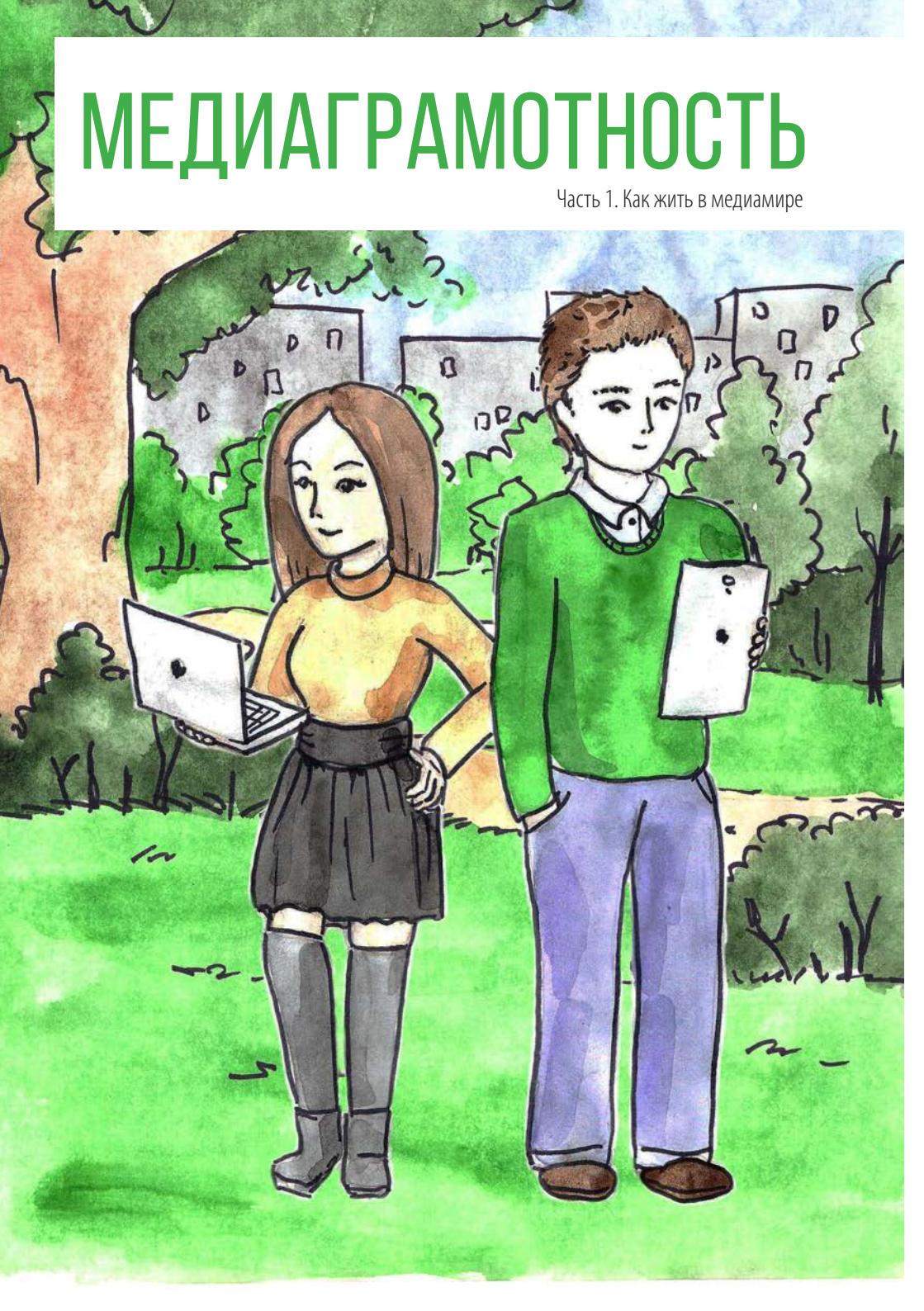
МЕДИАГРАМОТНОСТЬ

Часть 1. Как жить в медиамире



Автор: к.пед.наук. Денис ДУБОВЕР.

Редактор: Анастасия КУЗЁМА.

Иллюстрации: Марина БАСАЙ, Александр БЕЛОДЕД, Кристина ЕСИКОВА.

Дизайн и верстка:
Илья ДУДАКОВ, Андрей ЮРЧЕНКО, Валерия БЕССМЕРТНАЯ.

Донской государственный технический университет, Областной центр медиаграмотности. Ростов-на-Дону, 2015 г.

Пособие по медиа-информационной грамотности ориентировано как на широкий круг читателей, так и на студентов профильных факультетов медиакоммуникаций и журналистики и изучающих такие дисциплины, как «Медиа-информационная грамотность», «Культура медиапотребления». Первая часть пособия «Медиаграмотность: жизнь в медиамире» рассказывает об универсальных и эффективных способах работы с информацией разного уровня. Это и понимание новостных и информационных сообщений СМИ, и социальных медиа, умение эффективно и безопасно находиться в информационной среде социальных сетей, находить и критически осмысливать источники информации, работать с электронными финансами, противостоять угрозам глобальной медиасферы. Кроме этого, в пособии уделяется особое внимание проблеме детского интернета и «родительского контроля» над медиаповедением детей и подростков.

Все упоминания коммерческих продуктов, брендов и услуг не являются рекламой.

Благодарность за помощь в работе над пособием студентам факультета «Медиакоммуникации и мультимедийные технологии» Донского государственного технического университета:
Крицкой Анастасии, Нагаевой Ксении, Требухину Андрею, Цыганкову Олегу, ХорунжемуЭдварду, Орлову Константину, Литвинову Илье, Вербицкому Владимиру, Диброву Александру, Дубенцовой Елизавете, Антонову Антону.

ДГТУ

ОБЛАСТНОЙ ЦЕНТР МЕДИАГРАМОТНОСТИ

медиапарк
ЮЖНЫЙ РЕГИОН

содержание

1. Социальные сети **6**

2. Новостная грамотность **22**

3. Почтовые сервисы **30**

4. Облачные хранилища **44**

5. Электронные финансы **48**

6. Родительский контроль **54**

7. Digital-экология **66**

Вы держите в руках пособие по медиа-информационной грамотности. Его цель показать оптимальные способы жизни в информационном пространстве. Ключевые вопросы, которые рассматриваются на страницах пособия, – это безопасность работы в сети Интернет, сетевой этикет, умение критически воспринимать медиаконтент, проверять новостные сообщения, одним словом, быть полноценным и полноправным участником современной медиажизни, которая охватывает каждого из нас. И поэтому необходимо научиться управлять медиа, иначе медиа начнет управлять нами. Эти правила игры сегодня уже нельзя изменить. Но можно научиться жить и не дистанцироваться от медиа, а использовать его на все 100!

Стремительное развитие информационных и коммуникационных ресурсов, возрастающая доступность медиасредств (в первую очередь, смартфонов и планшетных компьютеров) открывают практически безграничные возможности для доступа к информации самого разного уровня, в том числе и к запрещенному контенту порнографического, экстремистского, дезинформирующего характера. Контролировать этот процесс крайне трудно. Кропотливая работа по запрету доступа к ресурсам сети Интернет, содержащим вредоносный контент, не может полностью обеспечить информационную безопасность Вам и Вашим детям, поскольку, когда блокируешь одни каналы, открываются другие. В условиях демократического общества невозможно полностью ограничить доступ к нелицензируемым и нелегитимным веб-ресурсам, сохранив право посещения только проверенных источников.

При этом представляется возможным формирование механизмов критической оценки данного контента, умения отличать настоящие новости от ненастоящих, проверять информацию, противостоять манипулятивному воздействию экстремистских организаций, призывающих к дестабилизации социально-политической жизни государства, формировать медиаповедение, направленное на конструктивное и всестороннее развитие.

Обучение медиа-информационной грамотности состоит из множества компонентов. Это умение работать с различной информацией, создавать и интерпретировать медиатекст, владеть навыками работы с современными медиакоммуникационными устройствами – гаджетами и девайсами, осознанно выбирать тот или иной медиаконтент, критически его осмысливать, интерпретировать и использовать для дальнейшего синтеза новой медиапродукции в блогах, социальных сетях или традиционных масс-медиа. Кроме того, медиакомпетентность в современном мире может стать важным инструментом в превенции негативных последствий техногенных катастроф, стихийных бедствий, а также предотвращения действий террористических группировок.

ПОСОБИЕ СОСТОИТ ИЗ СЕМИ РАЗДЕЛОВ:

Социальные сети. Социальные медиа. Коммуникаторы

Возможности и опасности социальных сетей и социальных медиа.
Как отличить фейк от оригинала.
Киббермобинг.
Правила поведения в социальных сетях.

Новостная грамотность

Сила информации: зачем нам нужны новости.
Журналистика фактов и журналистика мнений.
Проверка фактов и поиск истины.
Алгоритм оценки источников.
Механизм разбора новостей.

Почтовые сервисы. Облачные хранилища

Работа с почтовыми сервисами (Яндекс.Почта, Google, Rambler, Mail.ru).
Правила сетевого этикета и деловой корреспонденции.

Электронные финансы

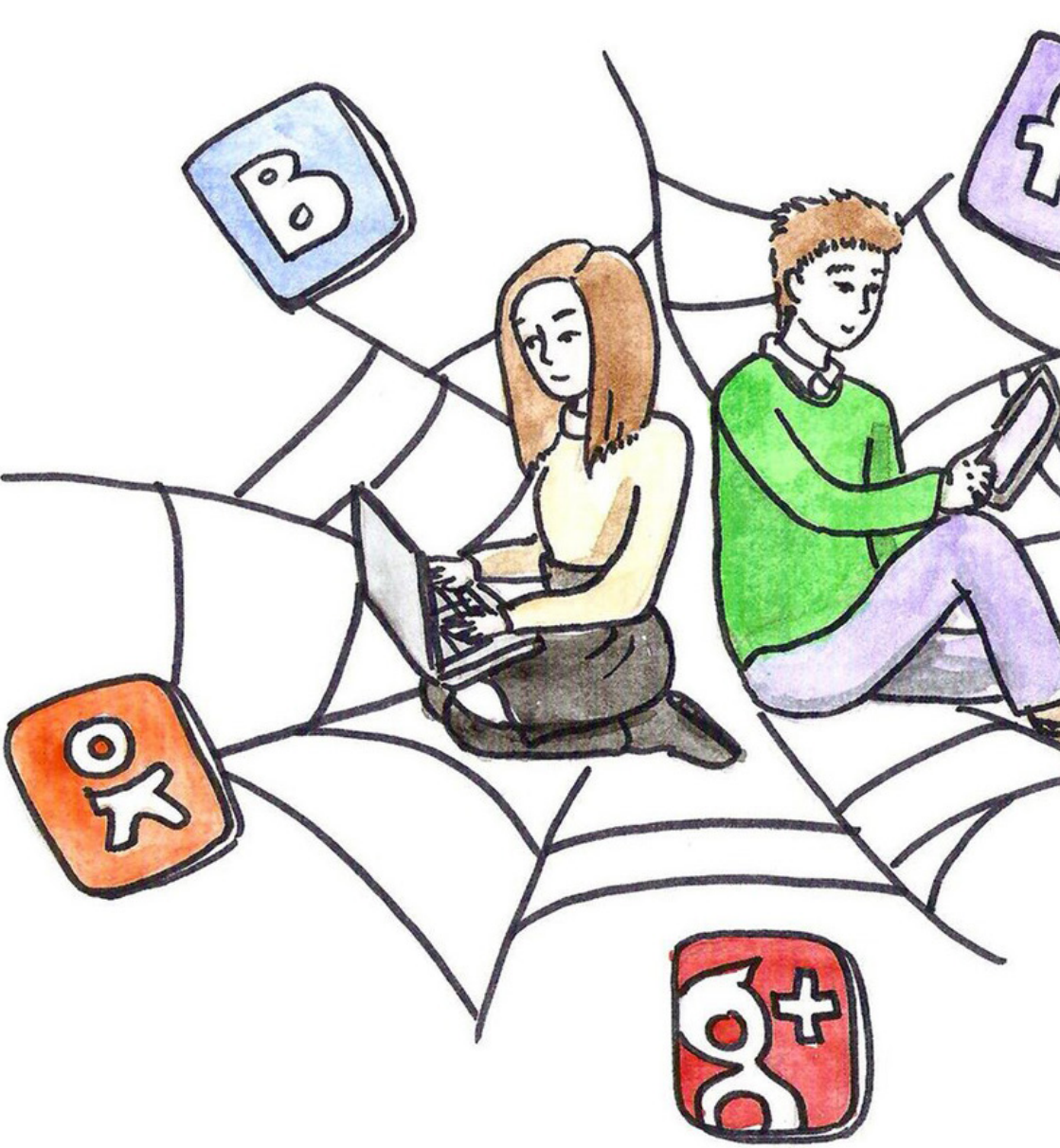
Электронная коммерция.
Мобильный банкинг (преимущества).
Правила безопасного пользования кредитными картами в сети Интернет.

Родительский контроль

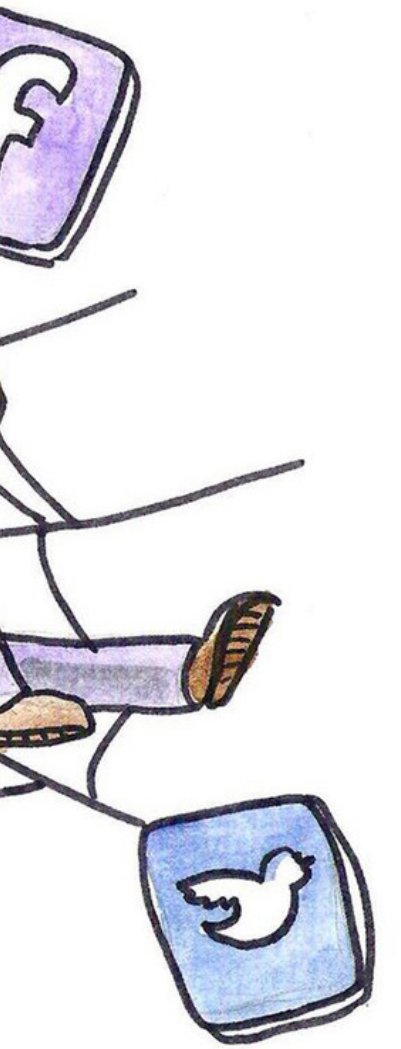
Приложения для обеспечения безопасного доступа детей в интернет.
Детский интернет.
Безопасность работы со смартфонами.
Правила для детей.

Digital-экология

Интернет-зависимость.
Чем опасна интернет-зависимость и как ее избежать?
Как жить в гармонии с медиа?



1 СОЦИАЛЬНЫЕ СЕТИ



СОЦИАЛЬНЫЕ СЕТИ

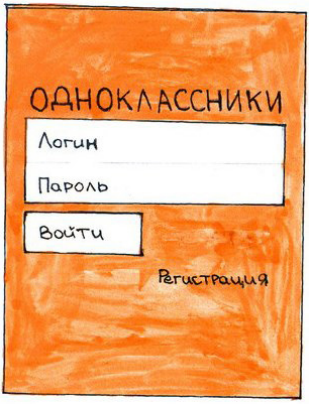
Социальные сети сегодня стали для нас больше, чем просто среда общения и обмена фотографиями. Простота работы со своими страничками со смартфонов и планшетов, недорогие тарифы для подключения мобильного интернета и доступный wi-fi позволяют быть on-line всегда и везде, а социальные сети превращаются в устойчивую привычку, без которой мы уже не можем представить современную жизнь.

Но легкая доступность сетей создает новые возможности и новые угрозы как для активных пользователей, так и для тех, кто проверяет свои «странички» один раз в день или даже реже.

