0.27	0.68	0.51	0.38	0.48	0.10	0.03	0.96	1.00	0.92	0.50
Respublika Adygeya	0.36	0.54	0.23	0.13	0.67	0.76	0.37	0.26	0.59	0.64	0.56	0.50	0.94	0.88	0.95	0.77	0.79	0.87	0.60	0.39	0.99	1.00	0.99	0.88
Respublika Altay	0.57	0.55	0.35	0.32	0.36	0.29	0.06	0.05	0.37	0.22	0.16	0.19	0.45	0.17	0.49	0.22	0.33	0.31	0.06	0.01	0.99	1.00	0.97	0.71
Respublika Bashkortostan	0.76	0.92	0.67	0.68	0.83	0.92	0.73	0.46	0.79	0.76	0.66	0.53	0.97	0.99	0.96	0.91	0.85	0.96	0.79	0.59	1.00	1.00	1.00	0.82
Respublika Buryatiya	0.51	0.58	0.35	0.31	0.29	0.47	0.13	0.06	0.65	0.62	0.48	0.38	0.62	0.36	0.62	0.46	0.44	0.57	0.19	0.13	0.98	1.00	0.94	0.68
Respublika Dagestan	0.91	0.93	0.89	0.91	0.86	0.93	0.84	0.85	0.81	0.88	0.77	0.87	0.96	0.91	0.96	0.88	0.88	0.94	0.85	0.73	1.00	1.00	1.00	0.95
Respublika Ingushetiya	0.94	1.00	0.93	0.79	0.96	0.99	0.95	0.47	0.96	0.97	0.92	0.64	0.97	0.80	0.96	0.74	0.96	1.00	0.96	0.69	1.00	1.00	1.00	0.92
Respublika Kalmykiya	0.40	0.52	0.33	0.32	0.80	0.73	0.51	0.47	0.63	0.60	0.58	0.58	0.88	0.70	0.89	0.74	0.59	0.50	0.18	0.12	1.00	1.00	1.00	0.82
Respublika Kareliya	0.02	0.39	0.24	0.03	0.24	0.47	0.02	0.00	0.02	0.09	0.19	0.03	0.11	0.04	0.16	0.11	0.21	0.50	0.02	0.01	0.91	1.00	0.73	0.09
Respublika Khakasiya	0.45	0.41	0.19	0.15	0.26	0.49	0.05	0.02	0.39	0.25	0.19	0.16	0.42	0.18	0.46	0.28	0.16	0.49	0.05	0.00	0.98	1.00	0.95	0.64
Respublika Komi	0.63	0.60	0.30	0.19	0.33	0.50	0.07	0.03	0.16	0.14	0.16	0.06	0.35	0.11	0.38	0.20	0.23	0.52	0.07	0.01	0.93	1.00	0.79	0.19
Respublika Krym	–	–	–	–	0.63	0.71	0.16	0.15	0.74	0.72	0.35	0.91	0.91	0.86	0.91	0.77	0.60	0.78	0.20	0.12	1.00	1.00	1.00	0.96
Respublika Mariy El	0.80	0.63	0.41	0.25	0.58	0.41	0.11	0.05	0.37	0.20	0.11	0.10	0.71	0.37	0.73	0.51	0.52	0.42	0.05	0.01	0.95	1.00	0.90	0.51
Respublika Mordoviya	0.90	0.98	0.87	0.89	0.90	0.98	0.87	0.86	0.88	0.86	0.78	0.79	0.99	0.88	0.99	0.88	0.91	0.97	0.77	0.64	1.00	1.00	1.00	0.91
Respublika Sakha Yakutiya	0.75	0.77	0.54	0.52	0.56	0.61	0.27	0.09	0.58	0.40	0.30	0.11	0.51	0.21	0.55	0.24	0.53	0.62	0.24	0.06	0.98	1.00	0.93	0.63
