

Hackers claim breach of Russian election systems days before parliamentary vote

By Daryna Antoniuk

Published: 2026-09-17 · Archived: 2026-09-19 02:00:19 UTC

An anonymous hacking group claimed to have broken into computer systems connected to Russia's election infrastructure just days before the country begins voting for a new parliament.

The group, calling itself CikLeak, said it gained access to systems belonging to Russia's Central Election Commission and companies involved in developing Vybory, the state-run platform used to administer elections.

The hackers claimed to have stolen internal documents, server configurations, passwords and employee communications from the commission and its contractors, including Russian telecom giant Rostelecom.

They provided the stolen material to Important Stories, an independent Russian investigative outlet that [said](#) it had authenticated the documents. However, it remains unclear how deeply the hackers penetrated the election infrastructure or whether they gained access to systems directly involved in voting or counting ballots.

"We infiltrated the infrastructure of Russia's Central Election Commission and downloaded secret documents and developers' internal chats," the group claimed on its [website](#).

CikLeak said it did not intend to disrupt voting or interfere with the work of election commissions. Instead, the group said its goal was to expose how the Russian electoral system works internally and what it described as opportunities for authorities to manipulate election results.

The hackers also published screenshots purportedly showing compromised systems and urged Russians to vote in person on the final day of the election, arguing that doing so would make manipulation more difficult.

Russia will hold elections for all 450 seats in the State Duma, the lower house of parliament, over three days beginning Friday. It will be the first election for the chamber since Russia launched its full-scale invasion of Ukraine in February 2022.

The vote will also be the first federal election conducted using the Vybory 2.0 platform. Use of the system began this year, replacing an earlier version that had been used since the late 1990s.

Russia's Central Election Commission (CEC) had warned of growing cyber threats as voting approached.

A day before CikLeak disclosed the alleged breach, Russian election officials tested the security of the Vybory portal, remote electronic voting system and video surveillance infrastructure. The assessment [identified](#) the video surveillance system, particularly the uninterrupted transmission of its feeds, as a "weak link."

CEC Chair Ella Pamfilova said the number of attacks targeting election systems and related infrastructure had been rising ahead of the vote.

“We have been dealing with this for years, but what is happening now is difficult to compare with anything in terms of the intensity, volume and speed of the various attacks,” Pamfilova said.

Her comments followed [assurances](#) in August that the election system was fully protected against cyberattacks. Pamfilova said information about eligible voters was updated online twice a year and stored in a closed-access system.

Russian election infrastructure [has been targeted](#) during previous votes.

During the March 2024 presidential election, hackers launched distributed denial-of-service attacks and set up phishing sites and fake Telegram channels designed to imitate official Russian services.

Rostelecom said at the time that most attacks against election infrastructure originated from Ukraine, Western Europe and North America and involved what it described as professional hacking groups.

Hackers also targeted online services belonging to United Russia, President Vladimir Putin’s political party, as well as government services in several Russian regions.

Ukraine’s military intelligence agency, known as HUR, later [acknowledged](#) that it was behind attacks on United Russia and Russia’s electronic voting system.



Know what matters.

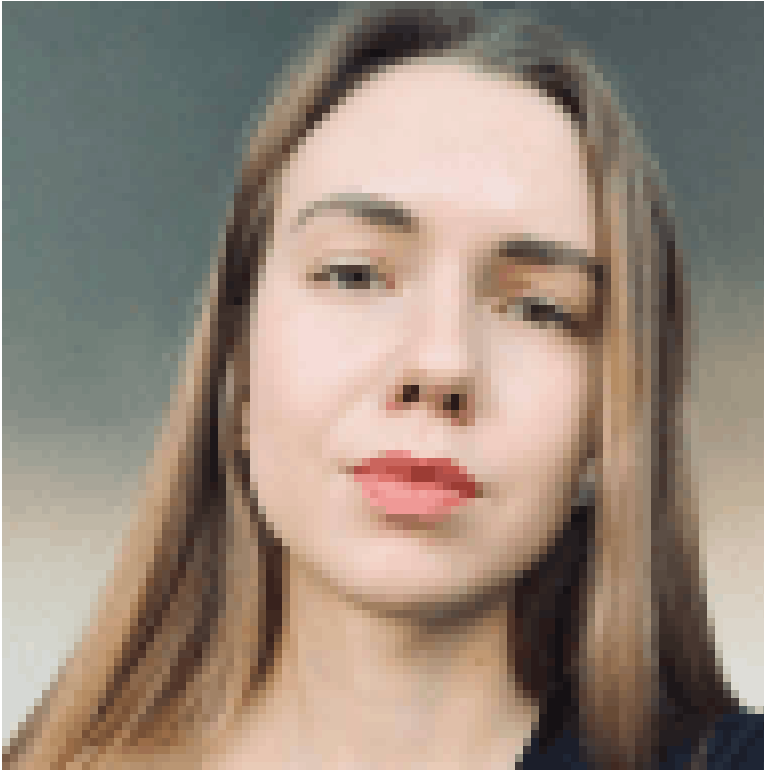
Act first.

Get started



No previous article

No new articles



[Daryna Antoniuk](#)

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.

Source: <https://therecord.media/russia-election-hackers-breach>