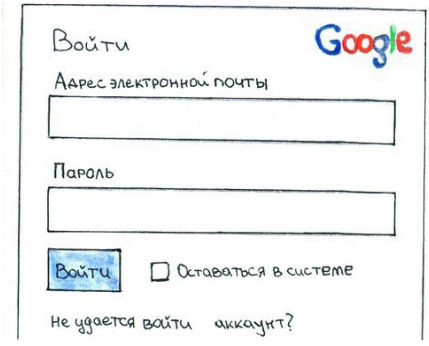
Социальных сетей и социальных медиа с каждым днем становится все больше и все труднее выбрать какую-то одну для удовлетворения всех медийных потребностей. Но разбираться в них необходимо, чтобы избежать лишних трудностей и нежелательных последствий.

vk.com – самая популярная в России и крупнейшая в Европе социальная сеть. Изначально «Вконтакте» позиционировала себя как социальная сеть, предназначенная для общения и обмена информацией студентов и выпускников вузов, позднее аудитория стала более разнообразной. «Вконтакте» позволяет общаться со своими друзьями, обмениваться и делиться фотографиями, аудио-, видеофайлами и другими документами, отмечать («лайкать») понравившиеся материалы, играть в мини-игры, а также создавать и вступать в группы по интересам.

facebook.com – одна из самых первых социальных сетей в мире. По аналогии с «Вконтакте» позволяет общаться с друзьями и обмениваться медиафайлами.



odnoklassniki.ru – в отличие от vk.com и facebook.com «Одноклассники» пользуются популярностью у более старшей аудитории.



google+.com – проект поискового гиганта Google. Новая альтернативная социальная сеть, которая пока еще не пользуется особой популярностью. Однако она удобна для пользователей смартфонов на платформе Android, поскольку Вы сможете войти во все сервисы Google с помощью одного и того же аккаунта и пароля, а также сделать синхронизацию более удобной для всех сервисов между собой.

СОЦИАЛЬНЫЕ МЕДИА И КОММУНИКАТОРЫ

Помимо социальных сетей в жизни каждого большую роль играют социальные медиа. Самые популярные из них – это:

Twitter – нужен для публичного обмена короткими сообщениями. Максимальная длина такого сообщения составляет 140 символов. К ним можно прикрепить картинку или фотографию. Публикация таких текстовых заметок называется «микроблоггингом».

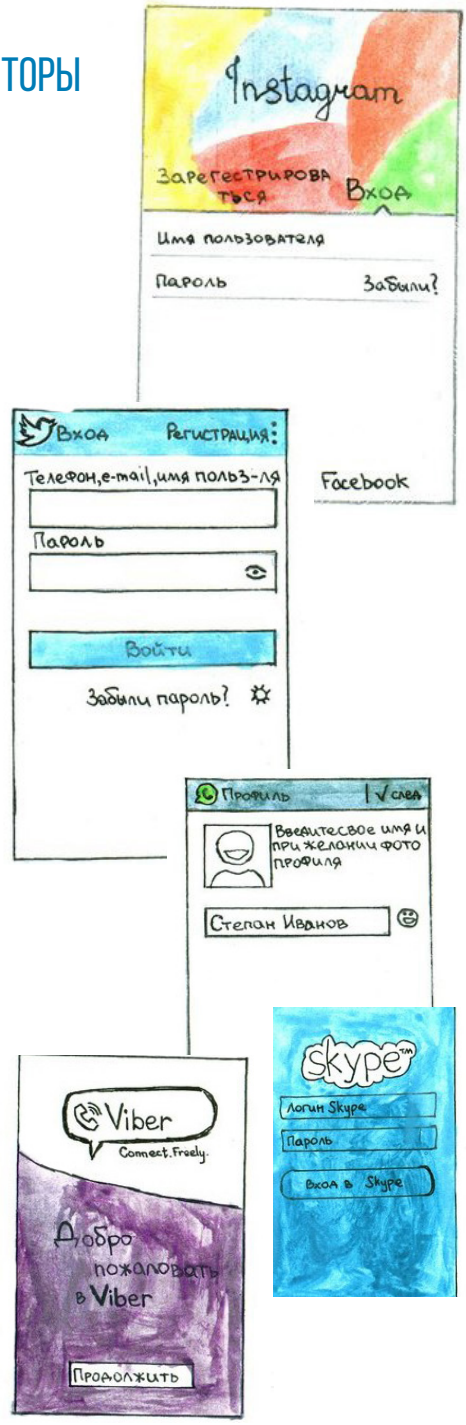
Instagram – бесплатный сервис обмена фотографиями и короткими видеозаписями. Приложение позволяет фотографировать и снимать видео на свой девайс, редактировать, а также накладывать различные фильтры и эффекты.

Foursquare – программа по обмену мнениями о местах и заведениях. Ориентируется на вашу геолокацию. Для того чтобы получить информацию или отзыв о каком-либо месте, нужно просто отметиться («зачекиниться»), и сервис даст рекомендации о данном заведении и покажет интересные места неподалеку.

Whatsapp – приложение для обмена короткими сообщениями между двумя и более пользователями. Заменяет классические sms/mms сообщения. Привязывается к номеру мобильного телефона пользователя.

Viber –позволяет совершать аудиозвонки через интернет и обмениваться мгновенными сообщениями. Так же, как и Whatsapp, привязывается к номеру.

Skype – программа позволяет совершать не только аудио-, но и видеовызовы. Требуется лишь подключение к интернету и камера.



КАК ОТЛИЧИТЬ ФЕЙК ОТ ОРИГИНАЛА

В контексте социальных сетей фейками называют поддельные страницы реальных людей с идентичными фотографиями и данными. Чаще всего фейковые страницы создают под профайлы известных людей. Как же отличить фейк от оригинала? Существует несколько признаков фейковых страниц.

1. Фотографии, «вырванные» из других социальных сетей или поисковых сервисов. Когда Вы выкладываете фотографию, многие социальные сети помечают её своим логотипом и скачать ее из сервиса без него невозможно. Также при скачке таких фото теряется качество изображения. Если Вы заметили, к примеру, что в профайле «вконтакте» много фотографий из «одноклассников» и качество оставляет желать лучшего, вполне вероятно, что страница фейковая.

2. «Пустой» профайл. Обычно создатели фейковых страничек не особо стараются повторить оригинал: не указывают личную информацию, интересы и так далее. Если никаких данных, кроме имени, не указано, стоит насторожиться.

3. В общении с другими людьми обладатель фейковой страницы обычно пишет общими фразами, никогда не указывает детали.

4. Если страница создана пару дней назад, а все фотографии загружены одной датой – это тоже, вероятнее всего, фейк.

5. От фейков приходит много спама, так как многие мошенники создают такие странички для накрутки голосов или приглашения людей в свои ресурсы.

6. Первые 100 друзей у фейка обычно реальные люди, поэтому, если вы решили проверить липовая страница или нет, просмотрите всех друзей в ленте.

7. Если указана школа/университет и год окончания, то проверьте, есть ли в друзьях у человека люди из этой школы. Напишите им, спросите, знакомы ли они с человеком лично.

8. Посмотрите записи на стене и найдите первую. Когда она была сделана? Чем старше аккаунт, тем выше вероятность, что он подлинный.

Страничка в социальных сетях – это мощный инструмент формирования имиджа человека, поэтому так необходимо внимательно относиться к тому, как она выглядит. Но как найти эту грань между излишней скрытностью и чрезмерным хвастовством? Ведь сегодня принято встречать человека по аватарке, а провожать по контенту страницы.

Медиамир стал настолько реальным, что мы воспринимаем страницу человека, как его самого. Смотрим на записи и делаем выводы.

Если у Вас «открытые» аккаунты в социальных сетях, то нужно понимать, что информацию в них может увидеть любой пользователь.

В связи с этим, важной проблемой становится эмоциональная зависимость от социальных сетей и излишняя откровенность. Большинству пользователей зачастую трудно удержаться от соблазна рассказать о приобретении машины, квартиры, повышении на работе, путешествии или утреннем кофе.

Контент страницы – личная информация, контакты, фотографии, геолокация – позволяет узнать Ваше окружение, интересы и виды активности. Визуальный контент обычно проходит внутреннюю модерацию, позволяет оценить уровень уверенности, смелости и адекватности.

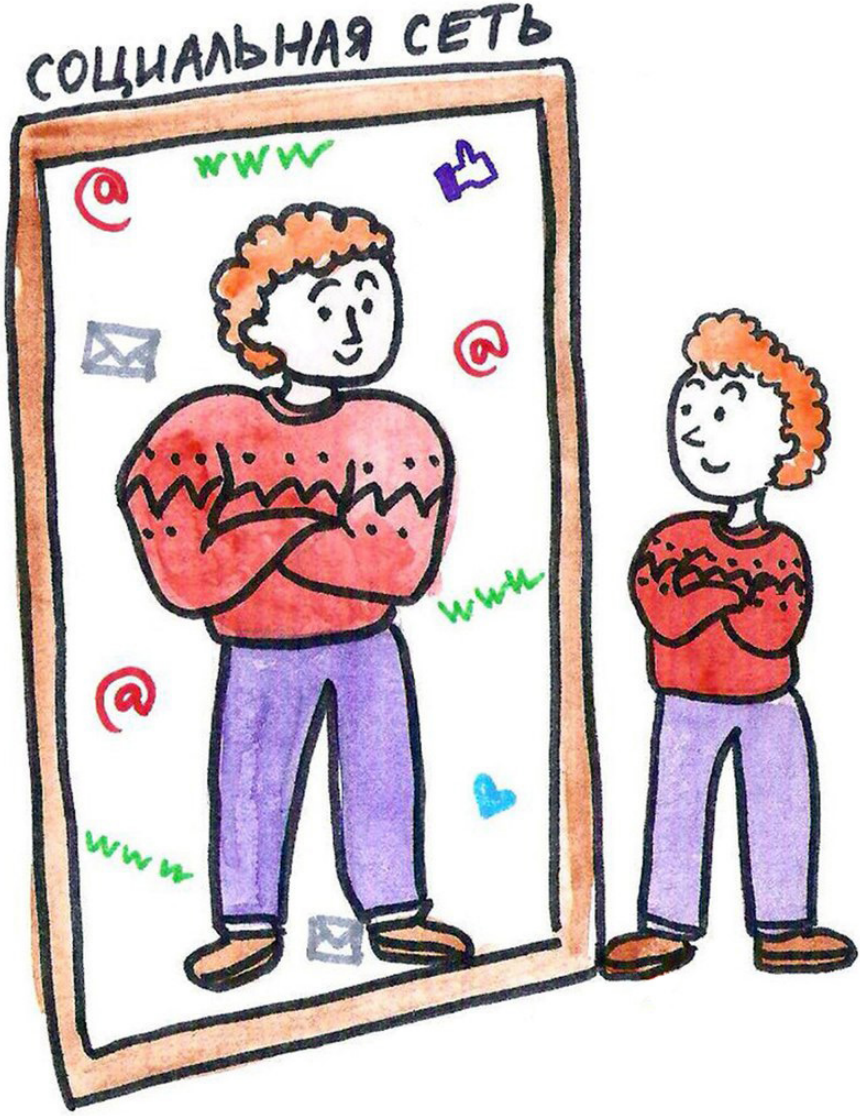
Мы не призываем Вас оставлять аккаунты пустыми, но не стоит забывать о настройках приватности.

При этом важно заметить, что быть и казаться – разные понятия. То, что демонстрируется в социальных сетях, не всегда соответствует реальности.

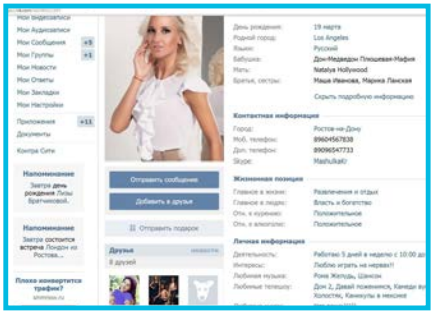
Нельзя забывать, что в современном мире социальные сети – это ваше лицо. И если Вы хотите произвести хорошее впечатление, оставляйте все самое личное «под замком».

ВСТРЕЧАЮТ ПО АВАТАРКЕ, А ПРОВОЖАЮТ ПО КОНТЕНТУ

НЕ СТАРАЙТЕСЬ ПОКАЗАТЬСЯ В СЕТИ ЛУЧШЕ, ЧЕМ ВЫ ЕСТЬ



КАКОЙ НЕ ДОЛЖНА БЫТЬ СТРАНИЧКА В СОЦ. СЕТЯХ



Не стоит использовать чужую фотографию в качестве аватарки для своей странички. Герой «украденного» кадра может пожаловаться в администрацию соц.сети, и Ваш аккаунт заблокируют.

Указывайте настоящее имя. «Псевдонимы» могут негативно характеризовать Вас в глазах коллег и будущих работодателей.

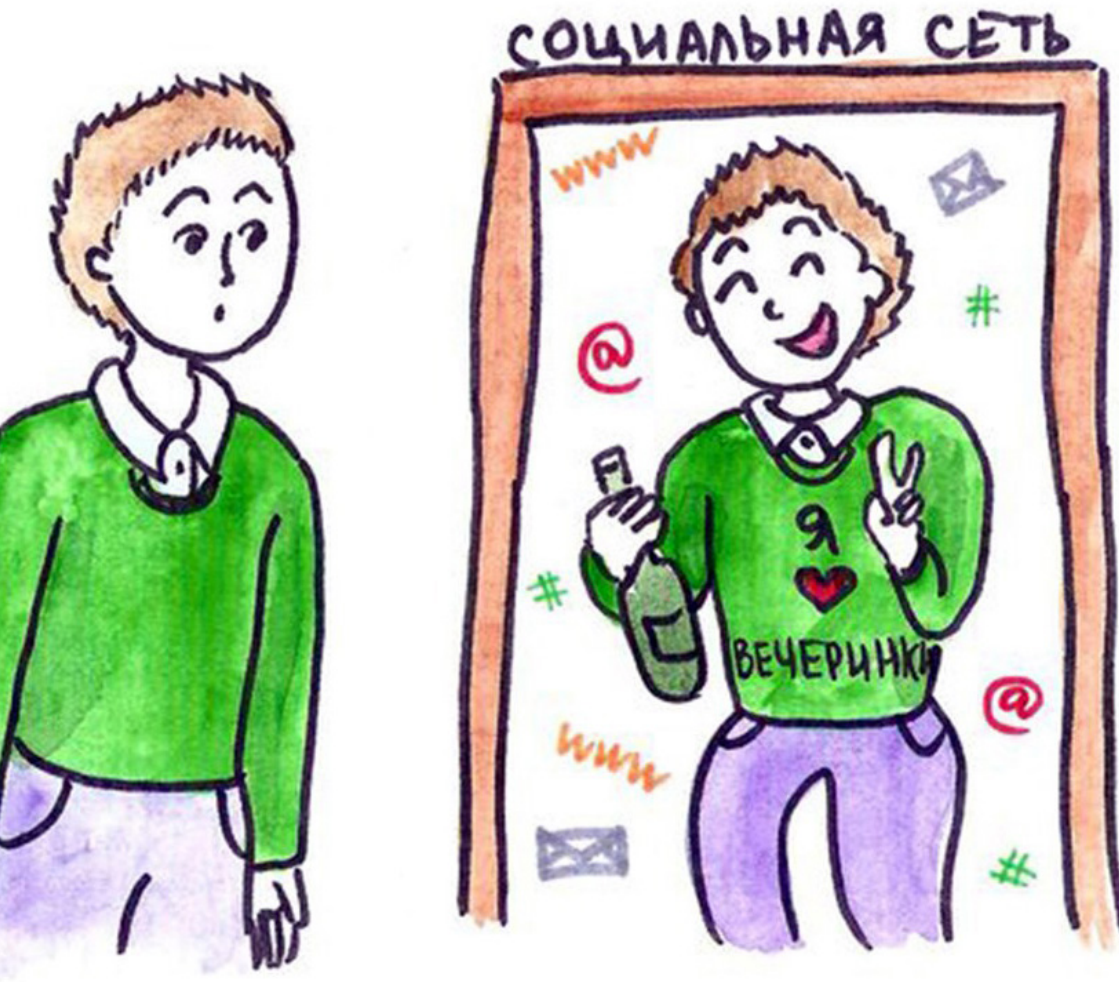
Не размещайте персональные данные, которые могут Вас скомпрометировать или стать причиной для излишнего беспокойства.

