МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ул. Артёма, 129-А, г. Донецк, 283000
тел. +7 (949) 321 44 37
e-mail: info@mondnr.ru, www.mondnr.ru

28.03.2025 № 14-09.3/4249-25
на №_____ от _____

Руководителям департаментов, управлений, отделов образования администраций городских и муниципальных округов Донецкой Народной Республики

Руководителям образовательных организаций, подведомственных Министерству образования и науки Донецкой Народной Республики

Уважаемые руководители!

Министерством образования и науки Донецкой Народной Республики получено письмо Прокуратуры Донецкой Народной Республики от 25 марта 2025 г. № 7-25-2025/, о проведении органами прокуратуры республики надзорных мероприятий, направленных на обеспечение информационной безопасности граждан, профилактику и предупреждение преступлений и правонарушений, связанных с использованием информационно-телекоммуникационных технологий (далее – ИТТ).

Учитывая изложенное, с целью формирования правовой культуры граждан, осведомленности в сфере совершения преступлений и правонарушений с ИТТ, а также мер защиты от них, Вам необходимо распространить приложенный информационно-разъяснительный материал на информационных стендах, официальных сайтах образовательных организаций Донецкой Народной Республики.

Приложение: на 1 л. 1экз.

Заместитель министра

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0083324BA091D00ECDCFE1DBDCAADD611B
Владелец **Пестрецов Виталий Викторович**
Действителен с 24.01.2025 по 19.04.2026

В.В.Пестрецов

Растопчина Татьяна Анатольевна
Руденко Оксана Викторовна

Памятка: «Информационная гигиена»

В современных условиях активного использования информационных технологий и Интернета соблюдение принципов информационной гигиены становится особенно актуальным.

С целью повышения осведомленности граждан о мерах безопасности, которые помогут защитить личные данные, компьютерные устройства и смартфоны от несанкционированного доступа и утраты информации, необходимо соблюдать следующие правила.

Внимательность при переходе по ссылкам. Избегайте переходов по неизвестным ссылкам, не открывайте ссылки, полученные из ненадежных источников, включая электронную почту, сообщения в мессенджерах и социальных сетях от незнакомых лиц или подозрительных аккаунтов.

Проверяйте адреса сайтов. Перед вводом личной информации убедитесь, что адрес веб-страницы начинается с "https://" и соответствует официальному сайту организации. Внимательно изучите адресную строку на предмет подозрительных признаков.

Будьте осторожны с акциями и предложениями. Если вам предлагают слишком выгодные условия, скорее всего, это может быть обман. Проверяйте легитимность предложений через официальные каналы.

Защищайте личные данные. Не передавайте личные данные незнакомым лицам. Избегайте предоставления своих данных, таких как номера телефонов, паспортные данные, реквизиты банковских карт, если у вас нет полной уверенности в безопасности общения.

Используйте надежные пароли. Создавайте сложные пароли для своих аккаунтов, меняйте их регулярно и не используйте одни и те же пароли на разных ресурсах.

Установите двухфакторную аутентификацию. Включите двухфакторную аутентификацию на всех доступных сервисах, что значительно увеличит уровень безопасности ваших аккаунтов.

Защитите компьютерную технику и смартфоны. Обновляйте программное обеспечение, регулярно устанавливайте обновления операционных систем и программ, чтобы устранять известные уязвимости и повысить уровень безопасности.

Установите антивирусные программы. Используйте лицензионные антивирусные решения и регулярно проводите полное сканирование ваших устройств.

Не оставляйте устройства без присмотра. Будьте внимательны к своим устройствам, не оставляйте их без наблюдения в общественных местах.

Не забывайте, что соблюдение информационной гигиены является необходимым условием защиты ваших личных данных, а также повышение уровня безопасности компьютерной техники и мобильных устройств.

Подготовлено управлением по надзору за исполнением федерального законодательства прокуратуры республики