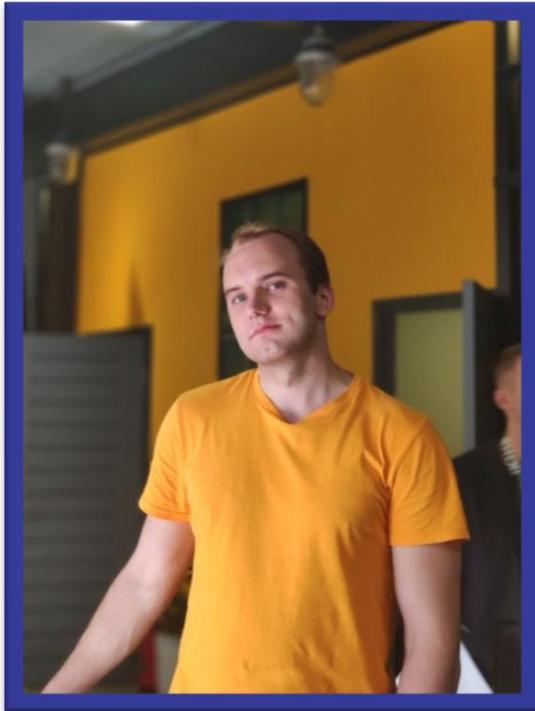




корпорация
российский
учебник



Быть начеку в сети. Основы кибербезопасности

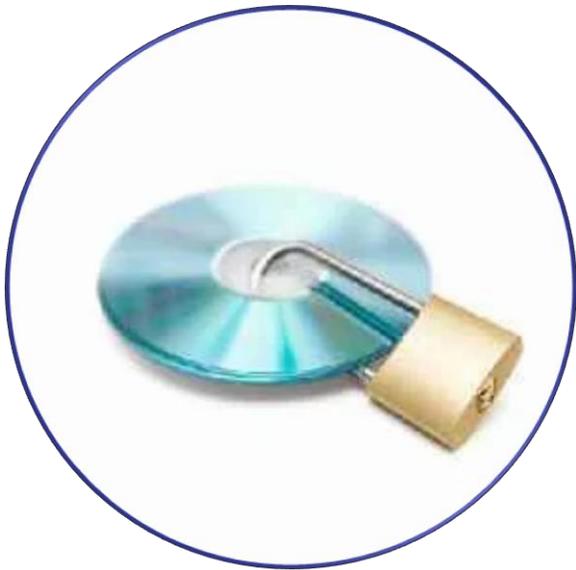


Малиновский Алексей

менеджер образовательных проектов Региональной общественной организации “Центр интернет-технологий”

Кибербезопасность – это обеспечение:

Целостности



Конфиденциальности



Доступности



Безопасность

Цифровых устройств



Онлайн-безопасность



Психологическая безопасность



Угрозы для цифровых устройств

Вирусы



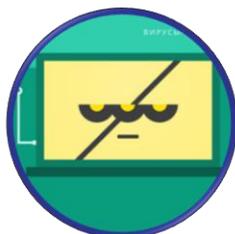
Потеря/кража



Самые опасные виды вирусов



Майнеры – добывают криптовалюты и отправляют злоумышленникам



Шифровальщики – шифруют файлы и папки и требуют деньги за расшифровку



Банковские трояны – воруют данные банковских карт, перехватывают банковские SMS и выдают себя за банковские приложения

Опасность в случае потери/кражи устройства



Прочтение ваших SMS и личных сообщений в социальных сетях/мессенджерах



Потеря денежных средств (через SMS-банкинг, звонки на платные номера или использование банковских приложений)