Уделяйте значение тому, о чем Вы пишете на странице, и тем репостам, которые делаете из пабликов и со страниц своих друзей. Они также работают на Ваш имидж.

С особым вниманием заполняйте поля Вашей карьеры: слишком быстрая смена работы может стать причиной отказа при конкурсе на желаемую должность. Сегодня работодатели уделяют особое внимание Вашему образу в сети: если он негативный и может причинить вред репутации компании, Вы можете просто не дойти до собеседования.

Не забывайте об этом и всегда смотрите на Вашу страничку со стороны.

Вы можете рассмотреть страничку в полном объеме по следующему id в соц.сети «Вконтакте». vk.com/id208522397



«Нет смысла надеяться, что другие оценят Вас за Ваш характер и личность, не обратив внимания на то, как Вы выглядите». **Трейси Б.**

«То, как ты выглядишь, заглушает то, что ты хочешь сказать». **Эмерсон Р.**

КИБЕРМОББИНГ

Пользователи социальных сетей все чаще сталкиваются с кибермоббингом. Кибермоббинг - это использование средств электронной коммуникации для унижения и оскорбления других людей. Иначе говоря, кибермоббинг – это социальное давление, перенесенное в плоскость электронного общения.

Кибермоббинг осуществляется посредством электронной почты, социальных сетей, программ для мгновенного обмена сообщениями, размещения на порталах, а также посредством мобильного телефона, через SMS-сообщения.

ВИДЫ КИБЕРМОББИНГА:

Оскорбление Происходит посредством оскорбительных комментариев и вульгарных обращений, происходящих в публичном пространстве интернета.

Домогательство Кибер-атаки от незнакомцев, адресованные конкретно Вам.

Клевета Выставление жертв в неблагоприятном свете с помощью фото-видеоматериалов.

Использование фиктивного имени Выдавать себя за другого человека, используя пароль жертвы.

Публичное разглашение личной информации Распространение личной информации для шантажа или оскорбления жертвы.

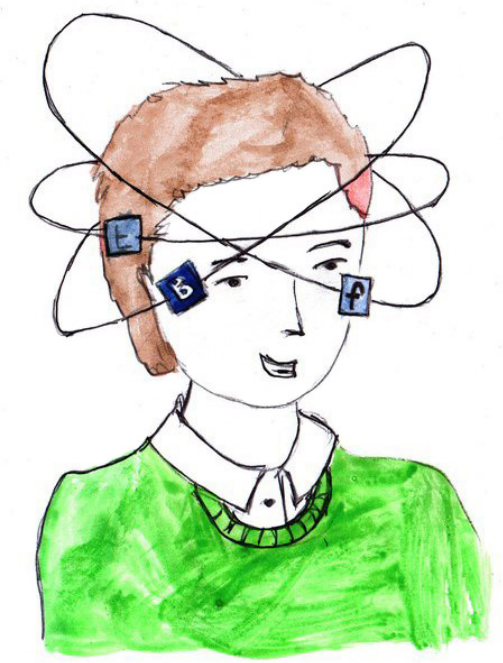
Угроза физической расправы Угрозы причинения телесных повреждений и угрозы убийства.

Продолжительное домогательство и преследование Продолжительное (сексуальное) преследование жертвы, которое сопровождается домогательствами и угрозами.

Иллюстрация: Томас Плассман

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОББИНГА, ВОСПОЛЬЗУЙТЕСЬ СЛЕДУЮЩИМИ ПРАВИЛАМИ:

1. Не выкладывайте в сеть лишнюю информацию или медиафайлы, которые могут компрометировать Вас или Ваших знакомых. Также не стоит отправлять такую информацию людям, которые не вызывают доверия.
2. Не вступайте в словесные перепалки в комментариях, на форумах, в беседах. У комментаторов может появиться желание мести.
3. Игнорируйте сообщения, в которых Вас оскорбляют, унижают или угрожают. Также стоит уведомить о таких сообщениях администрацию сайта или сервиса.
4. Не угрожайте хулигану «найти и наказать». Это лишь спровоцирует его на продолжение социального давления и усугубит ситуацию.
5. Удалите злоумышленника из социальных сетей, заблокируйте доступ к Вашей странице, добавьте в черный список.
6. Не присоединяйтесь, если Ваши друзья дразнят кого-то в сети. Попросите их остановиться, предупредите о вредных последствиях кибермоббинга.
7. Чаще меняйте пароли в социальных сетях, так как злоумышленники могут писать от Вашего имени.



СОЗДАЕМ СВОЮ «СТРАНИЧКУ»

Для того, чтобы зарегистрироваться в любой социальной сети, Вам понадобится адрес электронной почты. Указывайте существующий email, так как с помощью него Вам нужно будет подтвердить Вашу личность. Обычно администрация сайта присылает письмо с ссылкой, по которой нужно пройти для завершения регистрации.

Иногда помимо электронной почты для регистрации нужно придумать логин, который впоследствии будет являться Вашим именем в сервисе.

Как и в создании почты, здесь главная часть регистрации – это пароль. Пароль не должен быть слишком простым, иначе его будет легко подобрать, и тогда персональные данные могут попасть в руки злоумышленников. Не указывайте в качестве пароля дату своего рождения, используйте помимо цифр буквы с разным регистром.

После регистрации Вам будет предложено заполнить профиль: указать краткую информацию о себе, дату рождения, интересы, место работы/учебы и так далее. Также Вы можете загрузить фотографию профиля – аватар. Не стоит указывать личные данные и размещать фотографии, которые в дальнейшем могут Вас скомпрометировать: по информации на страничке будет создаваться первое впечатление. Как говорится: «Встречают по аватарке, а провожают по контенту».

ОСНОВНЫЕ ПРАВИЛА ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

Прежде всего, не нужно указывать слишком много информации. Помните, что другие пользователи, которые Вами заинтересуются, прочитают все до последней буквы. Личная информация должна оставаться личной.

Не следует выкладывать фотографии или другие медиафайлы, на которых Ваши друзья показаны не в очень выгодном свете: Вы можете испортить репутацию не только себе, но и знакомым.

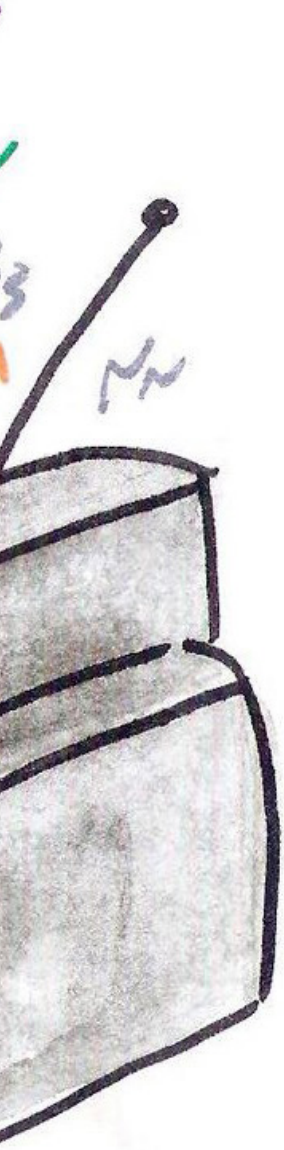
Не смешивайте работу/учебу и отдых. Преподаватели или работодатели не должны знать о Вас все.

По возможности не используйте одинаковые пароли для разных сервисов. Этим могут воспользоваться злоумышленники.

Старайтесь писать сообщения без использования жаргонной и ненормативной лексики, с соблюдением правил орфографии и пунктуации. Общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, начальством или администрацией - это не допускается.

НОВОСТИ
ИНФОРМАЦИЯ
ШОУ
РЕКЛАМА
ПРОГРАММЫ

2 НОВОСТНАЯ ГРАМОТНОСТЬ



Как оценить достоверность новостной информации?

1. Отвечает ли текст на ключевые вопросы: Что? Где? Когда? При каких обстоятельствах? Кто главные действующие лица?
2. Постарайтесь проверить, совпадает ли заголовок, лидер-абзац и текст новости? Говорят ли они об одном и том же?
3. Какие доказательства использует корреспондент? Видел ли он это сам или пересказывает чьи-то слова?
4. Оцените надежность источников.
5. Раскрывает ли корреспондент методы своей работы?
6. Указывает ли журналист контекст истории? (предыстория, связи, сравнения)
7. История сбалансированная и честная?

И главный вопрос: Что потребитель новости может **сделать** с этой информацией? Новость **полезна?** Можете прийти к четкому заключению?

Вы можете что-то сделать после этого? Вы готовы сделать суждение? Вы можете поделиться этим с кем-либо?

ОТКРЫТОСТЬ РАБОТЫ ЖУРНАЛИСТА

Журналист должен открывать методы своей работы. В противном случае следует задаться вопросом, почему нет комментария компетентного лица, очевидца, участника. Возможно, журналисту не хватает доказательств, и он предлагает свое собственное мнение под видом объективной новостной информации.

Журналист, не предоставляя источники информации, должен объяснить читателю, почему он не раскрывает эти данные.

Прозрачность – это открытость методов. Например, журналист может написать:

«Источник был недоступен».

«Пожелал остаться анонимным из страха потерять работу».

«Репортер попытался пообщаться с героем у него дома, но никто не подошел к двери».

«Информация не может быть независимо подтверждена».

Тогда читатель должен сделать вывод, что такой новости нельзя доверять, а необходимо ее проверить, поскольку нет понимания, кто ответственн за те или иные высказывания и суждения.

ПРОВЕРКА ФАКТОВ И ПОИСК ИСТИНЫ

В случаях, когда новость вызывает сомнения и ее необходимо проверить, следуйте следующим правилам:

- Первым делом Вам необходимо обратить внимание на источник информации, поскольку одним из доказательств достоверности является наличие ссылок на источники.
- Если в качестве доказательства достоверности Вам предоставляют фото, необходимо убедиться, что изображение действительно имеет отношение к описанным событиям. Для этого мы рекомендуем найти данную новость на каком-либо интернет-ресурсе и воспользоваться сервисом Google «поиск по картинкам», далее следует обратить внимание на первоисточник и дату публикации изображения и соотнести с источником информации.
- Если Вы хотите проверить подлинность видео, перейдите на сайт YouTube, кликнув по логотипу в нижнем правом углу плеера, прочтите описание к видео, посмотрите, когда и кем данное видео было загружено, а также обратите внимание на комментарии к нему. Обращайте внимание на детали: номера машин, названия улиц.
- Свидетельства очевидцев — один из самых сложных методов проверки достоверности. Здесь необходимо обращать внимание, подтверждает ли очевидец те тезисы, о которых нам сообщает журналист, или же говорит про общие вещи, которые могут косвенно или же вообще не относиться к теме.

МЕТОДЫ ОЦЕНКИ ИСТОЧНИКОВ ИНФОРМАЦИИ

Первым делом необходимо убедиться в компетентности источника, разбирается ли он в данном вопросе.

Если информация получена из интернета, проверьте регистрацию рессурса как СМИ, иначе он имеет полное право публиковать любые «новости».

Также можно выяснить рейтинг источника, на котором размещена информация, его популярность, степень доверия и авторитетность.

НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ

Ученые выяснили, что прием поливитаминов может привести к раку

Группа американских и британских ученых провела ряд исследований и пришла к выводу, что прием поливитаминов может нможет спровоцировать онкологические заболевания.

На протяжении длительного времени они изучали анамнез и истории болезни пятисот тысяч человек. Выяснилось, что побочным эффектом употребления поливитаминов может стать рак. Также повышаются риски сердечно-сосудистых заболеваний. Но это касается людей, которые придерживаются нормального пищевого рациона и одновременно принимают поливитамины.

Подобное заключение ученых вызвало ряд критики и неодобрения у скептиков. Последние уверены, что кроме правильного питания, в рацион людей необходимо добавить поливитамины. Что диета и правильный рацион не может обеспечить организм человека достаточным количеством витаминов и микроэлементов. Для этого необходим прием поливитаминов.

Но множество других научных исследований подтверждают тот факт, что употребление поливитаминов не только не оправдывает возложенных на них надежд, а часто даже усугубляет болезни и провоцирует новые.

С треском провалились исследования по изучению влияния, которое оказывает применение поливитамина Е на увеличение продолжительности жизни, снижение риска заболевания атеросклерозом, а также как профилактика инфарктов и инсультов. Продолжительность жизни людей, которые регулярно принимали витамин Е, оказалась на четыре процента ниже, чем у не принимавших. А вот прием витамина А и вовсе на шестнадцать процентов укоротил жизнь пациентов.

И вовсе неожиданным стал результат эксперимента, целью которого стало исследование дополнительного приема пациентами поливитамина С. Оказывается, всеми любимая с детства аскорбинка влияет на развитие болезней сердца. Однако не менее широкомасштабные наблюдения за людьми, употребляющими в питании много овощей и фруктов, содержащих ту же аскорбиновую кислоту, но в натуральном виде, дали замечательные результаты — такие люди значительно реже заболевали раком и сердечно-сосудистыми болезнями.

Вывод напрашивается сам собой. Витамины полезны, но только в натуральном виде.

http://wek.ru/uchenye-vyyasnili-chto-priem-polivitaminov-mozhet-privesti-k-raku

Упоминания американских, британских и иных ученых из любых других стран должны, первым делом, стать сигналом о том, что автор материала либо не знает, либо скрывает имена конкретных людей, их лабораторий и университетов. Таким сообщениям нельзя доверять, так как под прикрытием **«ученых»** можно рассказывать любые небылицы и запутывать неопытных читателей.

Если автор текста ссылается на исследования, то обязательно необходимо указывать название исследовательского проекта, группу исследователей, принимавших в нем участие, название организации, под эгидой которой проводились научно-исследовательские работы. А также год и город. В противном случае, такая информация должна восприниматься не иначе, как авторский вымысел, и ей не нужно уделять большого внимания.

А вот здесь было бы уместно указать фамилии и должности **«скептиков»**, у которых заключение ученых вызвало «ряд критики и неодобрения».

Внешне логичная конва рассуждения смотрится как полноценное аналитическое сообщение, однако, если всмотреться внимательно в суть слов-якорей, окажется, что они совсем не имеют веса.

Автор нанизывает, словно бусины, новые и новые факты, ссылаясь на исследования, имеющие громкий резонанс в научном сообществе, но вот совсем не понятно, что же это за исследование.

При этом, динамика текста, противопоставление и сталкивание позиций создают ощущение привлекательности, и текст хочется дочитать до конца.

Подобные тексты несут огромную опасность для читателей. Не потому, что можно перестать употреблять поливитамины, а потому, что таким же образом можно рассказать о кандидате на выборную должность, о политическом и экономическом скандале, о других странах и народах, разжечь межнациональный конфликт, рассорить соседей и друзей.

