

"Презентация подготовлена для  
конкурса "Интернешка"  
<http://interneshka.org/>".

# БЕЗОПАСНАЯ РАБОТА В СОЦИАЛЬНЫХ СЕТЯХ



Работу выполнила  
ученица 10 класса  
МБОУ  
«Октябрьская  
СОШ»

Корицкая  
Кристина

# ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

Если Вы используете социальные сети, то должны заранее позаботиться о том, чтобы Ваши личные данные не попали в руки злоумышленников. Сегодня очень многие сервисы привязаны к номерам телефонов, и их утрата может обернуться для Вас существ...



# СЛЕДУЕТ

# ЗАПОМНИТЬ

- 1- При регистрации в соц.сетях используйте надежный пароль
- 2- Обращайте внимание на ссылки, по которым переходите
- 3- Никогда не публикуйте лишнюю информацию
- 4- Контролируйте информацию о себе
- 5- Не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты
- 6- Не добавляйте в «друзья» тех людей, которых Вы не знаете
- 7- Не регистрируйтесь в тех социальных сетях, которые не собираетесь использовать



# НЕСКОЛЬКО ВИДОВ СОЦИАЛЬНЫХ СЕТЕЙ

- Сервис закладок
- Библиотеки
- Многопользовательские игры
- Геоинформационные сети
- Профессиональные сети
- Сети определенных социальных групп
- Блоги
- Wiki
- IRC
- IM
- Интернет-форумы



# БЕЗОПАСНОСТЬ ПОДРОСТКОВ

*В последние годы в России тема безопасности подростков в сети Интернет стала активно обсуждаться, что дало возможность выявить некоторые характерные угрозы, что, практически, в полной мере характерно и для социальных сетей, как объективной реальности*



## *К числу таких угроз относятся:*

- сексуальная эксплуатация несовершеннолетних;
- склонение несовершеннолетних к сексуальным действиям (груминг);
- контент с признаками разжигания расовой, национальной, религиозной вражды, пропаганды тоталитарных сект;
- пропаганда и публичное оправдание терроризма;
- киберунижение и кибертравля;
- сцены физического насилия над несовершеннолетними;
- пропаганда и распространение порнографии;
- интернет-мошенничество и программно-



# АККАУНТ

## ПОЛЬЗОВАТЕЛЯ

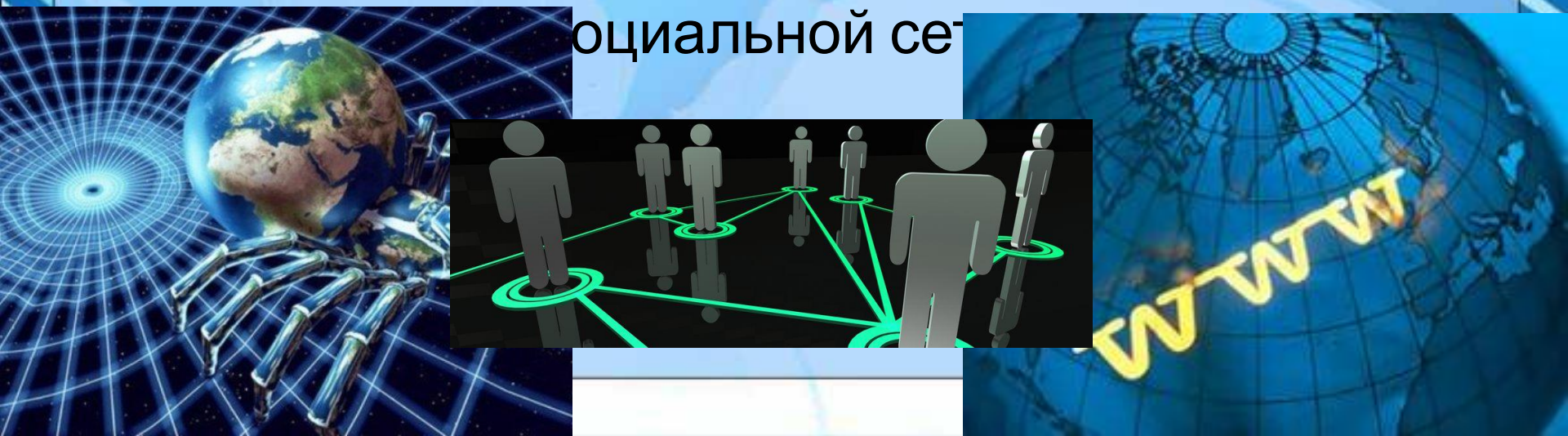
Что такое аккаунт пользователя в социальной сети?

- Учетная запись, которая может включать в себя адрес электронной почты подростка
- Реальные имя и фамилия пользователя
- Дата рождения
- Адреса: учебного заведения, домашний, точек интересов
- Контактные телефоны и «сетевые» контакты
- Фотографии, видеозаписи
- Перечень интересов, сообществ
- Друзья, посетители профиля



В связи с этим важно знать, что опираясь на эти общедоступные сведения любой человек может получить практически полную информацию о пользователе сети. На мой взгляд, здесь важно воспитание чувства privacy – ответственности за себя, свое личное пространство, в том числе пространство информационное. Человек должен очень четко понимать, какую информацию, в каком объеме и в каком сочетании можно размещать в

социальной сети





# ИНТЕРНЕТ – ТЕМНАЯ

## УЛИЦА

*Люди просто безудержно делятся личной информацией, доверяют сохранение паролей браузерам и ошибочно полагают, что Интернет — это нечто белое и пушистое.*

**Современный Интернет** – это некая темная улица, где вы можете столкнуться не только со случайными прохожими, но и с настоящими преступниками, которые без особого труда будут следить за вами на протяжении длительного времени, собирая личную информацию для последующей кражи или обмана.

**Интернет сегодня** – это гораздо больше, чем просто общение с друзьями, социальные сети, игры, онлайн-покупки. Это открытая система информации, и если кажется, что вам нечего скрывать или ваша информация никому не нужна, вы глубоко заблуждаетесь. Любая информация о вас может быть использована не теми, кому

# ВЕДЕТСЯ СЛЕЖКА!

Вы когда-нибудь замечали такую интересную особенность: если вчера обсуждали на форуме котиков, то сегодня у вас обязательно промелькнет информация о новых видах корма, если обсуждали новые девайсы, то ждите рекламы с предложениями купить новый смартфон и так далее, а ведь это самый безобидный пример слежки за вами со стороны маркетинговых агентств.



# БУДЬТЕ БДИТЕЛЬНЫ!

- 1) Не доверяйте предложениям от спамеров.
- 2) Не переходите по ссылкам присланным незнакомцами.
- 3) Не оставляйте личные данные на малоизвестных сайтах.
- 4) Не участвуйте в сомнительных интернет-лотереях.
- 5) Используйте лицензионное ПО для защиты своего ПК.



**СПАСИБО ЗА  
ВНИМАНИЕ!**