Передача ваших личных фотографий и видеозаписей третьим лицам

Как защитить своё цифровое устройство



Блокировщики рекламы для браузеров



Антивирусные программы



Пароли

Как защитить своё цифровое устройство



Блокировщики рекламы для браузеров



Антивирусные программы



Пароли

Угрозы онлайн-безопасности

Мошеннические сайты



Мошеннические страницы в социальных сетях и мессенджерах



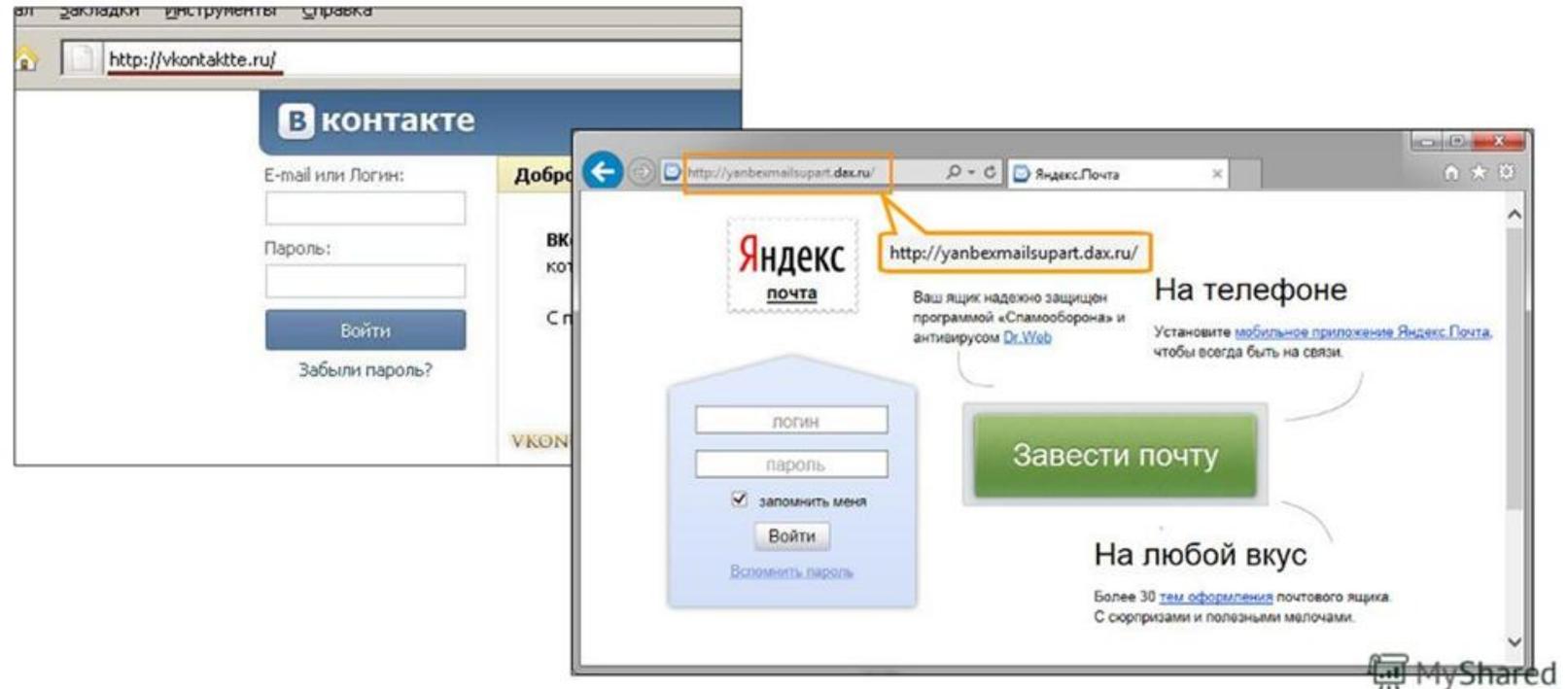
Мошеннические электронные письма



Мошеннические сайты

Чаще всего подделываются:

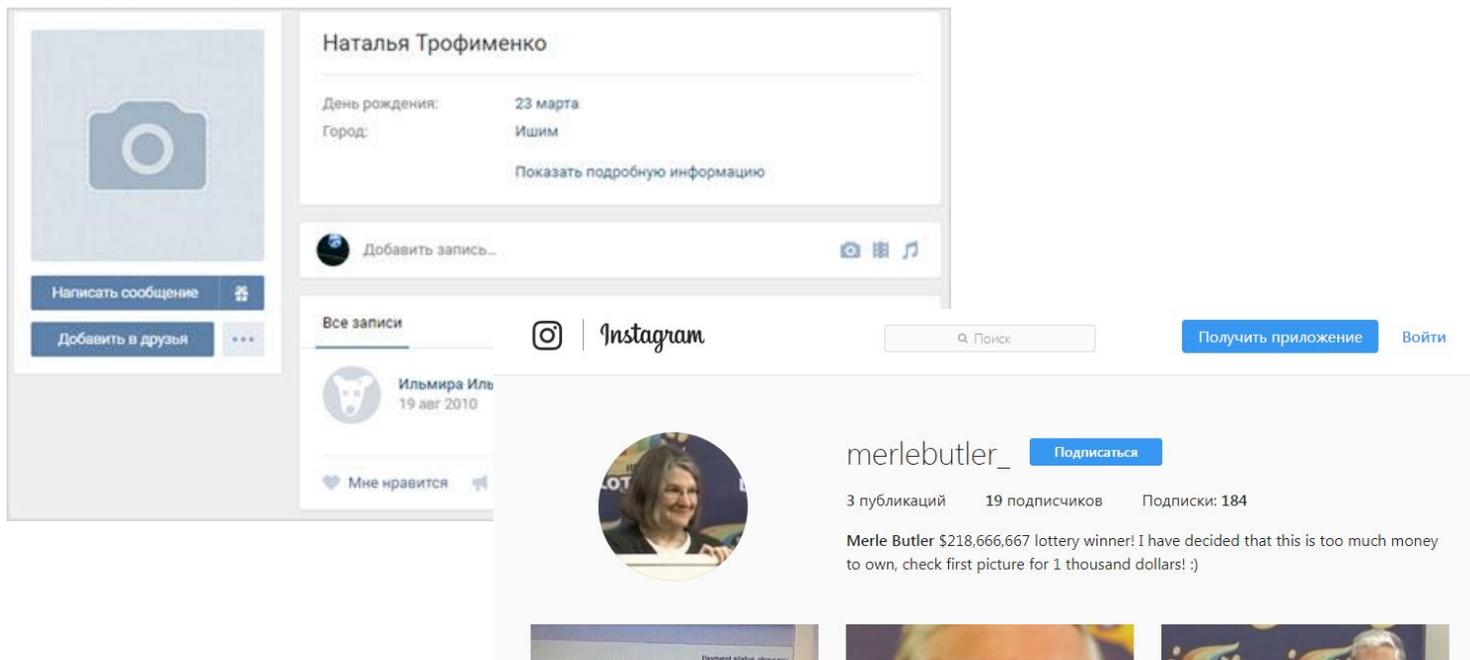
- Банки, платежные системы
- Сайты мобильных операторов
- Социальные сети
- Интернет-магазины
- Почтовые сервисы
- Билетные кассы
- Правительственные или налоговые сайты
- Онлайн-игры, онлайн-казино



Что хотят злоумышленники?

- Украсть данные ваших банковских карт и счетов
- Подписать вас на платные услуги
- Заразить ваше устройство вирусами
- Украсть данные вашего аккаунта в социальной сети или почтового ящика

Мошеннические страницы в социальных сетях и мессенджерах



- Зарегистрированы недавно
- Имеют мало друзей/подписчиков
- Фотографий либо нет, либо взяты из интернета

+32 232 882-22-31

ПРИВЕТ)) НЕ ВЫРУЧИШЬ?
НУЖНО 8000 НА КАРТОЧКУ



Мошеннические электронные письма

- Приходят с незнакомых доменов (@dsdjwe.com)
- Приходят с доменов, маскирующихся под реальные
- В письме к вам обращаются не по имени (“Уважаемый клиент...”)
- В них есть вложения в формате .exe, .vbs, .scr
- Могут попасть в папку “Спам”
- На них реагирует антивирусная программа

[adm] Просьба срочно сменить пароль!

Входящие x



Main Admin <[redacted]@[redacted].ru>

10:23 (5 мин. назад)



кому: мне

Здравствуйте уважаемый Иван Иванович!

В целях соблюдения безопасности, срочно требуется сменить пароль от почты.

Для смены пароля просьба СРОЧНО пройти по ссылке: <http://blackdiver.net?rid=4d222e2e889b2ad21497eff7f031113820714e7f04ce11c6199e42f88ed42c23>

Или воспользоваться программой, приложенной к этому письму.

Main Admin

Кто-то завладел Вашим паролем

Здравствуйте, [redacted]!

Кто-то только что пытался войти в аккаунт [redacted]@gmail.com через небезопасное приложение.