Выводы, которые приводятся в таких материалах, как правило, громкие и безапелляционные. Но можно ли им верить, можно ли эти выводы воспринимать всерьез? Медиаграмотному читателю - однозначно нет!

#newsapp
Apple встроит датчики пульса и давления в наушники EarPods.

В знаменитых наушниках EarPods от Apple появятся датчики, измеряющие сердцебиение и кровяное давление. Об этом сообщает The Guardian со ссылкой на анонимного автора записи в сервисе Secret.

По словам анонимного автора, в следующей версии наушников EarPods будут встроены специальные фитнес-сенсоры, измеряющие кровяное давление и пульс. Кроме того, в них будут встроены датчики iBeacon, точно определяющие положение устройства в пространстве, чтобы их было проще найти при помощи другого Apple-устройства.

Сообщается, что наушники будут подключаться через порт Lightning — именно поэтому в новых айфонах аудиопорт был перенесён на нижнюю часть корпуса.

Данные о пульсе и давлении будут храниться в зашифрованном виде, не позволяя идентифицировать пользователя — так же, как это реализовано в датчике отпечатков пальцев Touch ID. С другой стороны, владелец наушников может использовать собранную информацию для консультации с доктором, замечает инсайдер.

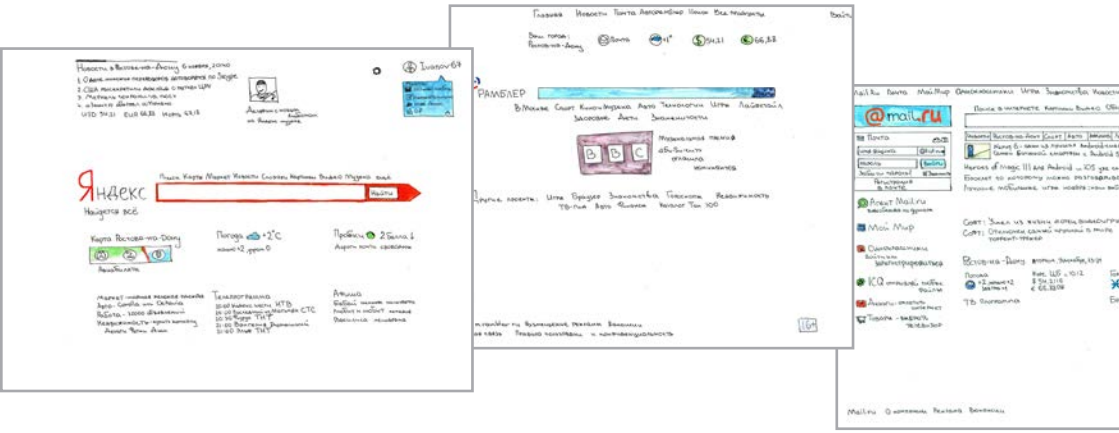
Наушники выйдут одновременно с iOS 8, помимо сенсоров, будут иметь новый пульт управления с улучшенным шумоподавлением у микрофона. Автор записи отмечает, что новые наушники станут промежуточным продуктом для выхода iWatch — хотя это ещё не финальная версия названия браслета от Apple.

Материалы опровержения ищите здесь:

Авторы материала ссылаются на анонимный источник информации, а это значит, что такой новости нельзя доверять. Необходимо перепроверить данное заявление на авторитетных ресурсах, например официальном сайте компании Apple (www.apple.com)

В предложении отсутствует комментарий официального представителя компании, нет доказательств, подтверждающих или опровергающих данные утверждения.

Продолжая ссылаться на анонимный источник, авторы статьи анонсируют важные преимущества нового продукта, касающиеся даже здоровья пользователя.



3 ПОЧТОВЫЕ СЕРВИСЫ

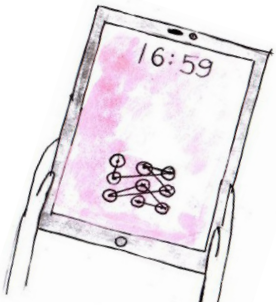
Мы уже давно живем в то время, когда люди для удобства общения и различных переписок используют электронную почту.

В этом разделе мы расскажем Вам о самых популярных службах электронной почты, об их возможностях и о правилах ведения почтового ящика.

Ваш почтовый адрес должен быть удобен в произнесении и понятен Вашему собеседнику. Используйте в названии своего ящика реальные имя и фамилию, это позволит облегчить связь с Вами. В названии почты не стоит употреблять посторонние слова, т.к. это может Вас скомпрометировать. Например, если вас зовут Екатерина Иванова, то Ваш почтовый ящик следует назвать Katelvanova или Ekaterinalvanova, если такие почтовые ящики уже существуют, то следует добавить Ваш год рождения или хотя бы две последние цифры (Katelvanova76 или Ekaterinalvanova1976). Согласитесь, что говорить Вашу почту «Ekaterinalvanova1976» не стыдно, в отличие от «Kotenok1976».

ПАРОЛЬ

Ваш пароль не должен быть простым, так как простой пароль — наибольшая угроза вашей учетной записи. Обычные слова (marina, begemot), а также предсказуемые сочетания букв (qwerty, 123456) могут быть легко подобраны программами для взлома паролей. Не стоит использовать в качестве пароля общеизвестные данные — имя, день рождения или номер паспорта. Для того, чтобы создать сложный пароль, следует использовать и прописные, и строчные латинские буквы; цифры; знаки пунктуации (допускаются знаки ` ! @ # $ % ^ & * ( ) _ = + [ ] { } ; : « \ | , . < > / ?).



Очень хороший вариант для пароля – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Такой пароль легко запомнить, и в то же время сложно взломать. Например, буквосочетание «вишневый_пирог» в английской раскладке выглядит как «dbiytdsq_gbhju».

Вернемся к почтовым сервисам. Самым популярными сервисами считаются: Yandex.ru, Google.com, Rambler.ru, Mail.ru. Так как Яндекс наиболее популярен среди российских пользователей интернета, то на примере Яндекс.Почты мы рассмотрим принцип работы электронного почтового ящика и его возможности.

ЯНДЕКС.ПОЧТА

После регистрации на Яндекс. Почте Вы получаете почтовый ящик размером 10 ГБ. При регулярном пользовании сервиса объем ящика автоматически увеличивается на 1 ГБ. Яндекс позволяет Вам выбрать индивидуальное оформление Почты на свой вкус, установив понравившуюся тему. Также Вы можете группировать письма по темам, присваивать им метки, настраивать персональные кнопки и пользоваться горячими клавишами.

В почтовом ящике доступны следующие стандартные папки:

Входящие В эту папку по умолчанию попадают все новые письма (кроме спама).

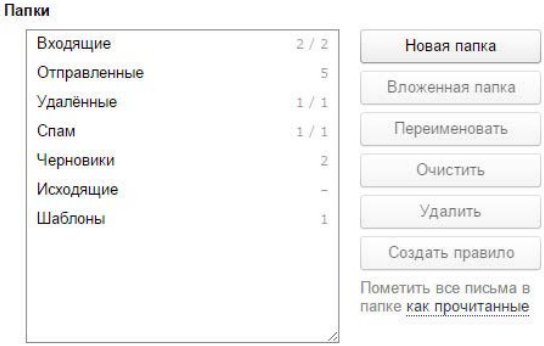
Отправленные Сюда автоматически сохраняются все отправленные Вами письма.

Удалённые В папку попадают все удаленные письма.

Спам В папку попадают письма, которые были определены как спам.

Черновики Папка для хранения черновиков и шаблонов.

Исходящие Если при отправке письма соединение с интернетом было разорвано, письмо попадает в эту папку. Когда соединение будет восстановлено, письма будут автоматически отправлены.

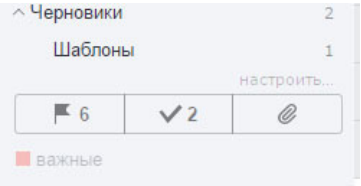


В меню **Настройка** → **Папки и метки** Вы можете создавать и редактировать другие папки:

- создавать вложенные папки внутри стандартных;
- переименовывать, очищать или удалять папки;
- помечать все письма в папке как прочитанные;
- создавать правила для автоматической сортировки писем.

Перемещать письма между папками можно несколькими способами:

- переложить письма вручную: выберите письма, а затем нажмите ссылку Переложить в папку (вверху справа);
- создать правила автоматической сортировки писем.



РАБОТА С МЕТКАМИ

Метки помогут Вам упорядочить и быстро найти нужные письма. По умолчанию в ящике уже создано несколько стандартных меток — **Важные** и **Непрочитанные** . Каждому письму можно присвоить любое количество меток.

Важные письма выделяются в списке красным цветом и значком.

ПОСТАВИТЬ МЕТКУ

Чтобы установить метку, выделите нужные письма и нажмите ссылку **Поставить метку** (вверху справа):

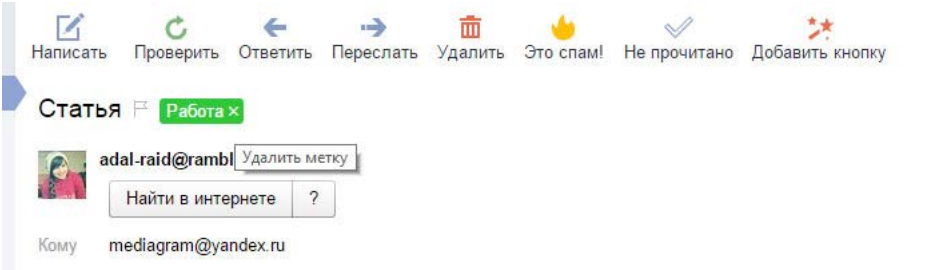
Введите название метки (максимум 15 символов) и нажмите на нее, чтобы применить изменения. Если вы хотите сразу задать цвет для новой метки, выберите в списке меток пункт **Новая метка.**

Если у Вас уже созданы метки, Вы можете просто перетащить письма на нужную метку или, наоборот, — перетащить метку на нужное письмо.

СНЯТЬ МЕТКУ

Чтобы снять метку, выделите письма и нажмите ссылку **Поставить метку** (вверху справа). В разделе **Снять метку** выберите название нужной метки и нажмите на нее, чтобы применить изменения:

Вы также можете снять метку на странице письма — для этого нажмите крестик в нужной метке.



РЕДАКТИРОВАТЬ МЕТКИ

В меню **Настройка → Папки** и метки Вы можете управлять метками:

- создавать новые метки;
- изменять и удалять метки;
- сортировать метки по количеству писем или по алфавиту;
- создавать правила для автоматической сортировки писем.

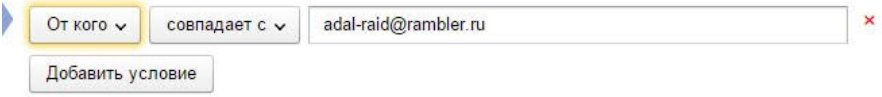
СОЗДАНИЕ И НАСТРОЙКА ПРАВИЛ

ЧТОБЫ СОЗДАТЬ ПРАВИЛО:

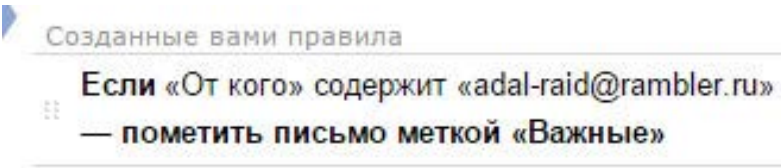
1. Откройте меню **Настройка** → **Правила обработки писем** и нажмите кнопку **Создать правило.**

2. В разделе **Применять** выберите из списков, к какому типу писем Вы хотите применять правило:

   В разделе **Если** задайте условия для обработки:



1. Выберите параметр из списка;
2. В поле справа введите значение для выбранного параметра (например, адрес или ключевое слово);
3. Выберите, насколько строго должно соблюдаться;
4. Для одного правила можно задать несколько условий, которые могут выполняться одновременно или по отдельности. Чтобы добавить другие параметры к заданному правилу;
5. В разделе **Если** нажмите кнопку **Добавить** условие, выберите параметр и его значение;
6. Уточните, должны ли указанные условия выполняться одновременно.



7. В разделе **Выполнить действие** выберите действие, которое будет выполняться для отфильтрованных писем;
8. При необходимости включите опцию **Не применять остальные правила;**
9. Если вы хотите задать имя для правила, нажмите ссылку **указать название;**
10. Чтобы сохранить правило, нажмите кнопку **Создать правило.**

ОТРЕДАКТИРОВАТЬ ПРАВИЛО

Чтобы отредактировать, выключить или удалить правило, воспользуйтесь ссылками справа от нужного правила на странице «Правила обработки почты».

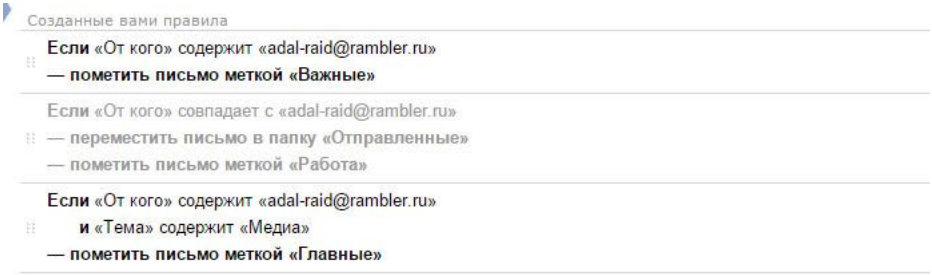
ПРИОРИТЕТ ПРАВИЛ

Приоритет выполнения правил зависит от их расположения на странице «Правила обработки почты» — чем выше расположено правило, тем выше его приоритет.

Например, если для нескольких правил были заданы одинаковые условия, но разные действия, выполнится только одно из этих правил — с самым высоким приоритетом.

Если Вы хотите поднять приоритет правила, перетащите его на позицию выше.

Если в одном из нескольких правил с одинаковыми условиями Вы включите опцию **Не применять остальные правила**, то правила с более низким приоритетом выполняться не будут.

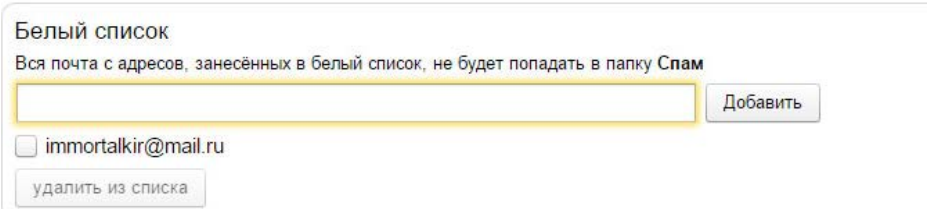


БЕЛЫЙ И ЧЁРНЫЙ СПИСОК

БЕЛЫЙ СПИСОК

Если Вы подписаны на рассылку, которая ошибочно определяется как спам, вы можете исключить этот адрес из фильтрации, нажав на странице чтения письма кнопку **Не спам!.** Адрес будет добавлен в белый список, и новые письма из рассылки будут приходить в папку **Входящие.**

Вы можете отредактировать белый список в любой момент в меню **Настройка → Правила обработки писем.** Чтобы добавить адрес в белый список, заполните поле и нажмите кнопку **Добавить.** Чтобы исключить адрес из белого списка, отметьте его и нажмите кнопку **удалить из списка**.



