УНИВЕРСИТЕТ ЛОБАЧЕВСКОГО
НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кибербезопасность молодёжи

Соболева Анна Владиславовна,
к.соц.н, доцент кафедры отраслевой и прикладной социологии ФСН ННГУ

JUL 2019

СОЦИАЛЬНЫЕ СЕТИ В МИРЕ

SOURCES: LATEST DATA PUBLISHED BY SOCIAL MEDIA PLATFORMS VIA PRESS RELEASES, INVESTOR EARNINGS ANNOUNCEMENTS, AND IN SELF-SERVE ADVERTISING TOOLS; ARAB SOCIAL MEDIA REPORT; TECHRASA; NIKI AGHAEI; ROSE.RU; KEPIOS ANALYSIS (ALL TO JULY 2019).

Hootsuite™ we are social

Кратко в цифрах

•Абсолютное большинство опрошенных школьников старше 14 лет, школьных учителей и родителей учеников 1-11 классов пользуются мобильными мессенджерами (96%, 96%, 95% соответственно).

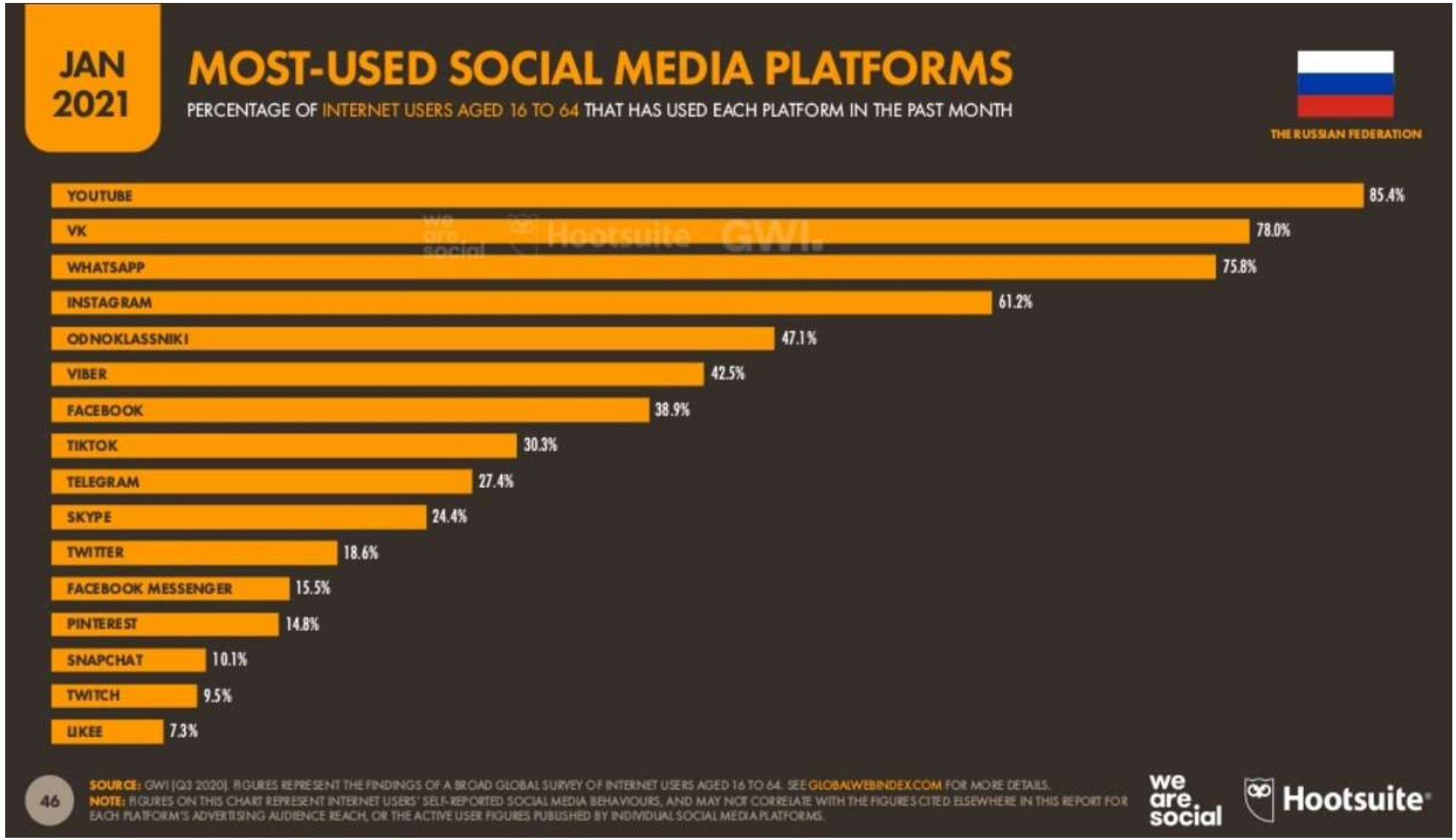
•Ежедневно в школьных чатах общаются 86% учителей, 71% школьников и 59% родителей.