Respublika Severnaya Osetiya	0.75	0.86	0.73	0.42	0.88	0.97	0.86	0.48	0.88	0.97	0.85	0.80	0.96	0.93	0.96	0.75	0.92	0.99	0.91	0.54	1.00	1.00	1.00	0.96
Respublika Tatarstan	0.73	0.98	0.65	0.78	0.80	0.99	0.69	0.78	0.73	0.86	0.66	0.70	0.94	0.86	0.94	0.80	0.85	1.00	0.83	0.71	1.00	1.00	1.00	0.89
Respublika Tyva	0.84	0.98	0.83	0.93	0.81	1.00	0.81	0.83	0.92	0.99	0.87	0.98	0.92	1.00	0.91	0.97	0.91	0.99	0.89	0.76	1.00	1.00	1.00	0.99
Rostovskaya oblast	0.39	0.51	0.20	0.12	0.52	0.72	0.28	0.16	0.43	0.42	0.35	0.31	0.90	0.78	0.91	0.67	0.42	0.77	0.25	0.13	0.98	1.00	0.97	0.74
Ryazanskaya oblast	0.35	0.35	0.15	0.10	0.44	0.55	0.22	0.17	0.44	0.35	0.25	0.26	0.86	0.51	0.87	0.57	0.57	0.69	0.31	0.20	0.99	1.00	0.96	0.73
Sakhalinskaya oblast	0.12	0.60	0.23	0.22	0.18	0.72	0.15	0.23	0.17	0.41	0.19	0.27	0.58	0.49	0.59	0.50	0.20	0.64	0.11	0.12	0.99	1.00	0.97	0.72
Samarskaya oblast	0.29	0.60	0.22	0.07	0.71	0.86	0.38	0.23	0.50	0.57	0.41	0.31	0.74	0.68	0.75	0.61	0.52	0.90	0.38	0.23	0.96	1.00	0.93	0.73
Saratovskaya oblast	0.54	0.64	0.38	0.29	0.79	0.79	0.62	0.37	0.54	0.53	0.48	0.41	0.93	0.75	0.93	0.69	0.69	0.84	0.50	0.31	0.99	1.00	0.98	0.75

Table C4: (Continued)

Region	**2012**				**2016**				**2018**				**2020**				**2021**				**2024**			
	Shp	EM_p	Em_h	Bfm	*Shp*	EM_p	Em_h	Bfm	*Shp*	EM_p	Em_h	Bfm	*Shp*	EM_p	Em_h	Bfm	*Shp*	EM_p	Em_h	Bfm	*Shp*	EM_p	Em_h	Bfm
Smolenskaya oblast	0.19	0.39	0.20	0.05	0.30	0.52	0.12	0.07	0.17	0.14	0.15	0.08	0.48	0.17	0.52	0.36	0.25	0.51	0.11	0.06	0.96	1.00	0.94	0.64
Stavropolskiy kray	0.28	0.70	0.38	0.10	0.41	0.74	0.13	0.06	0.63	0.61	0.50	0.43	0.93	0.91	0.93	0.75	0.78	0.92	0.63	0.26	1.00	1.00	1.00	0.82
Sverdlovskaya oblast	0.10	0.54	0.18	0.04	0.40	0.57	0.03	0.01	0.18	0.14	0.09	0.06	0.31	0.08	0.33	0.17	0.58	0.54	0.04	0.01	0.97	1.00	0.93	0.54
Tambovskaya oblast	0.67	0.62	0.40	0.34	0.58	0.68	0.34	0.31	0.73	0.73	0.63	0.64	0.94	0.87	0.94	0.85	0.83	0.89	0.60	0.36	0.98	1.00	0.97	0.81
Territoriya za predelami RF	0.40	0.94	0.41	0.76	–	–	–	–	0.48	0.97	0.47	0.89	–	–	–	–	–	–	–	–	1.00	1.00	1.00	0.65
Tomskaya oblast	0.11	0.33	0.17	0.03	0.13	0.50	0.13	0.02	0.08	0.08	0.13	0.02	0.15	0.02	0.22	0.09	0.26	0.39	0.02	0.01	0.91	1.00	0.82	0.20