Подробности:

вторник, 15 Ноября 2016 г., 12:51 (Восточная Европа, стандартное время)
Московская область, Россия*

Мы настоятельно рекомендуем входить в аккаунт только через безопасные приложения, например Gmail. В противном случае ваши данные могут оказаться под угрозой. Обратите внимание, что все приложения, разработанные Google, соответствуют новейшим стандартам безопасности. [Подробнее...](#)

Так как мы заблокировали подозрительную попытку входа, настоятельно рекомендуем Вам изменить пароль.

[Изменить пароль](#)

Сообщение о увеличении задолженности

Сбербанк ОнЛ@йн (manager@sberb.ru) [Добавить контакт](#)

19.05.2012 4:32

Кому:

† Данное сообщение имеет высокую важность.



СБЕРБАНК РОССИИ

СООБЩЕНИЕ ОБ УВЕЛИЧЕНИИ ДОЛГА

Здравствуйте

По нашим данным на 19.05.2012 Вы превысили максимальную отсрочку платежа
[посмотреть статистику по счету вы можете по ссылке ниже](#)

[ПОСМОТРЕТЬ СТАТИСТИКУ](#)



корпорация
российский учебник



Как защитить себя в онлайн?

- Не отвечайте на сообщения с **незнакомых страниц и номеров**
- **Не проходите по ссылкам**, которые приходят на почту с незнакомых адресов, **не открывайте вложения**
- **Никому не отправляйте** свои **имя, пароли** и детали от **банковских аккаунтов**
- Если вы получили **странное письмо** от знакомого человека, **позвоните и уточните** детали
- Используйте **анти-спам дополнения** для браузера
- **Позаботьтесь о цифровой гигиене**

Цифровая гигиена – что нельзя выкладывать в Сеть

Личные данные (адрес, номер телефона)



Фотографии документов



Фотографии билетов



Пароли



Двухфакторная аутентификация – лучший способ защиты



Психологические угрозы

Кибербуллинг



Гаджетозависимость



Кибербуллинг

Кибербуллинг или **интернет-травля** — намеренные оскорбления, угрозы и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Виды кибербуллинга:

- Оскорбление
- Преследование
- Запугивание
- Распространение слухов
- Распространение откровенных фото

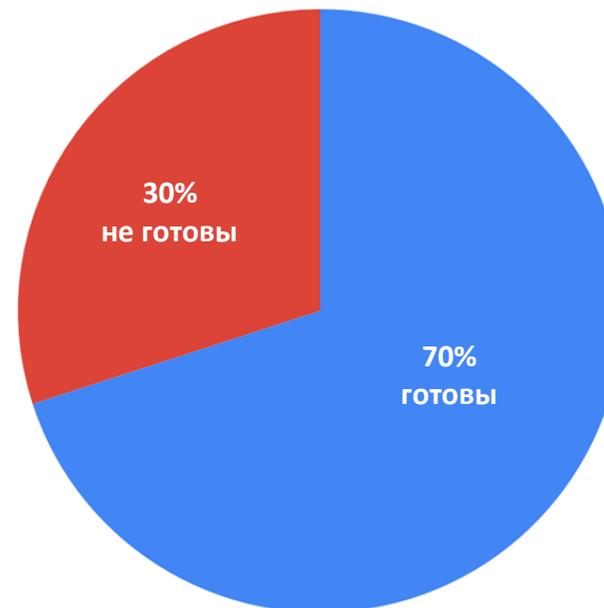
Кибербуллинг

Количество подростков, готовых обращаться за помощью при возникновении онлайн-травли