•Для большинства опрошенных целевых аудиторий мессенджеры являются основным (доля согласных — 80-87%) и самым удобным (82-89%) каналом коммуникации по школьным вопросам.

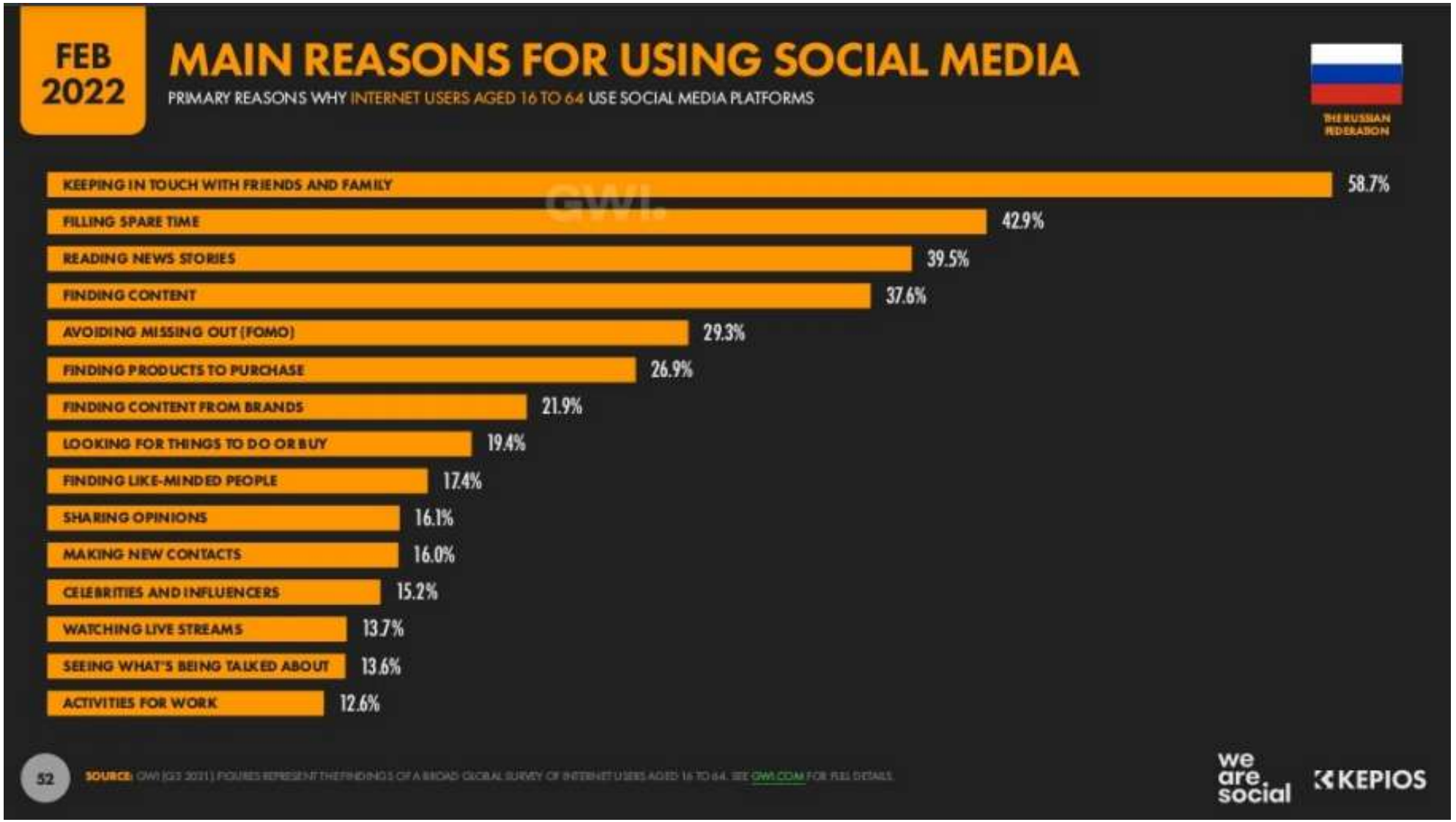
•В топ-3 самых популярных мессенджеров у школьников вошли «ВКонтакте» и/или «VK Мессенджер» (62%), Telegram и WhatsApp (58% и 55% соответственно). Четвертую и пятую строчки заняли Viber (14%) и TikTok (5%).