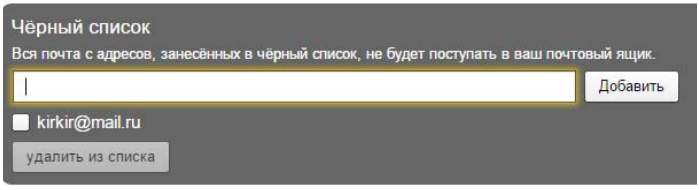
ЧЁРНЫЙ СПИСОК

Вы можете отредактировать черный список в любой момент в меню **Настройка → Правила обработки писем.** Чтобы добавить адрес в черный список, заполните поле и нажмите кнопку **Добавить.**

Ограничение. В черный список можно добавить только полный почтовый адрес, например, «khan.singh@revenge.ru». Неполные записи, например «*singh@revenge.ru» или «@revenge.ru», будут игнорироваться.

Письма от нежелательного адресата перестанут приходить только после того, как вы добавите адрес в черный список. Все уже пришедшие письма удалены не будут и останутся в вашем ящике.

Чтобы исключить адрес из черного списка, отметьте его и нажмите кнопку **удалить из списка.**



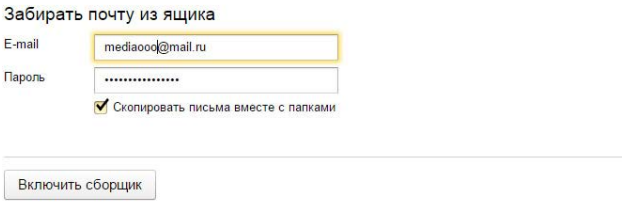
СБОР ПОЧТЫ С ДРУГИХ ПОЧТОВЫХ ЯЩИКОВ

Вы можете перенаправлять почту с других ваших почтовых ящиков в ваш ящик на Яндексе.

Примечание. В одном ящике можно создать не более 10 сборщиков.

СОЗДАТЬ СБОРЩИК ПОЧТЫ

1. Перейдите в меню **Настройка → Сбор почты с других ящиков.**
2. В блоке **Забирать почту из ящика** укажите логин и пароль, которыми вы пользуетесь для входа в другой ящик. Затем нажмите кнопку **Включить сборщик.**
3. В открывшейся странице установите правила для обработки собранной почты.

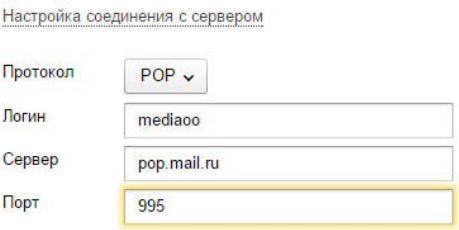


Если автоматически настроить соединение сборщика с сервером невозможно:

1. Нажмите ссылку **Настройка соединения с сервером.**
2. Введите имя почтового сервера и номер порта вручную. Значения этих параметров Вы можете узнать в службе поддержки почтового сервиса, на котором расположен Ваш ящик.

ОТРЕДАКТИРОВАТЬ НАСТРОЙКИ СБОРЩИКА

1. Перейдите в меню **Настройка → Сбор почты с других ящиков.**
2. Нажмите на название сборщика в списке подключенных ящиков.
3. Перейдите по ссылке **Настроить.** Здесь Вы сможете отредактировать правила обработки собираемой почты и параметры соединения сборщика с сервером.



Чтобы отключить сборщик, перейдите на страницу **Сбор почты** и нажмите ссылку **выкл.**

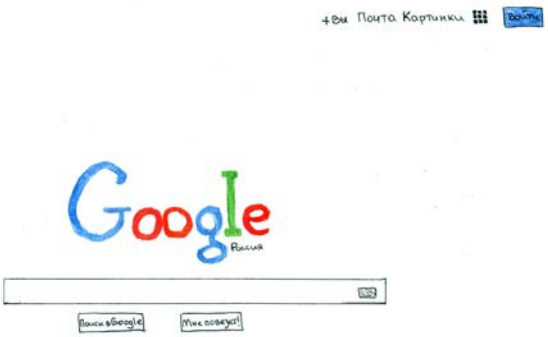
Если сборщик больше не нужен, нажмите на название сборщика, а затем на ссылку **Удалить.**

РАСПОЗНАВАНИЕ СПАМА

Если Вы считаете, что получили письмо содеражащее спам в папку **Входящие,** выделите нужное письмо и нажмите кнопку **Это спам!** — письмо будет перемещено в папку **Спам,** а необходимая информация будет отправлена в Спаморону. Изучение нежелательных рассылок позволяет улучшать алгоритмы фильтрации для новых видов спама.

Если письмо попало в папку **Спам** по ошибке, нажмите кнопку **Не спам!** — новые письма из рассылки будут приходить в папку **Входящие.**

Спамооборона учитывает как общие, так и «персональные» правила фильтрации, которые действуют для отдельного почтового ящика. Если вы считаете письма рассылки нежелательными, а пользователь другого почтового ящика — полезными, в вашем ящике они будут попадать в папку **Спам,** а в ящике другого пользователя в папку **Входящие.**



GOOGLE

Электронная почта на Google.ru - Gmail, заслуженно считается одним из лучших сервисов такого рода. Рассмотрим основные преимущества, которые даст вам использование ящика на Gmail.com.

Большой объем При регистрации новый пользователь получает 15 Гб свободного места.

Мощный спам-фильтр Систему защиты пользователей от спама, которая работает в Gmail, можно с уверенностью назвать одной из лучших.

Мгновенный поиск Не стоит забывать, что хотя Gmail и является почтовым сервисом, он принадлежит компании Google, поэтому нужную информацию через этот поисковый сервис искать удобнее.

Универсальный пароль Создав аккаунт, Вы получите универсальный ключ входа, который позволяет работать со всеми другими сервисами Google.

Удобная группировка писем Сообщения в Gmail автоматически группируются и отображаются в виде цепочек, что повышает удобство отслеживания и ведения переписки.

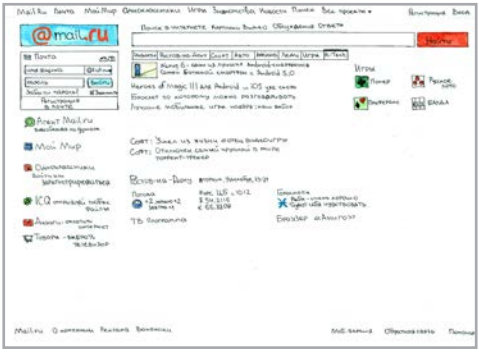
Упорядоченность С помощью таких встроенных функций, как ярлыки, фильтры, пометки и др., Вы получаете возможность управлять письмами и их группировкой.

Встроенная коммуникация Пользователи аккаунтов Gmail могут общаться с другими участниками путем голосового или видеочата.

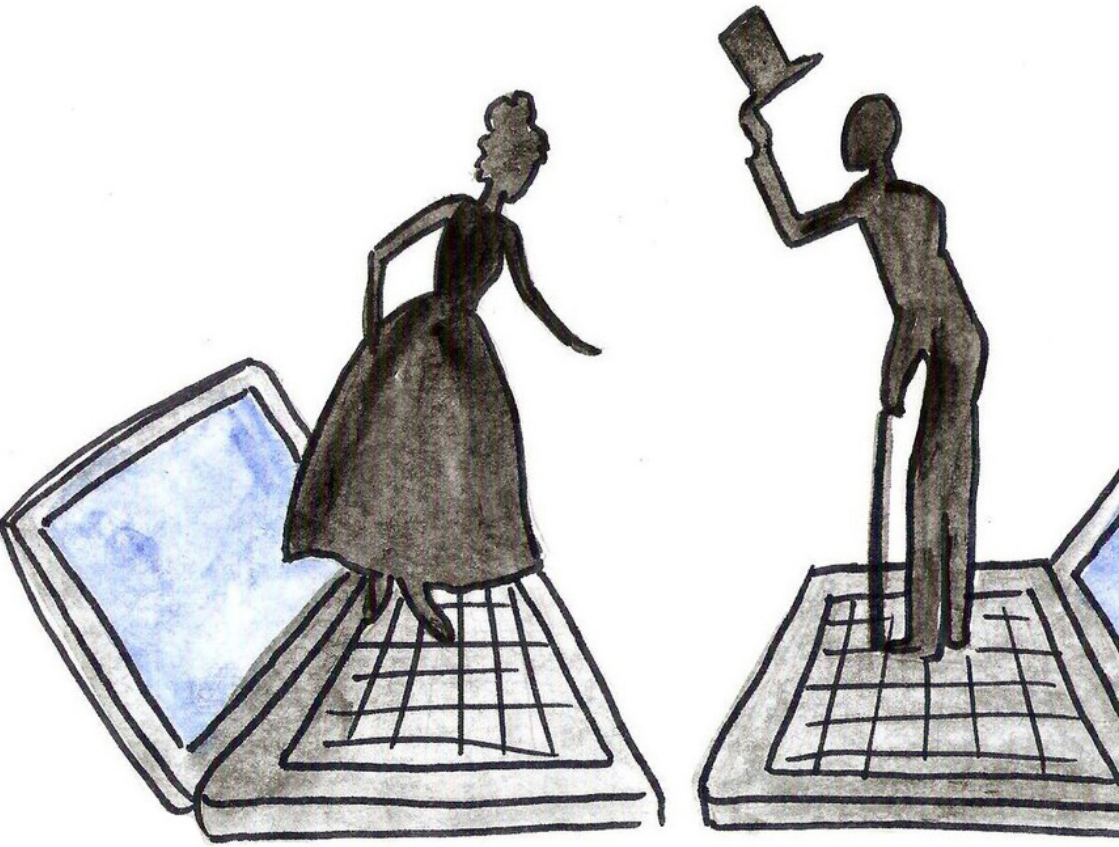
RAMBLER

К достоинствам этого сервиса можно отнести наличие виртуальной клавиатуры. Что касается письма, то его максимальный размер составляет 25 мегабайт, а это не так уж много. Что касается размера самого почтового ящика, то он составляет всего лишь 50 мегабайт. У ящика есть возможность увеличения на 50 Мб в сутки. В итоге максимальная величина, которую он может составить, - 100 мегабайт. Для людей, которые собираются вести серьёзную переписку с множеством писем и объёмными вложениями, почтовый сервис Рамблер может не подойти. К письму можно прикрепить исключительно один файл, размер которого доходит до 20 мегабайт.

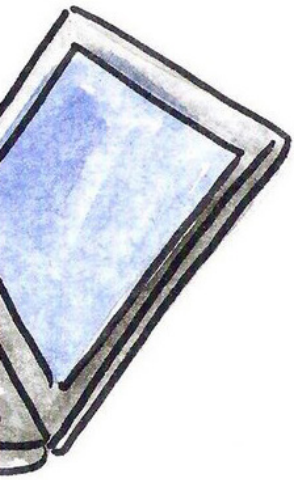
MAIL.RU



В почтовом сервисе Mail.ru размер почтового ящика не ограничен. При регистрации пользователю дается 10 Гб, затем по мере необходимости ящик можно увеличить. Все остальные возможности похожи на те, что есть в сервисе Яндекс.



ПРАВИЛА СЕТЕВОГО ЭТИКЕТА И ДЕЛОВОЙ КОРРЕСПОНДЕНЦИИ



1. **Время ответа** на письмо. Отсутствие своевременного ответа может затруднить работу людям, которые связаны с вами деловыми отношениями. А задержка с ответом клиенту – это нередко серьезный риск потерять его. Порог допустимого времени ответа – в течение дня.

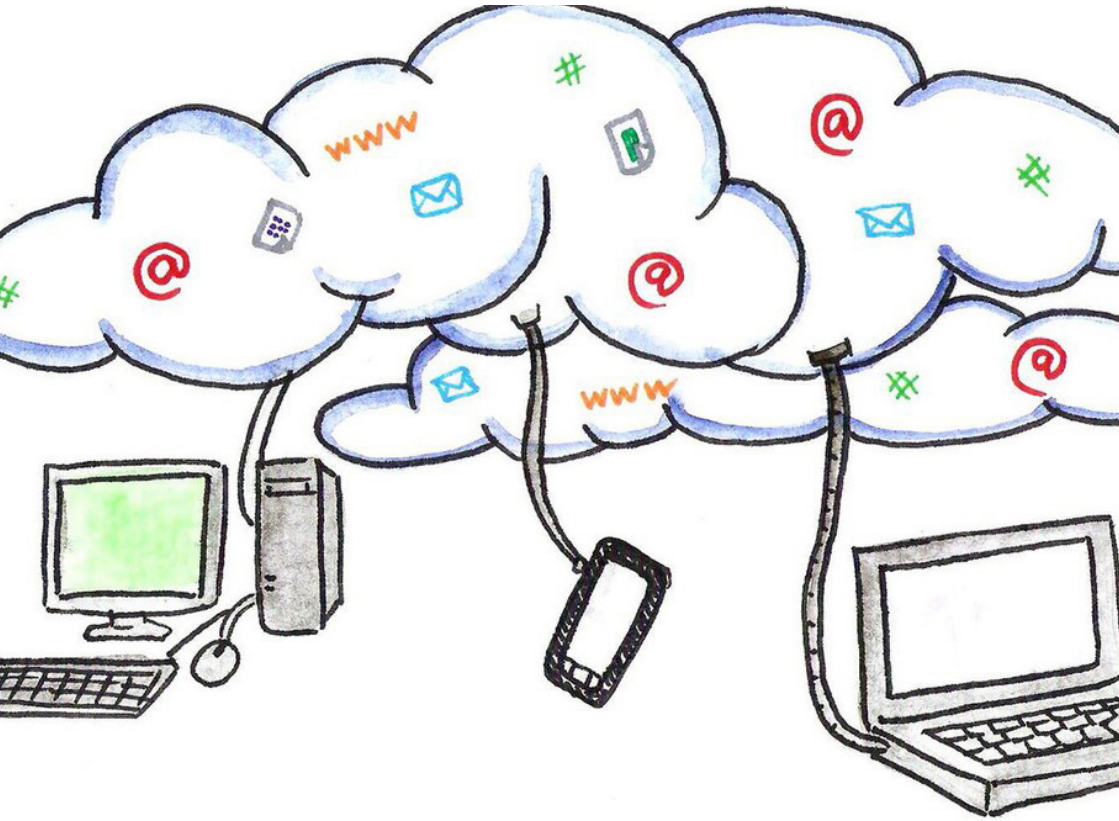
2. **Грамотное заполнение** поля «Тема». Название темы должно быть предельно подробным, содержательным и в то же время кратким.

3. **Персональное обращение.** Деловое письмо, начинающееся с персонального обращения и приветствия, отражает индивидуальную направленность письма, демонстрирует Ваше внимание и уважение к личности клиента/делового партнера.

4. **Выражение слов** признательности за обращение в компанию (за обращение к Вам). Ответное письмо, которое начинается с фразы «Спасибо за Ваше письмо», демонстрирует адресату, что Вы заинтересованы в общении с ним.

5. **Позитивное завершение письма.** Создайте у адресата хорошее настроение, чтобы ему и далее хотелось общаться с Вами.

6. **Подпись и блок контактной информации.** Любому человеку всегда важно понимать, кто находится «по ту сторону монитора». Поэтому каждое письмо должно заканчиваться подписью и блоком с контактной информацией.



4 ОБЛАЧНЫЕ ХРАНИЛИЩА

Почему это происходит? Владельцам интернет-ресурсов чаще гораздо дешевле и удобнее использовать для хранения файлов сторонние ресурсы бесплатно, чем загружать эти файлы на собственный хостинг.

Яндекс.Диск disk.yandex.ru Один из самых удобных и быстрых файлообменников в рунете. Это облачное хранилище – Ваша личная «флешка». Загрузить туда файлы можно только зарегестрировав Яндекс.Почту, но скачивать файлы можно довольно просто – достаточно лишь ввести код с картинки.