В России



В мире



Кибербуллинг

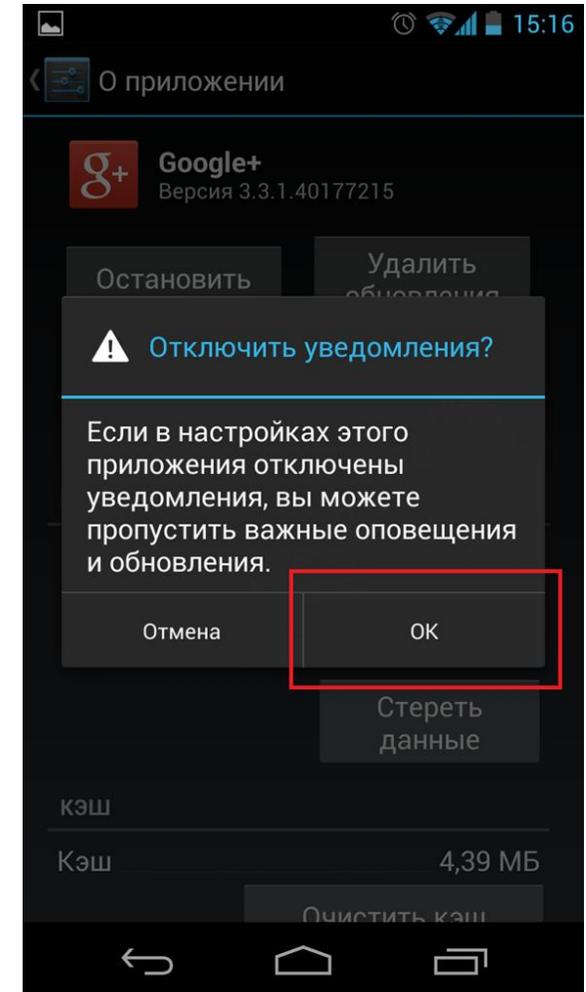
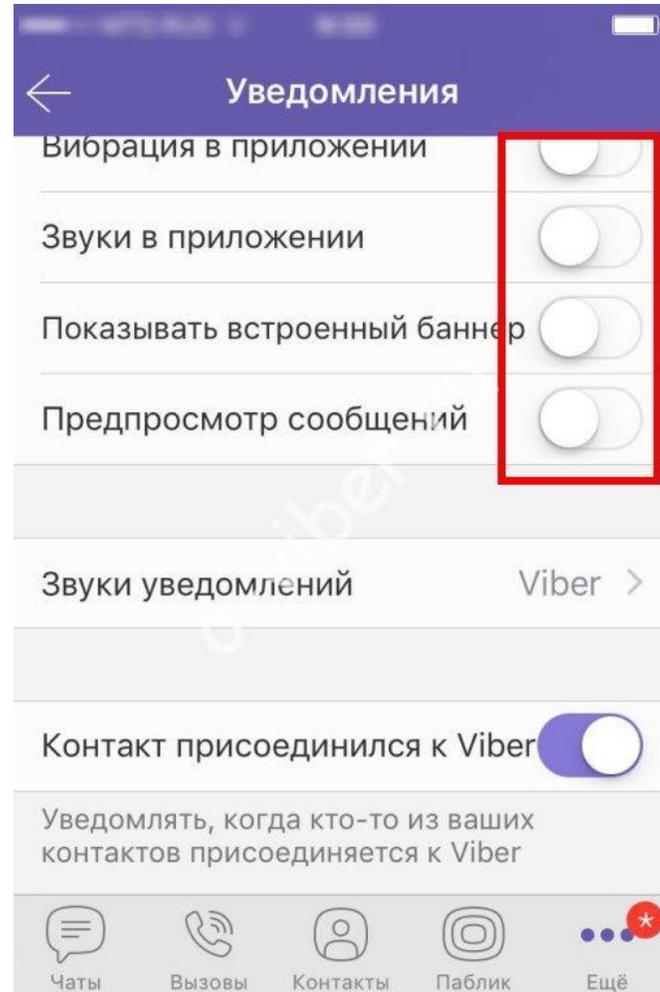
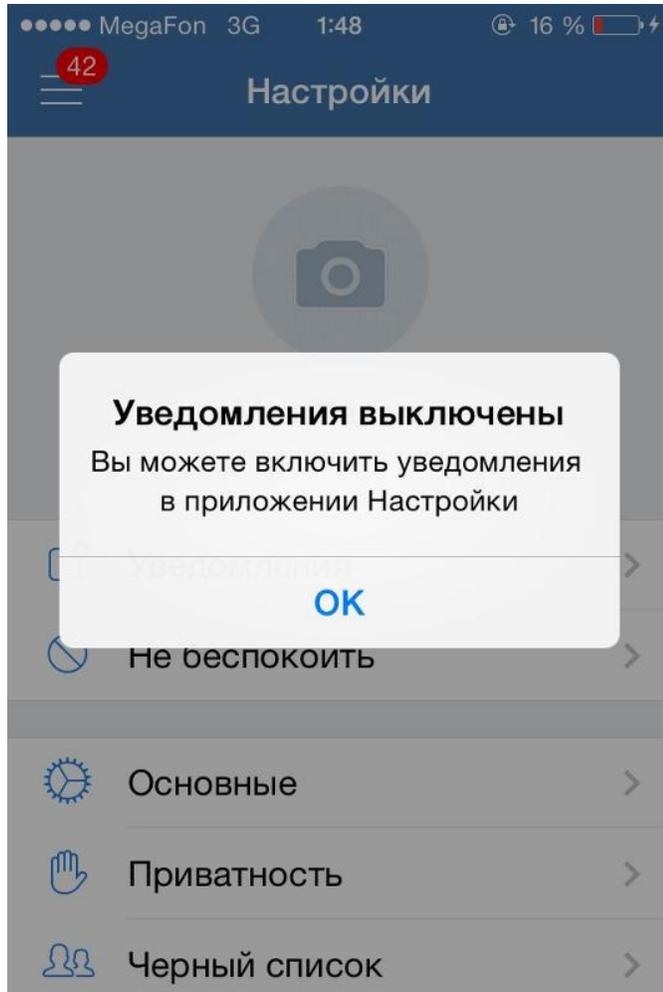
Как не стать жертвой онлайн-травли:

- Не ввязываться в глупые споры в сети
- Общаться только с тем, кому доверяешь
- Не воспринимать комментарии в интернете близко к сердцу
- Не делиться личной информацией с незнакомыми людьми

Что делать, если подросток подвергается онлайн-травле:

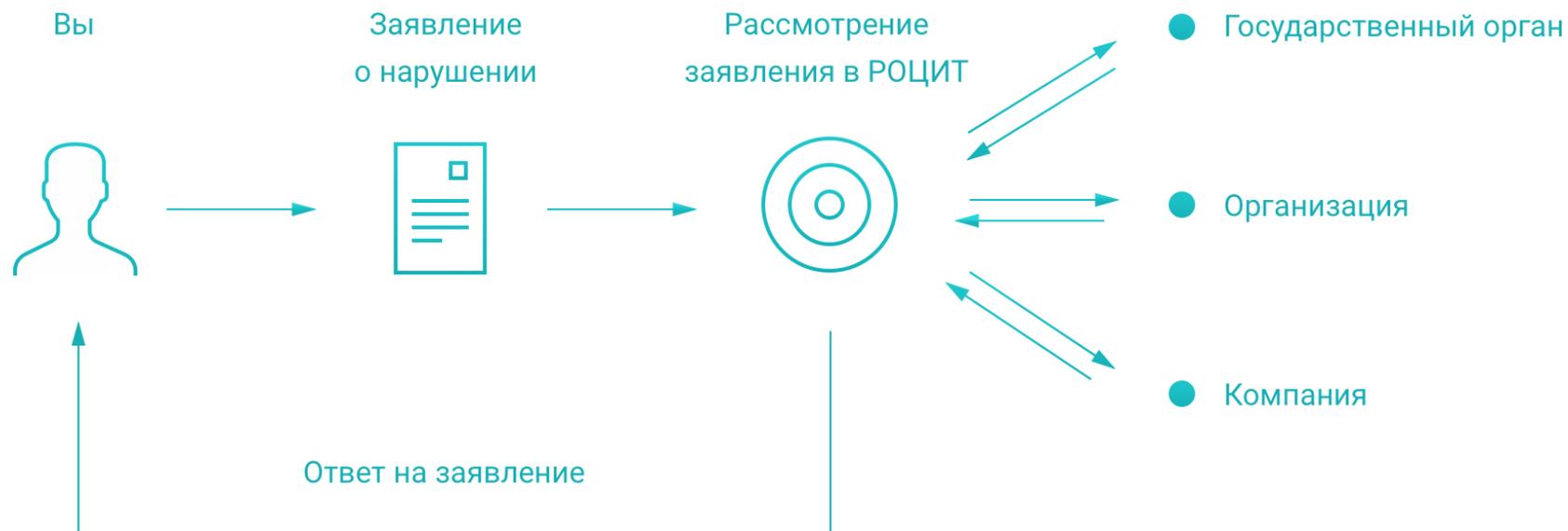
- Сохранять спокойствие
- Поделиться с близким человеком (родителями) и попросить помощь
- Не оставаться наедине с обидчиками
- Не пытаться мстить обидчикам самостоятельно

