ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Интернет-зависимость - навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн.

(Гриффит В., 1996)

*Фактически интернет-зависимость – это расстройство психики, заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии желания в нее зайти.

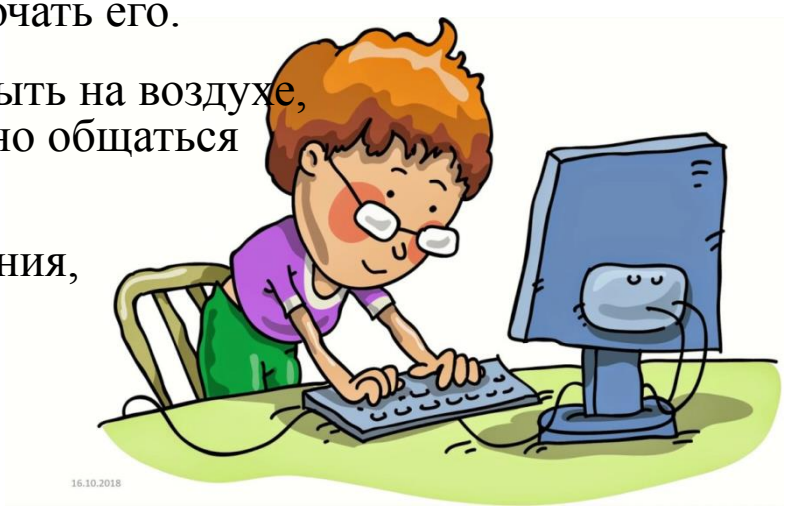
Главной группой риска в этом виде зависимости являются люди, испытывающие проблемы или дефицит реального общения. Отсутствие коммуникативных навыков погружает их в виртуальный мир, заменяющий им круг реальных друзей.

Интернет-зависимость опасна по различным причинам, которые приводят к:

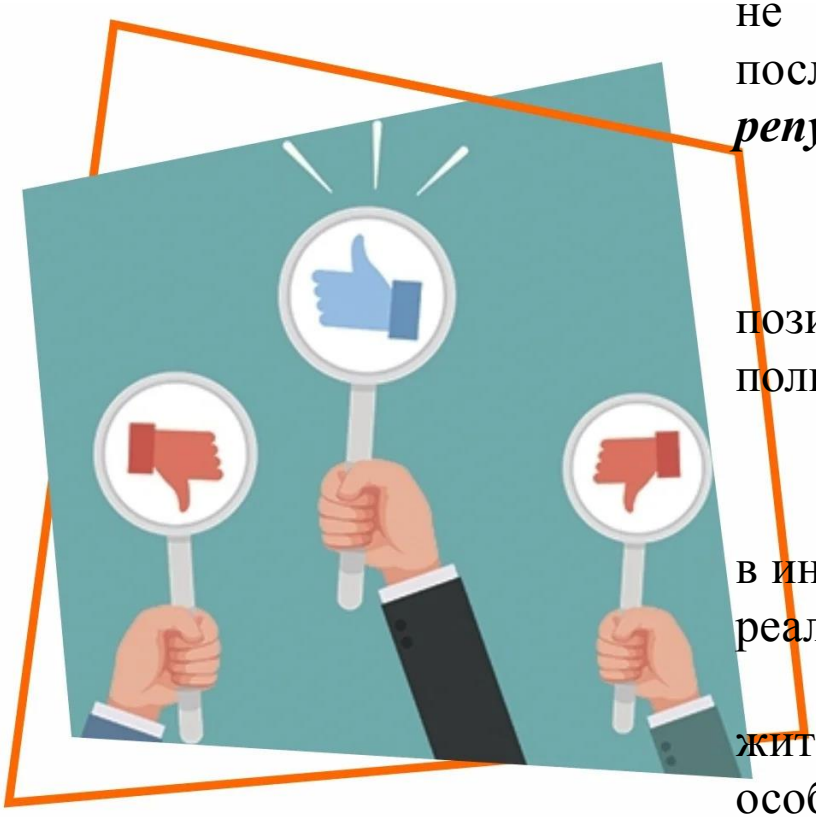
- Снижению концентрации внимания;
- Ухудшению памяти;
- Мыслительным и психическим расстройствам;
- Обострению физических заболеваний;
- Потере времени для жизни.