Tulskaya oblast	0.59	0.62	0.36	0.26	0.54	0.63	0.21	0.15	0.54	0.41	0.29	0.33	0.91	0.57	0.91	0.64	0.67	0.77	0.36	0.19	1.00	1.00	1.00	0.74
Tverskaya oblast	0.21	0.38	0.21	0.09	0.34	0.47	0.11	0.07	0.12	0.12	0.22	0.09	0.53	0.26	0.55	0.38	0.30	0.49	0.11	0.06	0.97	1.00	0.91	0.60
Tyumenskaya oblast	0.89	0.90	0.69	0.63	0.84	0.98	0.83	0.56	0.84	0.80	0.62	0.58	0.94	0.81	0.94	0.78	0.82	0.87	0.57	0.36	1.00	1.00	1.00	0.81
Udmurtskaya respublika	0.46	0.46	0.17	0.20	0.46	0.53	0.12	0.09	0.32	0.21	0.13	0.17	0.55	0.32	0.55	0.40	0.57	0.63	0.18	0.04	0.93	1.00	0.87	0.46
Ulyanovskaya oblast	0.47	0.57	0.29	0.17	0.76	0.79	0.43	0.28	0.47	0.40	0.35	0.28	0.64	0.43	0.72	0.45	0.52	0.74	0.29	0.14	0.99	1.00	0.95	0.67
Vladimirskaya oblast	0.03	0.49	0.37	0.01	0.27	0.54	0.07	0.02	0.30	0.12	0.06	0.03	0.41	0.13	0.49	0.21	0.18	0.54	0.05	0.01	0.95	1.00	0.92	0.44
Volgogradskaya oblast	0.43	0.57	0.25	0.15	0.42	0.56	0.10	0.06	0.53	0.45	0.30	0.28	0.96	0.83	0.97	0.72	0.86	0.92	0.69	0.23	1.00	1.00	1.00	0.78
Vologodskaya oblast	0.22	0.35	0.11	0.07	0.26	0.41	0.04	0.01	0.34	0.18	0.08	0.06	0.62	0.27	0.63	0.43	0.44	0.41	0.04	0.01	0.99	1.00	0.97	0.53
Voronezhskaya oblast	0.61	0.66	0.37	0.26	0.65	0.89	0.54	0.38	0.49	0.50	0.45	0.39	0.83	0.69	0.85	0.67	0.66	0.92	0.57	0.36	0.96	1.00	0.95	0.71
Yamalo-Nenetskiy ao	0.95	1.00	0.92	0.86	0.87	0.95	0.77	0.35	0.90	0.95	0.84	0.78	0.96	0.91	0.97	0.77	0.81	0.94	0.66	0.23	1.00	1.00	1.00	0.98
Yaroslavskaya oblast	0.31	0.38	0.09	0.06	0.20	0.58	0.05	0.02	0.22	0.12	0.08	0.06	0.53	0.24	0.55	0.35	0.22	0.57	0.05	0.01	0.96	1.00	0.92	0.53
Yevreyskaya ao	0.18	0.35	0.20	0.07	0.17	0.35	0.08	0.03	0.10	0.08	0.11	0.04	0.90	0.42	0.91	0.61	0.67	0.71	0.48	0.28	1.00	1.00	1.00	0.94
Zabaykalskiy kray	0.25	0.40	0.26	0.10	0.18	0.44	0.15	0.04	0.16	0.15	0.23	0.09	0.65	0.26	0.66	0.44	0.21	0.44	0.13	0.04	0.96	1.00	0.89	0.48

Notes: Shp – Shpilkin's estimates; (b) EM_p – univariate finite mixture model (precinct-based); (c) Em_h – univariate finite mixture model (histogram-based); (d) Bfm – Bayesian finite mixture model's estimates.