Инструкция по цифровой безопасности для администраторов и участников родительских чатов

1. Если аккаунт родителя взломан и с него начали присылать деструктивную информацию

• Немедленно удалить сообщения с деструктивным контентом.
• Ограничить доступ — временно исключить или заблокировать взломанный аккаунт до восстановления контроля пользователем.
• Сообщить родителю лично (по телефону или в личном сообщении) о возможном взломе.
• Рекомендовать срочно сменить пароль и включить двухфакторную аутентификацию.
• При повторных атаках — обратиться в поддержку мессенджера (Telegram, WhatsApp, ВКонтакте и др.) и при необходимости в правоохранительные органы.

Важно: участникам чата пояснить, что произошёл технический сбой и меры приняты. Это снижает риск паники и распространения слухов.

2. Если ссылка на чат попала «в плохие руки» и туда начали присылать некорректное содержимое

• Немедленно удалить сообщения и заблокировать неизвестных участников.
• Закрыть действующую ссылку-приглашение (в настройках большинства мессенджеров есть возможность «отозвать ссылку»).
• Создать новую закрытую ссылку и переслать её только проверенным родителям через личные сообщения или официальные школьные каналы.
• При возможности — включить одобрение заявок администратором (ручное добавление).
• Провести разъяснение родителям: не пересылать ссылку третьим лицам и хранить её конфиденциально.

3. Если администратор чата был уволен и аккаунт больше не принадлежит другим пользователям

• Назначить заранее резервных администраторов (желательно 2–3 человека из числа родителей или педагогов). Это позволит сохранить чат даже при потере основного аккаунта.

Если чат уже удалён вместе с аккаунтом администратора:

• Создать новый чат официально от имени школы или совета родителей.

• Прислать актуальную ссылку на новый чат только проверенным участникам.

• Ввести правило: администраторский доступ не должен концентрироваться в одних руках, а распределяться между несколькими ответственными.

• Обсудить и зафиксировать в сообществе правила цифровой безопасности (пароли, резервные администраторы, недопустимость использования чатов для личных конфликтов).

Общие рекомендации по цифровой безопасности родительских чатов

- Использовать сложные пароли и менять их раз в полгода.
- Подключать двухфакторную аутентификацию.
- Минимизировать количество администраторов, но оставлять минимум двух для резервного контроля.
- Создать регламент работы чата: правила общения, действия в случае взлома, ответственность администраторов.
- При подозрительной активности — не скрывать проблему, а оперативно информировать родителей и принимать меры.

Таким образом, цифровая безопасность родительских чатов строится на трёх принципах: оперативная реакция, резервные меры защиты и информирование родителей