При регистрации дается 10гб свободного пространства, увеличить его можно за деньги.

rusfolder.com Один из самых популярных российских файлообменников. Есть возможность загружать файлы без регистрации. После загрузки вашего файла он автоматически перезагружается еще на несколько серверов, именуемых зеркалами, это дает возможность скачивать файл на высокой скорости сразу нескольким людям. Когда проходит срок хранения, файл перемещается в архив.

mediafire.com Самый известный и удобный зарубежный файлообменник, скорость скачивания большая, практически неограниченная. Файл скачивается без ожидания, без проверки «робот-человек», но существует ограничение по размеру файла – 200 Мб. Ограничение по времени на хранение файла – один месяц с последней загрузки. Как и Яндекс.Диск, это облачный файлообменник. Загрузка файла невозможна без установки специального клиента на ваш компьютер. 2 гб выдается в ваше распоряжение бесплатно, с возможностью расширения.

Rghost.ru Простой и удобный файлообменник с возможностью добавлять комментарии к загружаемым файлам. Срок хранения файла – 3 месяца с момента последней заргузки. Есть возможность скачать файл при помощи torrent-клиента. Минус – нет возможности загрузить видео.

В сети существует ряд файлообменников с уклоном в мошенничество. Например, для скачивания вам нужно обязательно ввести свой номер телефона «для проверки» по SMS . Если Вы все же попались на эту удочку, то можете легко не досчитаться единиц на счете своего мобильного. Остерегайтесь таких сайтов, как: turbobit.ru, letitbit.net, 123cash.ru, vsckachke.com, rapidshare.com. На всех этих сайтах есть возможность попасться на «SMS-лохотрон».

ЯЗЫК ЗАПРОСОВ

Язык запросов поисковых систем — это специальные правила, используя которые Вы сможете улучшить эффективность Вашей работы. Он позволяет учитывать префиксы, регистр символов, морфологию, расстояние между словами. В большинстве поисковых систем существует функция расширенного поиска информации.

ЯЗЫК ЗАПРОСОВ В ЯНДЕКСЕ

Вы можете конкретизировать поисковый запрос с помощью специальных символов, которые уточняют наличие и взаимное расположение запрашиваемых слов в документе.

Яндекс ищет все формы слова, указанного в запросе. Исключение составляют случаи, когда используются символы **!** и **"**.

+ - поиск документов, в которых обязательно присутствует выделенное слово. Допустимо использовать несколько операторов + в одном запросе.

[Урал **+**Екатеринбург **+**билеты]

Будут найдены документы, в которых обязательно содержатся слова «билеты» и «Екатеринбург» и может присутствовать слово «Урал».

" - поиск по цитате, т.е. документов, содержащих слова запроса в заданной последовательности и форме.

[**"**Люблю грозу в начале мая**"**]

Будут найдены документы, содержащие данную цитату.

***** - поиск по цитате с пропущенным словом (словами). Один оператор * соответствует одному пропущенному слову. Внимание! Используется только в составе оператора ".

[**"**Люблю * в начале мая**"**]

Будут найдены документы, содержащие данную цитату, включая пропущенное слово.

& - поиск документов, в которых слова запроса, объединенные оператором, встречаются в одном предложении. Допустимо использовать несколько операторов **&** в одном запросе.

[культура **&** Россия **&** художники]

Будут найдены документы, в которых есть предложения, содержащие одновременно слова «культура», «Россия» и «художники».

| - поиск документов, в которых присутствует любое слово из запроса. Допустимо использовать несколько операторов | в одном запросе.

[автомобиль | запчасти | радиатор]

Будут найдены документы, в которых присутствует хотя бы одно из слов запроса: «автомобиль», «запчасти» или «радиатор».

- - поиск документов, в которых отсутствует заданное слово. Исключается только слово, перед которым стоит оператор.

[Театр -большой]

Будут найдены документы, в которых присутствует слово «театр», но нет слова «большой».

ЯЗЫК ЗАПРОСОВ GOOGLE

+ - поиск документов, в которых обязательно присутствует выделенное слово. Допустимо использовать несколько операторов + в одном запросе.

[Англия +виза +билеты]

Будут найдены документы, в которых обязательно содержатся слова «виза» и «билеты» и может присутствовать слово «Англия».

" - поиск по цитате, т.е. документов, содержащих слова запроса в заданной последовательности и форме.

["Люблю грозу в начале мая"]

Будут найдены документы, содержащие данную цитату.

*- поиск по цитате с пропущенным словом (словами). Один оператор * соответствует одному пропущенному слову. Внимание! Используется только в составе оператора ".

["Люблю * в начале мая"]

Будут найдены документы, содержащие данную цитату, включая пропущенное слово.

| или **OR** - поиск документов, в которых присутствует любое слово из запроса. Допустимо использовать несколько операторов | в одном запросе.

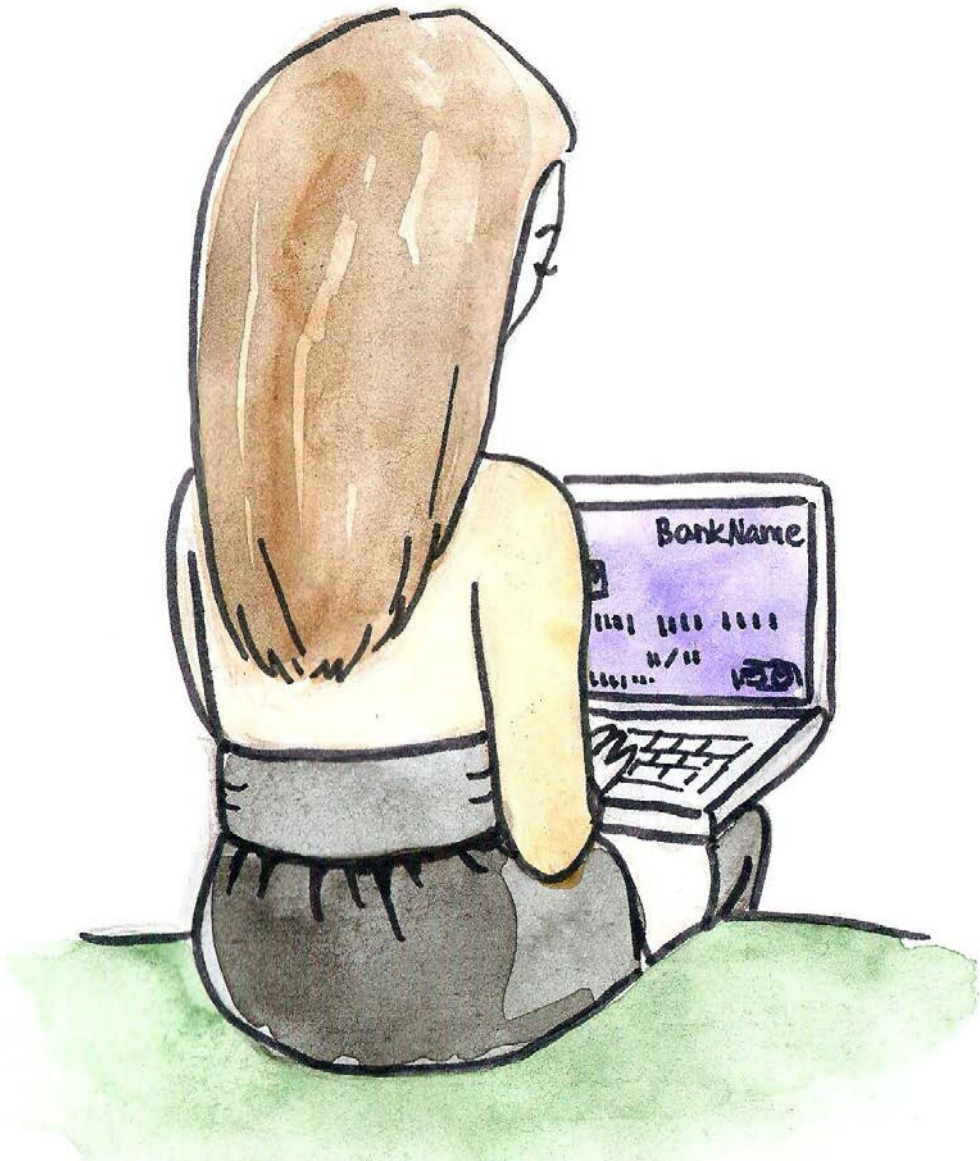
[диван | кровать | кресло]

Будут найдены документы, в которых присутствует хотя бы одно из слов запроса: «диван», «кровать» или «кресло». Или [диван **OR** кровать **OR** кресло]

- - поиск документов, в которых отсутствует заданное слово. Исключается только слово, перед которым стоит оператор.

[зоопарк -ростовский]

Будут найдены документы, в которых присутствует слово «зоопарк», но нет слова ростовский».



5 ЭЛЕКТРОННЫЕ ФИНАНСЫ

6 ПРОСТЫХ ПРАВИЛ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

Если Вы решили проверить баланс своей кредитной карты онлайн, оплатить счета, перевести деньги кому-либо, купить или продать что-нибудь в интернете, то эти 6 простых правил помогут Вам не потерять деньги.

1. **Защити свой компьютер.**

   Своевременно проверяйте обновления Программного обеспечения. Обязательно установите антивирусное и антишпионское ПО. Никогда не отключайте firewall. Защитите свой wi-fi роутер паролем и используйте usb-накопители с осторожностью.

2. **Используйте только сложные пароли.**

   Самые эффективные пароли – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Вам в любом случае будет намного проще и главное безопаснее создать свой сложный пароль, чем злоумышленникам такой пароль разгадать. Пароль «Denis1986» взламывается очень просто, поэтому мы советуем Вам придумать 2 вида паролей: 1) длинные и сложные пароли для платежных систем; 2) простые и легко запоминающееся для форумов и других, не представляющих опасности для ваших денег. Храните свои пароли в секрете. Не отправляйте их по SMS, e-mail или в социальных сетях.

3. **Не переходите по ссылкам. Набирайте адрес сайта самостоятельно.**

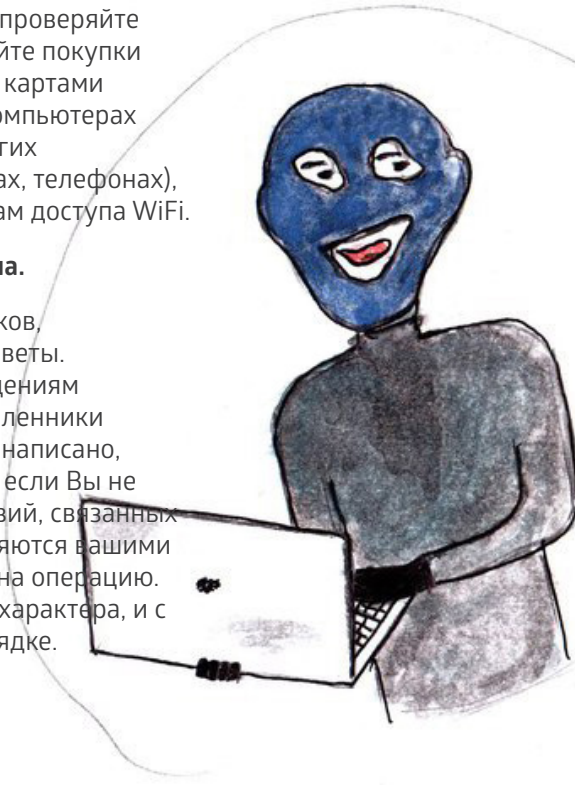
   При переходе по ссылке из сомнительных источников (e-mail,форумы, сообщения в соц.сетях, всплывающие окна), Вы рискуете попасть на «фишинговый сайт» (Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям, номерам кредитных карт, электронной почте и т.д.). Суть заключается в том, что мошенник создает интернет-страницу, идентичную настоящей, на которой у пользователя запрашивается конфиденциальная информация с целью ее получения мошенником. В первую очередь при переходе на сайт обращайте внимание на адресную строку. Зачастую мошенники подменяют одну или несколько букв в названии сайта (пример: http://www.sberbank.ru/ - http://www.sbenbank.ru/).

4 **Всегда проверяйте, установлено ли защищенное соединение.**

В сети Интернет используется в основном два протокола: HTTP и Secure HTTP. Перед тем как ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), обратите внимание на адресную строку, убедитесь, что имя протокола имеет вид https://, а не http ("s" – значит secure. англ. «защищенный»). Сертификаты подлинности получают только законопослушные компании, проверенные специалистами. Также о защищенности интернет-соединения свидетельствует значок амбарного замка на зеленом фоне рядом с адресной строкой.

5 **Совершайте транзакции только на домашнем компьютере.**

Никогда не оплачивайте счета, не проверяйте баланс личного счета, не совершайте покупки и другие операции с банковскими картами или электронными деньгами на компьютерах с общим доступом, а также на других мобильных устройствах (планшетах, телефонах), подключенных к публичным точкам доступа WiFi.



6 **Придерживайтесь здравого смысла.**

Чтобы защитить себя от мошенников, тщательно изучите эти простые советы. Внимательно относитесь к оповещениям из своего «банка». Часто злоумышленники присылают сообщения, в которых написано, что Ваш счет будет заблокирован, если Вы не предпримите немедленных действий, связанных с переводом денег, или представляются вашими родственниками и требуют денег на операцию. Не доверяйте сообщениям такого характера, и с Вашими деньгами все будет в порядке.

ЭЛЕКТРОННАЯ КОММЕРЦИЯ

Электронные платежи уже несколько лет являются актуальным трендом. Но за восхищением от открывшихся возможностей скрывается проблема безопасности.

Электронные транзакции в интернете завоевали заметные позиции на мировом рынке. Основное препятствие развития этого рынка — это недостаточная защита интернет-платежей.

Говоря о платежных системах, нельзя не упомянуть такое средство, как «электронные деньги». Это абстракция вроде единиц на телефонном счете. Технология удобна как для клиентов, так и для продавцов. Цифровые деньги хранятся в специальном электронном кошельке либо на сервере платежной системы.

Самые известные в России системы цифровой наличности – «Яндекс.Деньги» (money.yandex.ru) и Web-money (www.webmoney.ru)

Уже значительное время цифровые деньги принимают во многих российских интернет-магазинах. Также ими можно расплатиться за коммунальные услуги либо пополнить счет мобильного телефона.

Яндекс деньги

WebMoney

МОБИЛЬНЫЙ БАНКИНГ

Сегодня среднестатистический потребитель не выпускает телефона из рук почти 24 часа в сутки.

У мобильного банкинга есть множество преимуществ. Это хорошая безопасность, легкий доступ и разнообразные приложения для смартфонов. Самым большим преимуществом является то, что у Вас появляется больше возможностей контроля своих денег. Мобильный банкинг возвращает нас к временам, когда мы использовали пароли. Например, Вы можете сидеть в аэропорту и проверять баланс вашего счета или изучать последние сделки. Недостатком является то, что мобильный банкинг еще не так хорош, каким он мог бы быть. Многие услуги достаточно просты. Люди используют его, чтобы проверить баланс и контролировать расходы, а это во многом просто небольшое дополнение к интернету. В итоге, функционал мобильного банка только лишь приближается к интернет-банкингу.

Потребители могут избежать мошенничества в режиме реального времени с помощью SMS. Это помогает банкам и потребителям контролировать мошеннические операций.

Географическое положение также помогает сократить случаи мошенничества, опираясь на GPS-возможности смартфона, можно остановить некоторые случаи мошенничества прежде (и даже раньше), чем они произойдут. Например, если кредитная карта используется в сотнях километров от месторасположения телефона, то есть вероятность, что один или другой был украден.