Как побороть гаджетозависимость



Горячая линия Рунета

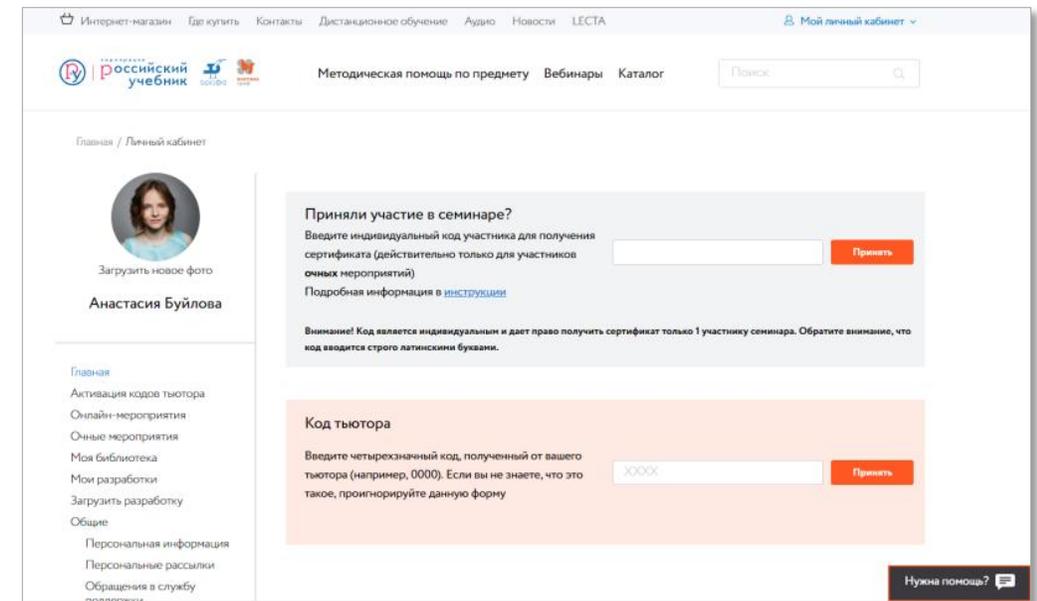
Горячая линия Рунета — это сервис защиты и информационной поддержки пользователей. Сообщайте о некачественном сервисе, противозаконных материалах и мошенничестве в интернете. Мы поможем!



<https://rocit.ru/hotline>

РЕГИСТРИРУЙТЕСЬ НА САЙТЕ ROSUCHEVNIK.RU И ПОЛЬЗУЙТЕСЬ ПРЕИМУЩЕСТВАМИ ЛИЧНОГО КАБИНЕТА

- Регистрируйтесь на очные и онлайн-мероприятия
- Получайте сертификаты за участие в вебинарах и конференциях
- Пользуйтесь цифровой образовательной платформой LECTA
- Учитесь на курсах повышения квалификации
- Скачивайте рабочие программы, сценарии уроков и внеклассных мероприятий, готовые презентации и многое другое
- Создавайте собственные подборки интересных материалов
- Участвуйте в конкурсах, акциях и спецпроектах
- Становитесь членом экспертного сообщества
- Сохраняйте архив обращений в службу техподдержки
- Управляйте новостными рассылками



rosuchebnik.ru, [росучебник.рф](http://rosuchebnik.ru)

Москва, Пресненская наб., д. 6, строение 2
+7 (495) 795 05 35, 795 05 45, info@rosuchebnik.ru

Нужна методическая поддержка?

Методический центр
8-800-2000-550 (звонок бесплатный)
metod@rosuchebnik.ru

Хотите купить?

 **book 24**

Официальный интернет-магазин
учебной литературы book24.ru



LECTA

Цифровая среда школы
lecta.rosuchebnik.ru



Отдел продаж
sales@rosuchebnik.ru

Хотите продолжить общение?



youtube.com/user/drofapublishing



fb.com/rosuchebnik



vk.com/ros.uchebnik



ok.ru/rosuchebnik