Однако с любой проблемой можно справиться, если осознавать в этом необходимость. Для того чтобы не попасть в компьютерную зависимость, помогут следующие действия:

- Для входа в Интернет должна быть обоснованная цель пребывания в интернете. Можно планировать, какие сайты посетить, что там сделать и посмотреть, сколько времени на это выделить. Если работа с устройством в учебных целях, необходимо следить за тем, чтобы не отвлекаться на ненужные ресурсы.
- Необходимо уменьшать количество времени, которое пользователь проводит в интернете, чтобы в конечном итоге свести его к минимуму. Возможно установление временных интервалов для работы и отдыха в интернете, а смартфон можно ограничить графиком проверки сообщения, например, один раз в полчаса, а ночью выключать его.
- Если появилось свободное время, то лучше быть на воздухе, двигаться и заниматься спортом, а также лично общаться с друзьями и знакомыми.
- Необходимо урегулировать режим сна и питания, исключив практику питания за компьютером.



Цифровая репутация



Старая пословица гласит «Написанное пером, не вырубишь и топором». В Интернете эта пословица получила название ***«Цифровая репутация».***

Цифровая репутация - это негативная или позитивная информация в сети «Интернет» о пользователе.

Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на реальной жизни.

К такой информации можно отнести место жительства, учебы, финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

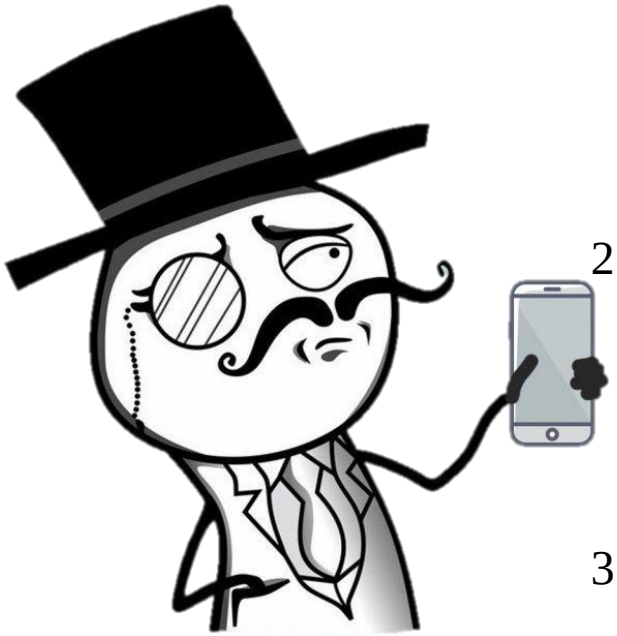
«Цифровая репутация» - это имидж, который формируется из информации в интернете.

Основные советы по защите цифровой репутации

- Перед публикацией любой информации, например, публикацией фотографии или осуществлении любого действия, например, комментирования какого-либо поста в сети «Интернет» необходимо подумать о возможных последствиях и защите себя и близких сейчас и в будущем;
- Установить в настройках профиля ограничения на просмотр профайла и его содержимого;
- Нельзя размещать и указывать информацию, которая может кого-либо оскорбить, обидеть или унизить.

Сетевой этикет

В ходе сетевого общения необходимо придерживаться следующих правил поведения:



1. Помнить о том, что ведется диалог с человеком и не забывать об эмоциональной сфере. В ходе дискуссии можно очень легко ошибиться в толковании слов собеседника, забыв, что собеседник имеет чувства, привычки, позицию и мировоззрение.
2. Необходимо следить за формулировками и используемой лексикой, избегать жаргонной и ненормативной лексики и соблюдать правила орфографии и пунктуации, поскольку любая информация может быть включена в новый контекст и поменять смысл.
3. Необходимо правильно выбирать модель поведения, ведь принимаемая в одном месте, она может быть неприемлема в другом. Также общение с друзьями может включать в себя некую расслабленность, но в коммуникации с учителями или другими лицами - это не допускается.