Будущее биометрических технологий открывает все новые возможности для безопасности. Новые смартфоны уже выпускаются с таким видом возможностей. Например, мобильная ОС Android использует технологию распознавания лиц, чтобы разблокировать телефон пользователя. A Siri от Apple на iPhone предоставляет возможность распознавания голоса, а также сканер отпечатков пальцев TouchID уже широко используется для оплаты.

Многие российские банки уже предоставляют услугу Мобильного банка. Это Сбербанк, Втб-24, Уралсиб, Альфа-банк и другие.

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ КРЕДИТНЫМИ КАРТАМИ В СЕТИ ИНТЕРНЕТ?

Всегда следует обращаться аккуратно со своими зарплатными, кредитными, дебитовыми картами, на которых есть доступные для списания средства. В случае с интернетом, для покупок лучше всего открыть специальную карту, на которую Вы будете переводить определенную сумму денег с основных карт только для совершения конкретных транзакций.

Никогда не упускайте из виду свою карту, когда передаете ее кассиру или официанту, ведь для того, чтобы совершить покупку в интернете зачастую достаточно знать только номер карты и срок ее действия.

Всегда следите за остатком на карте. Предпочтительно проверять баланс через специальную услугу SMS-информирования. В этом случае Вы не будете часто вводить логин и пароль в интернете. Если Вы вовремя заметили транзакцию, которую Вы не совершали, ее зачастую можно отменить, подав соответствующую заявку.

Вводите номер карты и срок ее действия только на проверенных сайтах, желательно аккредитованных. Об этом Вам скажут логотипы Verified by Visa и MasterCard SecureCode.

Для совершения покупок популярные интернет-магазины предоставляют специальные сервисы, которые обеспечивают высокую безопасность банковских транзакций, а также сводят к минимуму возможности мошенников.

Одна из таких систем была запущена интернет-аукционом eBay. PayPal позволяет совершать покупки в сети интернет, не раскрывая данных своей карты. Таким образом, утечка данных карты может произойти только, если на ваш компьютер попал вирус или троян. Так же у PayPal действует система защиты пользователей. По ее условиям, компания вернет вам ваши средства, если вы стали жертвой мошенника.

Многие компании-создатели антивирусных программ выпустили специальные пакеты, предназначенные для совершения безопасных платежей в сети Интернет. Самые популярные: Kaspersky Internet Security, Dr.Web, БастионAvast, Internet Security

6 РОДИТЕЛЬСКИЙ КОНТРОЛЬ

Развитие интернета и мобильных технологий, их простота и доступность для детей создают новые угрозы и заботы для родителей. Довольно трудно проверить, с кем общается ребенок, какие сайты он посещает, какие видео смотрит. Но вместе с развитием технологий, обеспечивающих доступ к медиаконтенту, создаются и системы для родительского контроля и создания безопасной среды пребывания детей и подростков в сети.

МЕДИАГРАМОТНОСТЬ

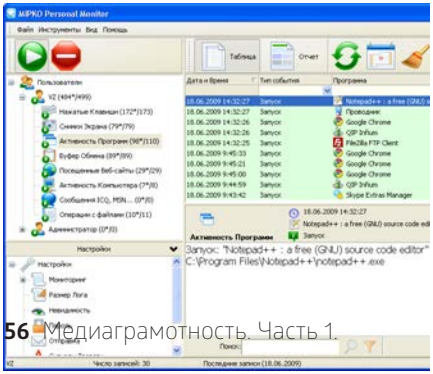
ПРОГРАММЫ ДЛЯ РОДИТЕЛЬСКОГО КОНТРОЛЯ ЗА ИНТЕРНЕТ-АКТИВНОСТЬЮ ДЕТЕЙ

Среди множества бесплатных и платных программ для осуществления родительского контроля Центр медиаграмотности выбрал наиболее распространенные и популярные, которые мы рекомендуем Вам.

MIPKO PERSONAL MONITOR:

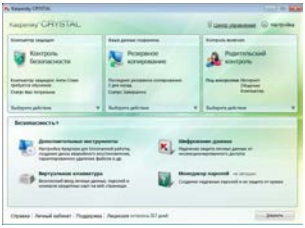
- Перехватывает все сообщения в ICQ, «Вконтакте», Facebook, «Одноклассниках», а также в других мессенджерах и социальных сетях.
- Записывает текстовые сообщения и звук в Skype.
- Автоматически делает скриншоты экрана и снимки веб-камерой.
- Ведет историю интернет-серфинга.
- Перехватывает нажатие каждой кнопки.
- Отправляет все перехваченные данные на электронную почту.

Источник:



KASPERSKY CRYSTAL И KASPERSKY INTERNET SECURITY

Источник:

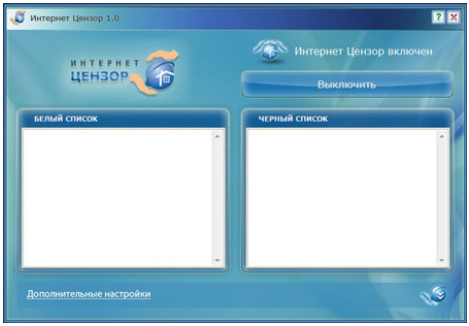


Оба пакета позволяют осуществлять родительский контроль на компьютере в полном объёме. Возможны ограничения по времени работы и по доступным ресурсам. Можно разрешить к запуску лишь определённый список программ.

Контроль за действиями в интернете тоже достаточно мощный. Отслеживаются не только web-страницы, но и системы обмена мгновенными сообщениями, электронная почта и социальные сети.

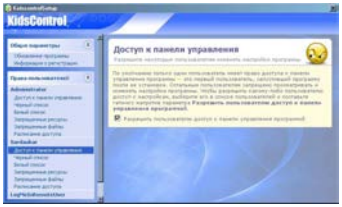
ИНТЕРНЕТ-ЦЕНЗОР

Данный интернет-фильтр предназначен для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология «белых списков», гарантирующая 100% защиту от опасных и нежелательных материалов. Программа содержит уникальные проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Интернет Цензор защищён от попыток ребёнка обойти фильтрацию или взломать программу.



Источник:

Источник:



KIDSCONTROL

KidsControl 2.02

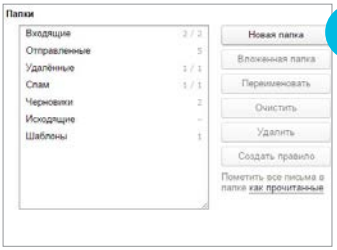
Цена: 870руб*

Основное назначение KidsControl - ограничение времени, которое ребенок проводит в интернете, а также блокировка нежелательных сайтов. Программа не афиширует свое присутствие, в случае попытки открыть запрещенный сайт, она выводит стандартное окно браузера, где говорится об отсутствии сети. В этом случае ребенок решит, что такого сайта вовсе не существует. Имеется возможность блокировки доступа к файлам определенных форматов. С помощью календаря существует возможность составления расписания доступа к компьютеру.

* цена указана по состоянию на декабрь 2014 г.

РОДИТЕЛЬСКИЙ КОНТРОЛЬ В WINDOWS 8

- Создаем учетную запись для Ваших детей или пользователей, которым необходимо ограничить доступ к нежелательному контенту. **скриншот 1**

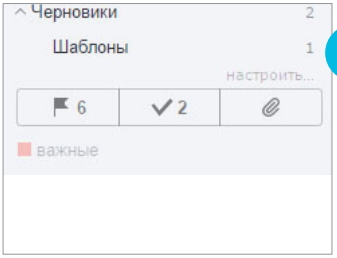


1

- Для этого переходим в Панель управления -> Учетные записи пользователей и создаем новую запись. После того, как учетная запись создана, необходимо перейти в этом же окне по ссылке «Семейная безопасность». **скриншот 2**

2

- Должно быть две записи. Выбираем ту, которую хотите ограничить. В новом окне включаем «Семейную безопасность». **скриншот 3**

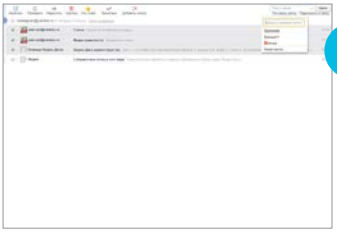


3

- Далее выбираем «Веб-фильтр» и устанавливаем переключатель «... может просматривать только те веб-сайты, которые я разрешу». **скриншот 4**

4

- Теперь установим уровни веб-фильтрации: 1) Выбираем в этом же окне ссылку «Установить уровень веб-фильтра» и видим такое окно. **скриншот 5**



5

● Здесь Вы можете сами выбрать какой переключатель установить. Сайты будут фильтроваться по списку, который уже сформирован кем-то в Microsoft`е. Либо можно поставить переключатель на «Только из списка разрешений» и вписывать туда сайты, к которым будет открыт доступ. **скриншот 6**

6

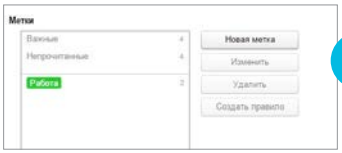
● Выбираем «Разрешение или блокировка определенных веб-сайтов» и составляем список. Если выберите этот способ, то лучше в нём перечислять сайты, к которым нужно запретить доступ, например соц. сети. **скриншот 7**

7

● Теперь возвращаемся к начальному окну и устанавливаем ограничение по времени. На выбор предлагаются 2 варианта ограничений: «Установить лимит времени» и «Установить запретное время». **скриншот 8**

8

● Снова возвращаемся на начальный экран настроек и выбираем пункт «Ограничения на игры и Магазин Windows» для того, чтобы пользователь не мог смотреть и устанавливать определённые игры и приложения из магазина. **скриншот 9**

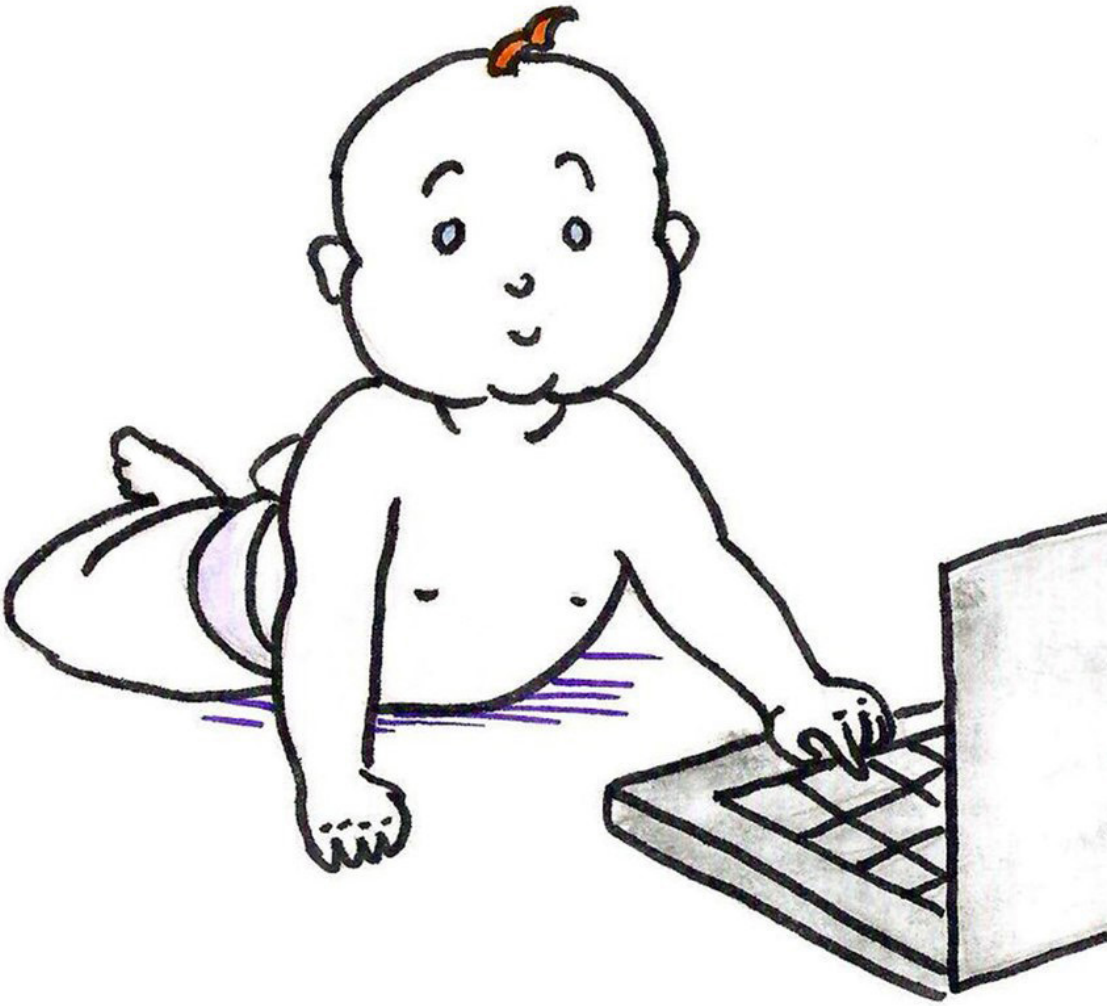


9

● Ставим переключатель на «... может пользоваться только теми играми и приложениями из Магазина Windows, которые я разрешу» и кликаем на ссылку «Задать категории для игр и приложений из Магазина Windows».

10

В этом окне можно просто поставить переключатель на «Для детей», предварительно выбрав пункт «Блокировать игры, категория которых не указана». **скриншот 10**

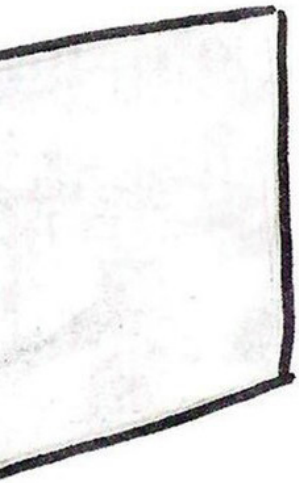


ДЕТСКИЙ ИНТЕРНЕТ

ДЕТСКИЙ ИНТЕРНЕТ-БРАУЗЕР ГОГУЛЬ

Бесплатный детский браузер **Гогуль** – средство родительского контроля детей в сети Интернет. Точнее говоря, это бесплатное расширение для браузера **Mozilla Firefox** для родительского контроля и ограничения детей в сети от нежелательного контента, разработанное российской компанией «Новое Поколение».

Принцип работы тоже прост – имеется каталог «белых», разрешённых к просмотру детьми сайтов, остальные будут блокироваться по умолчанию. Недостаток – постоянная проверка через онлайн. Опять же никто не запрещает воспользоваться другим браузером. Правда для решения последней проблемы есть **Angry Duck** – дополнительное приложение, блокирующее во время своей работы все браузеры, за исключением Гогуля. Блокировка снимается вводом родительского пароля, устанавливаемого при первом запуске приложения.



БЕЗОПАСНОСТЬ РАБОТЫ СО СМАРТФОНОМ

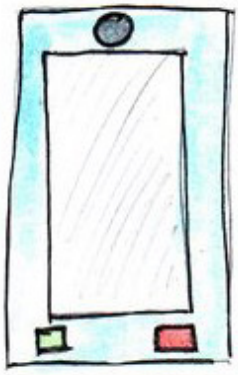
- Ограждение ребенка от нежелательной информации при посещении Интернета;
- запрет на скачивание и установку нежелательных (неизвестных и дорогостоящих) приложений в целях сохранности ОС устройства;
- ограничение общения с незнакомцами посредством мобильного устройства;
- ограничение времени работы на устройстве (например, запрет на игры во время уроков);
- блокировка входящих и исходящих звонков, а так же возможность обнаружения места нахождения ребенка через устройство.

