



Профилактика интернет - зависимости и киберрисков

Интернет-среда для студента - это и учебная площадка, и ключевой канал социализации, поэтому полный запрет интернета невозможен и неэффективен: профилактика должна строиться на развитии цифровой грамотности и формировании альтернативных офлайн-привычек.

Задача родителя - помочь взрослому ребенку увидеть разницу между использованием сети как полезного инструмента и разрушительным бегством от реальности.

Ниже подробно разобраны маркеры интернет-зависимости, правила цифровой гигиены и ключевые киберриски.

Часть 1. Профилактика интернет-зависимости (кибераддикции)

Студенты часто уходят в сеть из-за высокой тревожности, трудностей с учебой в вузе/колледже или дефицита живого общения. Виртуальный мир дает им быструю «дозу» дофамина через лайки, победы в играх и бесконечный скроллинг новостей.

Признаки формирующейся зависимости:

Потеря контроля: студент планировал зайти в сеть на 15 минут, а провел там 5 часов.

Синдром отмены (абстиненция): выраженная агрессия, сильная тревога или апатия, если временно пропадает доступ к Wi-Fi или ломается телефон.

Социальная изоляция: реальное общение с друзьями и семьей полностью заменяется виртуальным.

Разрушение быта и учебы: хронические прогулы пар, отказ от еды или сна ради нахождения в сети.

Стратегия родительской помощи

Не используйте шантаж и жесткие запреты. Отбирание роутера или смартфона у совершеннолетнего (или близкого к этому возрасту) студента вызовет только ответную ярость и окончательно разрушит ваши доверительные отношения.

Помогите внедрить «Цифровой детокс». Договоритесь о правилах, которые вы будете соблюдать *вместе* (будьте примером):

Внедрить «зоны без экранов» - никаких телефонов за обеденным столом и в кровати перед сном.

Практиковать «правило первого часа» - не брать смартфон в руки первые 30 - 45 минут после пробуждения.

Отключить **неважные всплывающие уведомления** (соцсети, маркетплейсы, игры), оставив звук только на звонках и учебных чатах.

Развивайте альтернативный досуг. Поддерживайте стремление студента к реальной активности: спорт, автошкола, живые квесты, походы, курсы рисования. Мозг должен получать дофамин из осязаемых достижений в реальном мире.

Часть 2. Защита от киберрисков (Информационная безопасность)



Студенческий возраст - основная мишень для киберпреступников, использующих методы социальной инженерии, манипуляций и шантажа.

Топ-4 главных киберриска для молодежи:

1. Цифровой след и репутация

В чем опасность: публикация избыточных личных данных, агрессивные комментарии или неоднозначные фото в открытых аккаунтах. Современные HR-специалисты крупных компаний и руководство вузов всегда проверяют профили соискателей.

Как защититься: объясните ребенку, что все попавшее в интернет, остается там навсегда. Проверьте вместе настройки приватности в соцсетях: профили должны быть закрыты от посторонних.

2. Кибербуллинг и доксинг (травля и деанонимизация)

В чем опасность: публичные оскорбления в чатах, создание фейковых страниц с целью унижения, публикация личного адреса или телефона студента.

Как защититься: Научите правилу: «**Не корми тролля**». Вступать в дискуссию с агрессорами бесполезно. Нужно делать скриншоты угроз (для возможного обращения в милицию/администрацию вуза) и отправлять обидчиков в тотальный черный список.

3. Сексторшн (сексуальный шантаж)

В чем опасность: Мошенники вступают со студентом в романтическую переписку, просят прислать интимные фото/видео, а затем под угрозой рассылки этих кадров одноклассникам, родителям и преподавателям вымогают крупные суммы денег.

Как защититься: Железное правило кибергигиены - никогда не пересылать интимные материалы в сети. Если это уже случилось и идет шантаж - **ни в коем случае не платить деньги** (требования продолжатся). Нужно немедленно закрыть аккаунты, обратиться к родителям или напрямую в правоохранительные органы.

4. Фишинг и финансовое мошенничество

В чем опасность: поддельные сайты стипендиальных программ, «выгодные» вакансии удаленной работы с требованием оплатить взнос за обучение, ссылки на покупку билетов на студенческие мероприятия, крадущие данные карт.

Как защититься: научите студента использовать двухфакторную аутентификацию (2FA) для всех аккаунтов, не переходить по ссылкам из писем-оповещений и никогда не вводить данные банковской карты на сомнительных ресурсах.

Сектор социально-педагогической и психологической работы

Телефон: **+ 375 17 369-12-70**

Эл. почта: spps2@bsmu.by

Адрес: 220083, г. Минск, пр. Дзержинского 83, корп. 6
(общежитие УО БГМУ №5), кабинет 109, 110, 113