**По результатам опроса ВЦИОМ, 21-27 октября 2022 года https://wciom.ru*

Популярность соцсетей в России



Причины использования соцсетей



Функции и преимущества сети

1.Возможность общения на больших расстояниях.

2. Возможность найти друзей, знакомых, одноклассников.

3. Организация досуга, заполнение свободного времени.

4. Поиск единомышленников.

5. Самовыражение путём выкладывания результатов своей работы и творчества.

6. Поиск познавательной информации.

7. Дистанционное обучение.

8. Возможность трудоустройства и работы в сети.

Что угрожает молодёжи в интернете

1. Взлом аккаунта.

   Если не защищать аккаунты, злоумышленники могут взломать их и использовать личную информацию. Например, шантажировать пользователя фотографиями, фактами из переписки или рассылать от его лица просьбы о помощи или спам. Кража игрового аккаунта может нанести урон подросткам, увлечённых играми и киберспортом.

2. Сбор личной информации.

   Некоторые подростки делятся на своих страницах в соцсетях подробностями частной жизни, чтобы произвести впечатление на друзей, рассказать о своей обыденной жизни или достижениях. И иногда мы забываем, например, о том, что опубликованные фото квартиры с дорогой техникой могут привлечь грабителей, а фото из отпуска подскажут им, когда никого не будет дома.

Что угрожает молодёжи в интернете

3. Фишинг (phishing, whaling).

Использование поддельных ссылок. Мошенники могут использовать доверчивость молодёжи и вынудить их перейти по фишинговым ссылкам на сообщения с информацией о выигрыше, выгодном предложении и т. д. Злоумышленники создают поддельные сайты, чтобы похищать логины, пароли, платёжные данные. Также при переходе по фишинговой ссылке может загрузиться программа, которая заразит компьютер или гаджет вирусом.

4. Кибербуллинг.

Травля в интернете. В цифровом пространстве молодые люди могут подвергаться травле. Обидчик может быть анонимным, поэтому его сложно вычислить. Кроме того, виртуальные издевательства происходят в личной переписке и родители могут не узнать, что ребёнка преследуют. Последствия кибербуллинга для детей сравнимы с реальной травлей: негативные эмоции, депрессия, проблемы с учёбой и взаимоотношениями.

По данным корпорации «Крибрум» в кибербуллинг вовлечены 3 494 500 подростков.