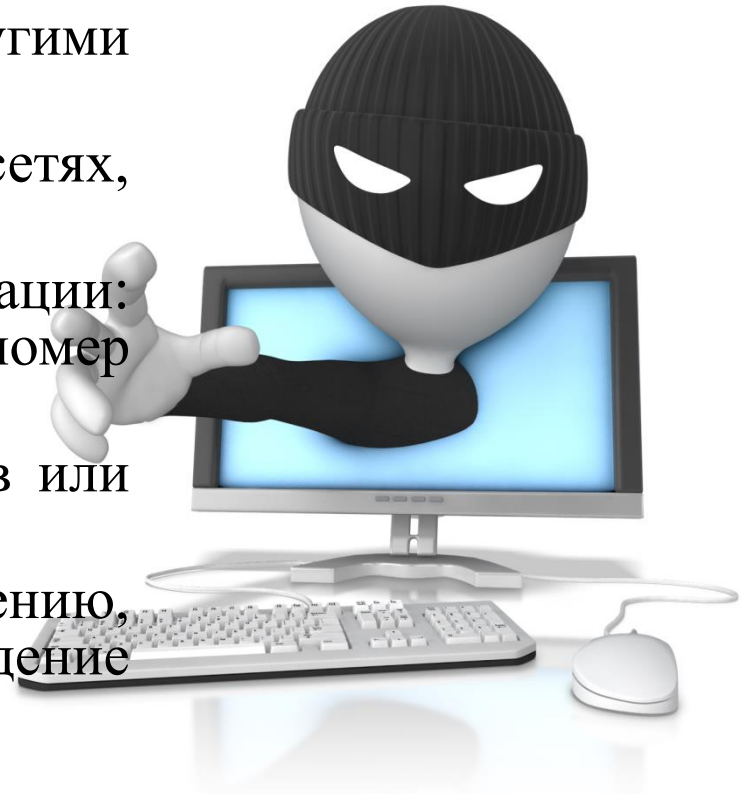
4. Проверять достоверность фактов и информации перед публикацией. Недостоверная информация способна вызвать негативную оценку со стороны собеседников.

5. Нельзя распространять личные данные, позволяющие идентифицировать пользователя, поскольку в реальной жизни его могут найти для причинения вреда его здоровью, а в сети невозможно быть абсолютно уверенным в том, что собеседник - это тот человек, за которого он себя выдает.

6. Помнить об отсутствии анонимности в сети и действии законов в сетевом пространстве. Выдавая себя за кого-то другого, оскорбляя и запугивая других пользователей, распространяя запрещенную информацию и осуществляя другие действия, незаконные или запрещенные администрацией сайта или сервиса, помнить о том, что администрация сайта или сервиса и правоохранительные органы могут определить любого пользователя по его IP-адресу.

Какие опасности есть в интернете?

- Анонимность и приватность, когда может пострадать репутация, карьера и жизнь.
- Финансовые онлайн-транзакции и снятие денег со счетов.
- Кибербуллинг и преследование другими людьми.
- Потеря аккаунтов в социальных сетях, управление группами или сайтами.
- Кража конфиденциальной информации: фотографии, паспортные данные, номер банковской карты.
- Рассылка СПАМа со своих аккаунтов или почты.
- Причинение вреда ближнему окружению, которое введено в заблуждение киберпреступниками.



Правила информационной безопасности в интернете

1. Используй безопасные и разные пароли везде. Регулярно их меняй. Отдавай предпочтение двухфакторной аутентификации и сверке по отпечатку пальца там, где наибольшие риски.

2. Меньше рассказывай о себе любимом в интернете. Эту информацию могут использовать совсем не в хороших и корыстных целях злоумышленники.

3. Не открывай незнакомые письма, а особенно подозрительные. Не переходи по ссылкам в письме. Все это чревато тем, что подвергаешься повышенному риску.

4. Установи и обновляй антивирусные программы. Это важнейший шаг к улучшению информационной безопасности.

5. Когда заходишь в социальные сети или на почту с чужого компьютера, то не забудь выйти.

6. Не пересылай конфиденциальную информацию через почту или социальные сети. Сразу удаляй сканы паспорта и документов

7. Тщательно проверяй программы и все, что скачиваешь с интернета, антивирусным обеспечением.

8. Не отвечай на спам и подозрительные сообщения. Игнорируй.

9. Банки, сервисы и магазины не рассылают подозрительных писем. В них может быть просьба перейти по ссылке или сообщить какую-то информацию. Это киберпреступники тебе пишут.

10. Не сохраняй в браузере пароли и номера банковских карт.

11. Пришло сообщение с просьбой денег? В 99,99% случаях это мошенники. Перезвони человеку по телефону или сообщи его близким, что идет рассылка СПАМа.