

10.10.2025 № MH-19/1298

Руководителям организаций,
подведомственных
Минобрнауки России

Ha N₀ OT

О выявленном инциденте и мерах по повышению информационной безопасности Российской Федерации

Департамент цифрового развития Минобрнауки России (далее – Департамент) в рамках обеспечения мер по информационной безопасности сообщает, что в настоящее время участились случаи мошеннических действий, которые направлены на сотрудников подведомственных организаций Минобрнауки России (далее – организации).

Так, участились случаи направления руководителям организаций поддельных документов с недостоверной информацией и призывами к действиям в мессенджерах «MAX» и «Telegram» (прилагается) (далее – инцидент информационной безопасности).

В соответствии с подпунктом «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и с целью предотвращения реализации угроз безопасности информации Департамент рекомендует:

1. Проинформировать работников организаций о факте обнаружения инцидента информационной безопасности.
2. Не отвечать на подозрительные сообщения, полученные посредством электронной почты.
3. Не открывать подозрительные чаты в мессенджерах, в том числе в «WhatsApp» и «Telegram».
4. Проверять подлинность источников информации.
5. Не переходить по ссылкам и не скачивать файлы, содержащиеся в письмах от неизвестных адресантов.

6. Не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями .rtf, .lnk, .chm, .vhd.

7. Не открывать и не загружать вложения из писем с тематикой, неотносящейся к деятельности организации.

8. Не передавать личную и служебную информацию через каналы, не прошедшие официальной верификации.

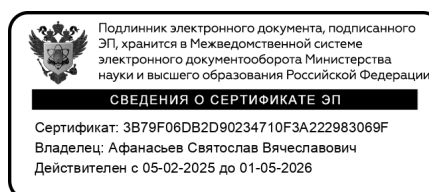
9. В случае обнаружения подозрительного поведения или при наличии сомнений относительно поступающей корреспонденции, общения с возможными злоумышленниками, выдающими себя за сотрудников Минобрнауки России или коллег, в мессенджерах или при телефонных звонках, рекомендуется подтвердить полученные поручения через другие официальные каналы связи.

В случае возникновения ситуаций, аналогичных вышеуказанной, Департамент рекомендует незамедлительно обращаться в отдел информационной безопасности Департамента по тел. +7 (495) 547-12-60 (доб. 2571, 2522) или по адресу эл. почты: cyberthreats@minobrnauki.gov.ru, suz@niisva.org.

Дополнительно информируем о необходимости принятия мер по недопущению распространения настоящих рекомендаций в информационно-телекоммуникационной сети «Интернет».

Приложение: на 1 л. в 1 экз.

Директор Департамента
цифрового развития



С.В. Афанасьев



АПС № 2315

АППАРАТ ПРИКОМАНДИРОВАННЫХ
СОТРУДНИКОВ ФЕДЕРАЛЬНОЙ
СЛУЖБЫ БЕЗОПАСНОСТИ
(АПС ФСБ РОССИИ)

107031, г. Москва, ул. Мухоморова, д. 1



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РФ

ЗАРЕГИСТРИРОВАНО

Регистрационный № 2315

от 04 Октября 2025 г.

Дата: 04.10.2025

ПРИКАЗ

О проведении проверки кадрового состава организации в связи с утечкой персональных данных клиентов

Название организации: [REDACTED]

В связи с выявленной утечкой персональных данных клиентов, зарегистрированных в информационных системах вышеуказанной организации, проводится проверка с целью выявления источника утечки и возможной причастности сотрудников (в том числе ранее работавших) к инциденту. Проверка проводится в интересах обеспечения информационной безопасности, в соответствии с Федеральным законом №152-ФЗ «О персональных данных».

Основание для проверки:

Нарушение порядка хранения, обработки и передачи персональных данных клиентов третьим лицам.

Порядок проведения проверки (обязательно к исполнению):

1. Уведомить сотрудников и лиц, ответственных за проведение бесед с куратором, ответственным за проверку.
2. Не допускать разглашения информации о проверке лицам, не являющимся участниками.
3. Беседы с проверяемыми будут проводиться по телефону без согласования времени. Задача обеспечить доступность для связи в день проведения проверки по средствам мессенджеров MAX и Telegram. В случае отсутствия на мобильном устройстве национального сервиса MAX, необходимо будет провести его установку для обеспечения безопасного общения и соблюдения Федерального закона от 24 июня 2025 года №156-ФЗ "О создании многофункционального сервиса обмена информацией".

Дальнейшие инструкции и действия по ситуации, согласовывать с руководителем в лице прикомандированного сотрудника по части проверки - Матвеев В.В.

Начальник Аппарата Прикомандированных
Сотрудников ФСБ РФ

В.И. Глухов