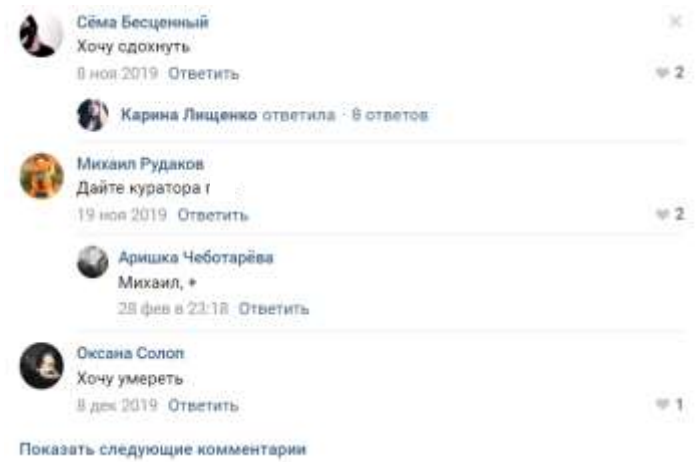
Что угрожает молодёжи в интернете

5. Формирование тревоги и чувства одиночества.
6. Паника на фоне прочтения новостей.
7. Рассылка откровенных фото, секстинг.
8. Подталкивание к суицидальному поведению.

   По данным ВОЗ средний показатель самоубийств среди российских подростков – 19-20 случаев на 100 тыс.чел. Это больше среднего показателя в мире в 3 раза.

9. Распространение деструктивного и экстремистского контента, вовлечение в экстремистскую деятельность.

   По данным МВД на учёте стоят свыше 450 молодёжных группировок экстремистской направленности численностью около 20 000 человек. В деструктивные сообщества вовлечены около 70 000 российских подростков.



Предотвращение фишинга и использования личных данных

1. Не открывать подозрительные ссылки и вложения, всегда проверять адреса сайтов, на которых вводятся данные.
2. Проверять имя и домен, с которого отправляется электронное письмо.
3. Проверить на орфографические ошибки, которые зачастую выдают подделку.
4. Поля «От» и «Кому» не должны быть обезличены. Если это так, это массовая рассылка.
5. Не сообщать в письмах и на сайтах учётные данные.
6. Подозрительно относитесь к требованиям «срочно» и «немедленно», они побуждают действовать сразу, не задумываясь.
7. Обратите внимание на нижний колонтитул, в нём часто содержатся явные признаки подделки.

Предотвращение фишинга и использования личных данных

8. Не открывать вложения и подозрительные ссылки, особенно сокращённые при помощи bit.ly или аналогичной службы. Имитацию рассылки от настоящих сервисов или интернет-магазинов можно определить по некорректному адресу отправителя. Он может отличаться от него одной или двумя буквами, например admin@notify.wk.com вместо admin@notify.vk.com
9. Не реагируйте на шантаж и угрозы о распространении каких-либо личных фото и видео.

Распознавание фейков и снижение информационного давления

1. Читайте новость целиком, а не только громкий заголовок.
2. Изучайте источник новости и автора, по необходимости найдите первоисточник.
3. Убедитесь, что читаете реальное медиа, а не фейк-аккаунт для вбросов.
4. Проверяйте информацию незнакомых аккаунтов в соцсетях, особенно при репостах.

Распознавание фейков и снижение информационного давления

4. Оцените предвзятость и заинтересованность автора.
5. Обратите внимание на грамотность текста.
6. Не стоит слепо доверять фото и видео.
7. Проверить информацию в разных источниках.

Основные правила безопасности в сети

1. Использовать надёжные пароли.
2. Подключить двухфакторную аутентификацию.
3. Настроить приватность в соцсетях.
4. Блокировать пользователей, которые пишут негативные комментарии.
5. Не переходить по ссылкам из подозрительных сообщений (фишинг).
6. Не публиковать в соцсетях информацию, которая может быть полезна преступникам.
7. Не общаться с незнакомыми людьми.
8. Не пользоваться важными приложениями при подключении к бесплатным wifi сетям.
9. Не провоцировать агрессию и не отвечать на неё.

УНИВЕРСИТЕТ ЛОБАЧЕВСКОГО

Спасибо за внимание!