«РОДИТЕЛЬСКИЙ КОНТРОЛЬ» ОТ МОБИЛЬНЫХ ОПЕРАТОРОВ «БОЛЬШОЙ ТРОЙКИ»

Для обеспечения безопасности детей, пользующихся мобильными устройствами, **МТС** предоставляет услугу **«Ребенок под присмотром»,** которая позволяет отслеживать перемещения ребенка на карте или с помощью SMS по местоположению его мобильного телефона (в том числе через социальные сети).

Билайн предоставляет продукты для родительского контроля для домашнего интернета. Оператор предлагает защиту домашнего ПК в трех направлениях – ограничение по возрасту (ограничение контента), отчет о посещении и ограничение по времени.

Мегафон предлагает услугу **«Детский интернет».** Это стандартный мобильный интернет со встроенными ограничениями на основе «белых списков», разработанных и регулярно обновляемых компанией. Стоимость услуги 300 р./мес.*



* цена указана по состоянию на декабрь 2014 г.

«РОДИТЕЛЬСКИЙ КОНТРОЛЬ» ВНУТРИ СМАРТФОНА

ANDROID

В мобильной платформе Android «Родительский контроль» не предусмотрен. Зато можно найти более 500 приложений, готовых защитить Вашего ребенка.

Одно из наиболее популярных приложений - бесплатное приложение Kids Place (Детская площадка) позволяет назначить ребенка отдельным пользователем на устройстве, сменить который можно только при наличии пароля. При перезагрузке устройства ребенок попадет в тот же аккаунт.

APPLE IOS

В iOS работает встроенная функция «Родительского контроля». В его возможности входит ограничение использования приложений, запуск/удаление приложений, отключение браузера Safari, клиента для просмотра видеороликов YouTube, камеры и приложения для покупок в интернет-магазинах iTunes.

Взломать защищенный паролем iPhone или iPad для ребенка практически невозможно, а родители смогут отслеживать попытки нарушить запрет.

WINDOWS PHONE 8

Приложение «Родительского контроля» в устройстве Microsoft Windows Phone 8 носит название Kid's Corner и работает по принципу «песочницы». Основной упор разработчики делают на ограждении родительской информации от случайного удаления с устройства.

BLACKBERRY

В данной операционной система родительский контроль реализован в приложении Parental Control, доступное на BlackBerry App World.

Функционально «Родительский контроль» Blackberry похож на iOS: можно запретить установку/удаление программ, разрешить звонки на определенные телефоны, установить запрет на использование камеры и Bluetooth. Так же, как у iOS, отсутствует фильтрация контента в интернете.

ДЕТСКИЕ ПРАВИЛА. КАК РЕБЕНКУ ВЕСТИ СЕБЯ В СЕТИ ИНТЕРНЕТ

1. Никогда не размещай информацию о себе, которая может указать, на возраст.
2. Вместо фотографии использовать рисованные аватарки.
3. Настроть доступ к личным фотографиям только для самых близких людей.
4. Не переходить по подозрительным ссылкам.
5. Поддерживать дружбу только с теми, кого знаешь лично.

ВРЕДОНОСНАЯ РЕКЛАМА В СЕТИ

Баннерная реклама

Этот вид рекламы можно встретить практически на всех сайтах, но он считается самым безобидным из всех. Она предполагает лишь показ контента, а не прямое воздействие на пользователя. Единственное правило – «Если не совершать каких-либо действий над ней, то она, в свою очередь, не сможет совершить никаких действий над вами» . Проще говоря – не кликать на баннеры.

Всплывающая реклама

Одним из самых навязчивых и неприятных пользователю реклам – всплывающие окна. Эта реклама всплывает над основным контентом сайта и мешает им пользоваться. Несмотря на то, что всплывающая (pop-up) реклама очень назойлива, она считается гораздо более эффективной, нежели баннерная, т.к. ее нельзя не увидеть.

Плавающая реклама

Так же очень навязчива и раздражающая. Зачастую,

этот вид рекламы перекрывает часть контента страницы (до 30%). Рекламный блок появляется сбоку сайта и «плавает» по странице. Изменяющийся контент рекламы привлекает внимание, поэтому его просто невозможно не заметить.

Redirect-реклама

Иногда, набрав ссылку на сайт, Вы можете увидеть объявление о том, что такая страница уже не существует. При этом предлагается перейти на «рабочую» версию сайта, которая выведет на рекламу.

Одними из самых эффективных способов борьбы с такой рекламой являются расширения для браузеров. Например, Adblock, ADFender, Adguard Web filter и др.

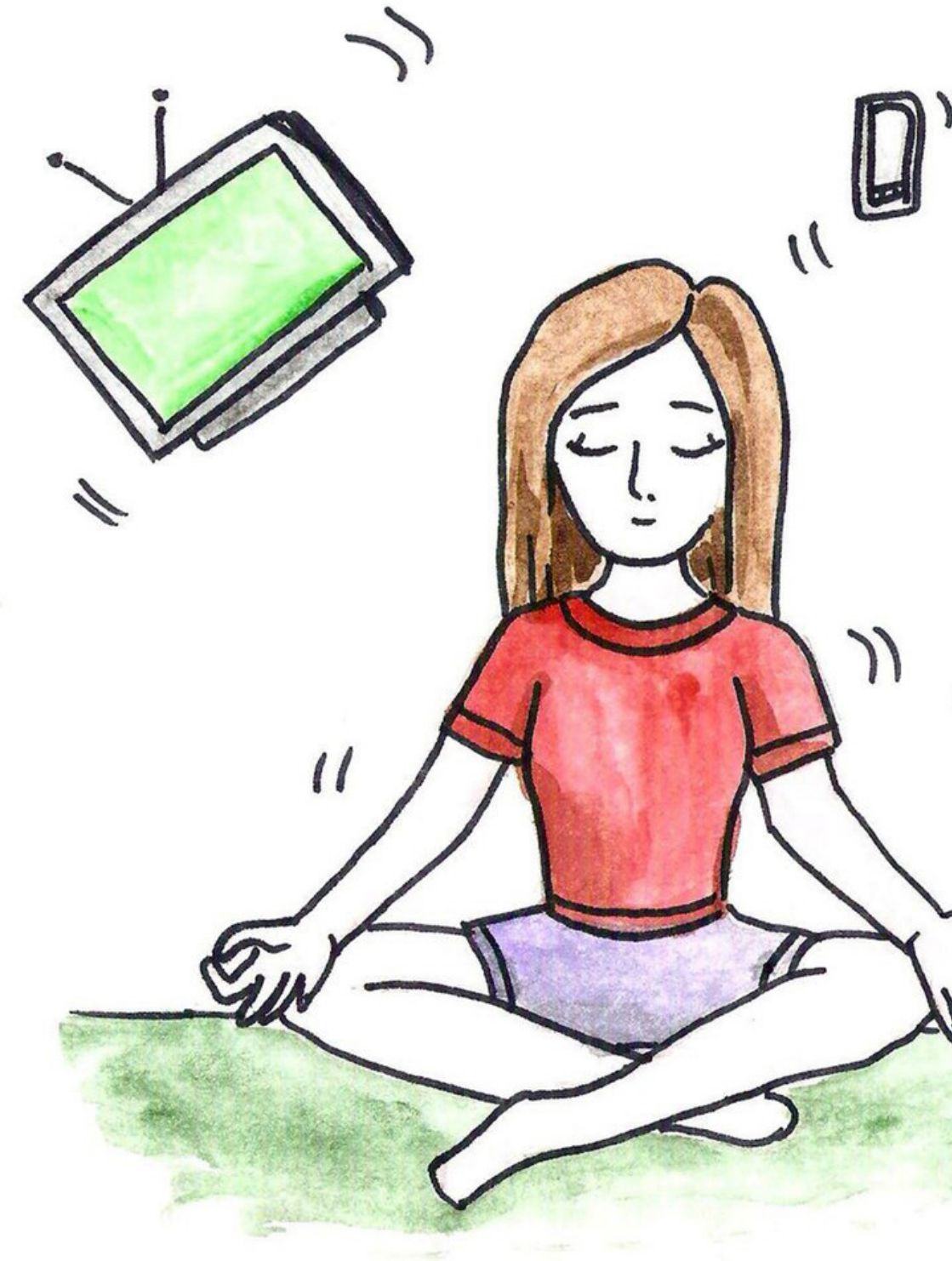
Шпионское ПО

Шпионское ПО - это такие программы, которые устанавливаются на Ваш компьютер самостоятельно, без предоставления Вам соответствующего уведомления. Зачастую шпионское ПО не подает никаких признаков своего существования, но при этом выполняет на компьютере потенциально опасные действия для Вашей информации и полноценной работоспособности ПК.

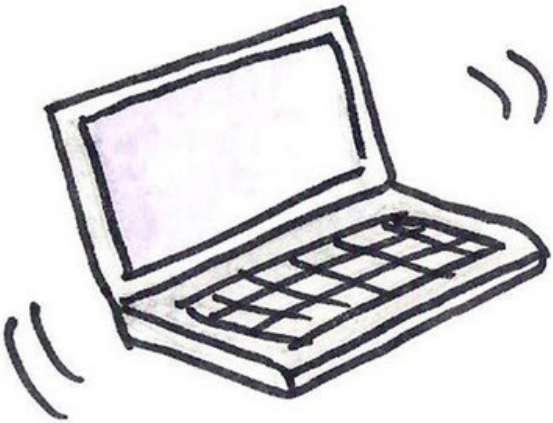
Такое ПО может заразить компьютер при установке программ из недостоверных источников, с CD, DVD-носителей и USB- накопителей. Очень часто вредоносное ПО может нанести ущерб Вашему компьютеру через бесплатный софт, заставки, либо по прямым ссылкам.

Единственный и самый верный способ борьбы и предотвращения вредоносного и шпионского ПО - это поддержание в актуальном состоянии Вашего антивирусного ПО. Также не забывайте изучать лицензионное соглашение перед установкой сомнительного ПО.

Но если все таки Ваш компьютер заражен, проведите обследование и чистку с помощью Вашего антивирусного ПО. Либо воспользуйтесь бесплатными утилитами, такими как Dr. Web CureIt и подобные.



7 DIGITAL ЭКОЛОГИЯ



«ГДЕ БЫ ТЫ НИ БЫЛ, БУДЬ ТАМ ЦЕЛИКОМ»,
ЭКХАРТ ТОЛЛЕ

ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Зависимость от интернета возникает по ряду причин и может проявляться в различных формах. Интернет-зависимость – это расстройство психики, заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии желания в нее зайти. Проявляется интернет-зависимость в следующих формах:

1. **Необходимость в беспрерывном онлайн общении.**

   Это могут быть всевозможные социальные сети, коммуникаторы, форумы, чаты и так далее. Главной группой риска в этом виде зависимости являются люди, испытывающие проблемы или дефицит реального общения. Отсутствие коммуникативных навыков погружает их в виртуальный мир, заменяющий им круг реальных друзей.

2. **Информационная интернет-зависимость (онлайн серфинг).**

   Проявляется в непреодолимой нужде в постоянном потоке новой информации и заставляет человека постоянно путешествовать по сети.

3. **Игровая зависимость.**

   В этом случае человек подсаживается и не может оторваться от онлайн игр. Многие игроки даже тратят реальные деньги, чтобы развить своих персонажей или купить дополнительные уровни ради мнимого превосходства над другими.

4. **Интернет-зависимость, связанная с азартными играми.**

   Во многом схожа с обычным пристрастием к игре на деньги. Здесь в качестве главной опасности выступают интернет-казино, которые действуют по аналогии с настоящими

5. **Киберсексуальное влечение.** Тяга к просмотру порнофильмов в сети.

В список основных видов интернет-зависимости можно добавить также хакерство; непроизвольную тягу к покупкам вещей на интернет-аукционах и в онлайн-магазинах; бесконечное скачивание с торрент трекеров видео- и аудио- материалов в целях создания собственной базы и т.д.

ЧЕМ ОПАСНА ИНТЕРНЕТ-ЗАВИСИМОСТЬ

1. Снижение концентрации внимания.
2. Ухудшение памяти.
3. Мыслительные и психические расстройства.
4. Обострение физических заболеваний.
5. Потерянное и невосполнимое для жизни время.

КАК ИЗБЕЖАТЬ ИНТЕРНЕТ-ЗАВИСИМОСТИ?

1. У вас должна быть обоснованная цель для пребывания в интернете. Планируйте, какие сайты посетить, что там сделать и посмотреть, сколько времени на это выделить.
2. Старайтесь уменьшать количество времени, которое Вы проводите в интернете, чтобы в конечном итоге свести его к минимуму.
3. Установите временной интервал для работы и отдыха в интернете.
4. Ограничьте смартфон графиком проверки сообщения, например, один раз в полчаса.
5. Выключайте телефон на ночь.
6. И самое главное, каждый раз, заходя в интернет с любого устройства, старайтесь отдать себе отчет: чему Вы хотите посвятить это время.

ЖИТЬ В ГАРМОНИИ С МЕДИАМИРОМ

С каждым годом нас все больше и больше вовлекают в медиаактивность посредством телефонов, смартфонов, планшетов и других девайсов, которые направлены на общение и работу в интернете. Мы становимся всё более зависимыми от этих девайсов, привыкая к изобилию сообщений, ведь интернет всегда под рукой. Но, действительно, очень мало людей замечает, что вовлечение в виртуальность отнимает много времени от нашей реальной жизни. Если противопоставить этому позицию, что мы многое успеваем, эффективны на работе, в учебе и т.д., то есть другой аспект, который остается за кадром, – это наш внутренний мир, внутренний голос, который фактически лишается права на высказывания. Происходит это, потому что мы постоянно находимся в ожидании сообщений, просматриваем ленту новостей, обновленя групп и друзей. И даже если мы целенаправленно заставляем себя не обращать внимания на обновления, все равно подсознательно находимся в стрессе. Фейсбук постоянно показывает уведомления об обновлениях друзей и сообществ, и если быть честным перед самим собой, то можно сказать, что обновления эти не несут значительной смысловой нагрузки, но именно они заставляют нас бросать все свои дела и просматривать их.

Постоянное вовлечение в медиажизнь становится привычкой и зависимостью. Как Вы чувствуете себя, если случайно забыли дома телефон или забыли оплатить интернет? Пустоту? Тоску? Тревогу? Все это первые признаки того, что что-то идет не так, что необходимо пересмотреть свои привычки и привязанности. Если у Вас действительно есть признаки зависимости от медиа, попробуйте отказаться от смартфона и использовать в течение одного месяца обычный мобильный телефон. Вначале будет сложно, но затем Вы привыкнете проверять почту и страницы соц. сетей посредством ноутбука или персонального компьютера в определенное время и с пониманием, для чего Вы заходите в интернет, что собираетесь там делать и сколько времени Вы готовы потратить на это. Через несколько недель появится забытое чувство: останется время для осмысления. Осмысления дел, жизни.

Умение жить в медиамире, гармонично и эффективно использовать девайсы и гаджеты, видеть мир вокруг и видеть мир внутри называется digital-экология. Освоение ее принципов является обязательно задачей каждого современного человека. Нужно беречь голос внутри себя, его легко заглушить мелодиями звонков и сообщений, но заглушив, трудно включить снова. Научитесь жить в медиа, научитесь использовать их по делу. Никогда жизнь в медиасреде не станет интереснее жизни вокруг и внутри Вас.

Вы дочитали до конца первое учебное пособие по медиаграмотности. Мы постарались охватить самые необходимые направления в медиаграмотности и жизни в медиамире. В следующей части мы расскажем о наиболее эффективных способах создания медиамира: фотографии, видеосъемке, ведении блогов и многом другом, без чего трудно сегодня называть себя медиаграмотным. А медиаграмотность – это грамотность XXI века.