

КОЛЛЕДЖ МЕДИЦИНСКИХ КОМПЕТЕНЦИЙ «МЕДСИ»

БЕЗОПАСНОСТЬ В ЦИФРОВОМ ПРОСТРАНСТВЕ



ПРАКТИЧЕСКОЕ РУКОВОДСТВО ДЛЯ РОДИТЕЛЕЙ

Уважаемые родители!

Ваш ребенок сделал важный шаг, выбрав одну из самых благородных профессий – медицину. Сегодня жизнь и учеба неразрывно связаны с цифровым миром. Этот мир открывает огромные возможности для обучения и общения, но и таит в себе специфические риски, особенно для будущего медицинского работника.

Цель этого руководства вооружить вас практическими знаниями. Мы расскажем, как вместе с ребенком создать безопасную цифровую среду, защитить его от мошенников и сохранить безупречную репутацию, которая критически значима для врача.

«Как педагог-психолог, я часто вижу, что тревога за детей в интернете разъединяет поколения. Мы хотим оградить, они хотят свободы. Но давайте помнить: наша главная задача не построить высокую стену, а **дать компас и научить им пользоваться**. Поэтому мои рекомендации не просто правила которые нужно соблюдать, чтобы обезопасить своего ребенка, это скорее приглашение к совместному диалогу.

Когда вы общаетесь со своим ребенком используйте «открытый диалог» проявите искренний интерес, а не пытайтесь вывести информацию будто допрашивая. Спросите не «Что ты делал в телефоне?», а «Какие смешные ролики ты сегодня смотрел? Покажешь?». Это ваш мостик в его мир.

Необходимо объяснить, что конфиденциальность - это не запрет, а правило личной безопасности, такое же, как мытье рук перед процедурой в будущей профессии. Личные данные - это как стерильный инструмент при манипуляции: свой и чужой не смешивают.

Очень болезненная тема для всех сторонников образовательного процесса это буллинг в сети (кибербуллинг). Самое важное, что вы можете сделать, стать для ребёнка надёжным тылом. Дайте ему твёрдую уверенность: «Что бы ни случилось в сети, твой дом - это то место, где тебя поймут и защитят. Мы всегда на твоей стороне».

И наконец, критическое мышление - главная вакцина против всего вредоносного в сети. Учите ребёнка задавать вопросы: «Кто это написал? Зачем? Какой реакции ждут?». Это умение, которое пригодится ему не только в соцсетях, но и в будущей врачебной практике.

Не бойтесь этого цифрового мира. Изучайте его вместе с ребенком. Ваше спокойствие, ваше доверие и ваша поддержка и есть тот самый «иммунитет», который поможет ему не заблудиться в сети и вырасти не только высококвалифицированным специалистом, но и счастливым, защищённым человеком».

*С уважением и верой в вашу семью,
педагог – психолог «Колледжа медицинских компетенций «Медси»,
Семенычева Алина Юрьевна*

Содержание:

Цифровая гигиена: основы безопасности.....	3
Особые риски: почему медики – лакомая цель для мошенников..... И как стать надежным щитом для вашего ребенка.	5
Кибербуллинг: как распознать и что делать?.....	7
Репутация будущего медика: все, что вы публикуете, может быть использовано против вас!.....	9
Куда обращаться за помощью?..... (горячие линии и ресурсы РФ)	11
Проверь свою цифровую защиту!.....	12

Цифровая гигиена: основы безопасности

Цифровая гигиена – это не просто «советы по безопасности». Для современного человека, а особенно для будущего медицинского работника, это такой же обязательный навык, как и мытье рук. Это ежедневные практики, которые защищают личные данные, репутацию и финансовые средства от цифровых угроз. Ниже приведены примеры как можно объяснить своему ребенку про цифровую гигиену и почему ее важно соблюдать.

1. Пароли и менеджеры паролей.

Проблема: Использование одного и того же простого пароля для почты, соцсетей и учебного портала является максимально небезопасным. Взлом одного аккаунта ведет к взлому всех.

Решение:

Создавайте сложные пароли: Минимум 8-12 символов, верхний и нижний регистр, цифры, специальные знаки (!, @, #). Пример: Вечер*На_ХирургииЮ52! (лучше всего использовать бессмысленные комбинации).

Уникальный пароль для каждого сервиса.

Используйте менеджер паролей: Это специальная программа (Bitwarden, KeePass, встроенные в браузеры и экосистемы Apple/Google/Яндекс), которая создает, хранит и автоматически подставляет сложные пароли. Вам нужно запомнить только один главный пароль (мастер-пароль). Это самый важный шаг.

2. Двухфакторная аутентификация (2FA/Двухэтапная проверка).

Это второй шаг для входа в аккаунт после пароля. Например, дополнительно приходящее СМС на номер телефона. Обязательно к подключению: Почта, все социальные сети (ВК, Telegram), онлайн-банк, учебный портал.

Почему это важно: Даже если мошенник украдет ваш пароль, без второго кода он не войдет в аккаунт.

3. Безопасность в социальных сетях: Ваш цифровой след.

Настройки приватности: Регулярно проверяйте, кто видит ваши посты, список друзей, фото. Установите свои настройки приватности.

Информация о себе: Не указывайте в открытом доступе точную дату рождения, домашний адрес. Мошенники используют это для социальной инженерии.

Осторожно с геолокацией: Подумайте дважды, прежде чем отмечать место учебы или домашний адрес в сторис или постах.

Доверяйте, но проверяйте запросы в друзья: Не добавляйте незнакомцев. Часто мошенники создают фейковые профили одноклассников или преподавателей.

4. Фишинг: Не клуйте на удочку!

