



**АДМИНИСТРАЦИЯ
ВОЛГОГРАДА**

ул. им. Володарского, д. 5, Волгоград, 400066,
тел. (8442) 30-12-83, факс (8442) 30-14-24
E-mail: kancelyaria@volgadmin.ru,
ОКПО 04024339, ОГРН 1023403433822,
ИНН/КПП 3444059139/344401001

Руководителям структурных
подразделений администрации
Волгограда
(по реестру)

от 10.10.2025 № 05-ч/3448
на № _____ от _____

Уважаемые коллеги!

В связи с письмом ГУ МВД России по Волгоградской области от 25.09.2025 № 6/7270 сообщая следующее.

По информации ГУ МВД России по Волгоградской области, за 8 месяцев 2025 года на территории Российской Федерации зарегистрировано 12,4 тысячи преступлений, предусмотренных статьей 207 УК РФ (заведомо ложное сообщение об акте терроризма), совершенных с использованием информационно-коммуникационных технологий. Данные преступления дезорганизуют работу органов государственной власти, организаций и предприятий, вынуждают правоохранительные органы и социальные службы задействовать значительные силы и средства для проверочных мероприятий и охраны общественного порядка.

Учитывая изложенное, направляю Рекомендации МВД России о мерах по повышению защищенности информационной инфраструктуры для учета в работе вашего структурного подразделения, а также подведомственных организаций.

Приложение: на 3 л. в 1 экз.

Руководитель аппарата главы Волгограда

Е.А.Алтухов

РЕКОМЕНДАЦИИ

о мерах по повышению защищенности информационной инфраструктуры образовательных учреждений Российской Федерации

Анализ сведений об угрозах безопасности информации, проводимый в условиях складывающейся обстановки, указывает на увеличение числа компьютерных атак и связанных с ними утечек персональных данных.

Продолжают фиксироваться факты большого количества фишинговых писем, попыток внедрения вирусов-шифровальщиков через почтовые вложения, а также рассылок заведомо ложных сообщений об актах терроризма.

В целях предотвращения реализации угроз безопасности информационной инфраструктуры образовательных учреждений Российской Федерации необходимо принять дополнительные меры защиты информации:

1. Обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных.

2. Настроить в средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на электронную почту вложений.

3. Проинформировать пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;

- не открывать письма от неизвестных адресатов;

- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

- не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т. д.);

- не нажимать на ссылки из письма, если они заменены на слова;

- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;

- не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

- не переходить по ссылкам и не скачивать файлы, содержащиеся во входящих почтовых сообщениях, если средствами антивирусной защиты в указанных вложениях обнаружено вредоносное программное обеспечение;

- внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;

- в случае появления сомнений, направлять полученное письмо как вложение администратору информационной системы.

4. Активировать (по возможности) механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM, DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий.

5. Заблокировать (при возможности) получение пользователя информационной системы в электронных письмах вложений с расширениями ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

6. Заблокировать доставку писем от зарубежных доменов-отправителей.

7. Обеспечить регулярное обновление используемого программного обеспечения, в том числе на сетевых устройствах (маршрутизаторах, коммутаторах).

8. Обеспечить использование устойчивых длинных паролей административных учетных записей.

При поступлении на адрес электронной почты заведомо ложного сообщения об акте терроризма необходимо принять следующие меры:

1. Поступившее сообщение об акте терроризма не удалять.

2. Осуществить копирование текста сообщения об акте терроризма в виде снимков экрана устройства (скриншотов либо фотоизображений, полученных посредством цифровой фотофиксации).

2.1. На скриншотах (фотоизображениях) должна отображаться следующая информация об объекте:

- название темы письма (в том числе если письмо не имеет названия: «<Без темы>»);

- адрес электронной почты отправителя письма, зафиксированный в графе, обозначенной реквизитом «От:»;

- дата и время отправления письма;

- текст письма (включая подпись к нему, например: «С уважением, Иван Иванов»), который может содержаться непосредственно в письме и/или во вложении к нему в виде прикрепленного файла.

2.2. Зафиксировать на скриншоте/фотоизображении наличие в письме вложения, а также при открытии его зафиксировать аналогичным способом текст, который оно содержит.

3. Исключить копирование текста сообщения об акте терроризма (скриншоты/фотоизображения) ненадлежащего качества, обусловленного небрежным копированием, фотографированием текстов.

4. При невозможности фиксации сообщений об акте терроризма в виде скриншотов/фотоизображений осуществить их фиксацию посредством функций копирования и вставки в документ Word (с сохранением указанной информации об объекте).

5. О поступившем сообщении об акте терроризма незамедлительно сообщить по единому номеру вызова экстренных оперативных служб «112» либо в ближайший орган внутренних дел.

МВД России

РЕЕСТР

от _____ № _____

Количество экземпляров	Наименование адреса	Примечание
1	2	3
1	Департамент по образованию администрации Волгограда	
1	Департамент ЖКХ и ТЭК администрации Волгограда	
1	Департамент муниципального имущества администрации Волгограда	
1	Департамент финансов администрации Волгограда	
1	Департамент по градостроительству и архитектуре администрации Волгограда	
1	Департамент городского хозяйства администрации Волгограда	
1	Комитет по культуре администрации Волгограда	
1	Департамент по жилищным и социальным вопросам администрации Волгограда	
1	Комитет гражданской защиты населения администрации Волгограда	
1	Комитет молодежной политики и туризма администрации Волгограда	
1	Комитет по строительству администрации Волгограда	
1	Комитет по физической культуре и спорту администрации Волгограда	
1	Правовое управление аппарата главы Волгограда	
1	Комитет по координации массовых мероприятий и взаимодействию с правоохранительными органами администрации Волгограда	
1	Департамент экономического развития и инвестиций администрации Волгограда	
1	Управление зарубежных и региональных связей аппарата главы Волгограда	
1	Отдел кадров аппарата главы Волгограда	
1	Комитет по информационной политике администрации Волгограда	
1	Контрольное управление аппарата главы Волгограда	
1	Управление бухгалтерского учета и финансово-экономического планирования аппарата главы Волгограда	
1	Отдел мобилизационной, секретной работы и защиты информации аппарата главы Волгограда	
1	Общий отдел аппарата главы Волгограда	
1	Отдел документационного обеспечения аппарата главы Волгограда	
8	Администрации районов	

Итого экземпляров: 31