Что это: Мошеннические письма, сообщения (ВК, SMS, email) и сайты, которые маскируются под легитимные (под колледж, банк, госуслуги). Цель - заставить вас ввести свои логин/пароль или данные карты.

Как распознать?

Срочность и угрозы: «Ваша учетная запись будет заблокирована в течение 2 часов!».

Ошибки: Орфографические ошибки, странные адреса отправителей.

Ссылки: Не нажимайте на ссылки в подозрительных сообщениях. Если сообщение якобы от колледжа - позвоните тьютору и уточните.

Неожиданность: «Вам начислена стипендия/штраф, перейдите по ссылке».

5. Обновления и антивирусы: Цифровая вакцинация.

Обновления операционной системы и программ: В обновлениях часто закрывают критические уязвимости безопасности. Включите автоматическое обновление для Windows/macOS, браузера и основных программ.

Антивирус: На персональном компьютере под управлением Windows наличие современного антивируса (даже встроенного Защитника Windows) — обязательно. Для macOS - также рекомендуется.

6. Резервные копии: Цифровая аптечка первой помощи

Что будет, если устройство украдут, оно сломается или его шифруют вирусы-вымогатели? Вы можете потерять все: конспекты, рефераты, личные фото.

Решение: Регулярно (раз в неделю/месяц) делать резервные копии важных данных на внешний жесткий диск или в надежное облако (Яндекс.Диск, Google Drive с включенной 2FA).

7. Публичный Wi-Fi: Не проводите там «операции».

Проблема: Данные, передаваемые через открытые сети Wi-Fi (в метро, кафе), могут быть перехвачены.

Решение: Не вводите пароли, не заходите в онлайн-банк и на другие критически важные сайты в публичных сетях.

Главный принцип цифровой гигиены: «Доверяй, но проверяй».

Здоровый скептицизм и внимательность в сети и есть лучшая защита. Прививайте эти привычки своему ребенку сейчас, чтобы в будущем, работая с конфиденциальными данными пациентов, они были для него естественными.

Особые риски: почему медики – лакомая цель для мошенников. И как стать надежным щитом для вашего ребенка

Выбор вашим ребенком пути медика наполняет нас глубоким уважением. Это путь служения, высокой ответственности и интеллекта. Но именно эти благородные качества, желание помочь, доступ к чувствительной информации и высокий социальный статус будущей профессии, делают студентов-медиков особой мишенью для цифровых мошенников.

Осознание этого не повод для тревоги, а **ключ к формированию мощной защиты**. Давайте посмотрим на это глазами психолога: чтобы защитить своего будущего медика, нам нужно понимать логику тех, кто пытается им манипулировать.

1. Цель: доверчивость и желание помочь.

Мошенники безжалостно эксплуатируют главную черту медицинского характера - эмпатию и готовность прийти на помощь.

Как это выглядит: Сообщение от «одногруппника»: «я в больнице, срочно нужна помощь!» или от «благотворительного фонда» с просьбой перевести деньги для срочной операции одного из педагогов. Или письмо от «деканата» с просьбой предоставить персональные данные для оформления срочной стипендии или документов.

Ваша поддержка: Объясните ребенку: «**Твое сердце - твой главный дар, но в цифровом мире сначала включи голову**». Настоящие коллеги и руководство всегда продублируют важный запрос по официальным каналам. Золотое правило: **всегда перезванивать знакомому номеру отправителя, чтобы подтвердить просьбу**. Это не недоверие, а профессиональная осторожность.

2. Цель: доступ к «дорогим» данным. Данные студента-медика - это не просто имя и фамилия. Это начало доступа к будущей медицинской практике, к базам пациентов, к рецептурным препаратам. Это ценный товар на черном рынке.

Как это выглядит: Фишинговые письма, маскирующиеся под официальные запросы от Минздрава, страховых компаний или администрации колледжа с требованием «обновить данные учетной записи» или «пройти обязательную аттестацию».

Ваша поддержка: Помогите ребенку запомнить: «**Официальные инстанции не рассылают срочные запросы на личную почту или в мессенджеры**». Настоящие документы требуют официального, часто бумажного, оформления. Настройте вместе с ним **двухфакторную аутентификацию** на почте и в соцсетях - это простейший и мощнейший барьер.

3. Цель: авторитет и репутация. Мошенники играют на страхе потерять то, что так тяжело дается - место в колледже, репутацию, возможность работать по профессии.

Как это выглядит: Сообщения о «блокировке учетной записи» в учебном портале, «нарушениях» и угрозе отчисления с требованием оплатить «штраф» или перейти по ссылке для «восстановления».

Ваша поддержка: Дайте ребенку абсолютную уверенность: «Любая подобная ситуация – это сначала ко мне, к тьютору, в учебную часть. Мы всегда разберемся вместе и поймем, где правда, а где – ложь». Ни одно учебное заведение не решает финансовые вопросы через Telegram или SMS.

Почему ваш ребенок может быть уязвим?

Не из-за наивности, а из-за колоссальной учебной нагрузки и стресса. В состоянии усталости когнитивные функции снижаются, и способность критически оценивать информацию притупляется. Мошенники именно на это и рассчитывают.

Ваша задача не контролировать, а быть надежной опорой.

Вы не можете оградить его от всех рисков. Но вы можете стать его «тыловым центром», куда он может прийти с любой проблемой без страха осуждения.

Создайте атмосферу доверия: Фраза «У меня проблемы, мне пришло странное письмо» должна встречать вашу поддержку, а не панику или упрек.

Будьте в курсе его цифровой жизни: Не как надзиратель, а как интересующийся собеседник. «Какие приложения ты используешь? Покажешь, что там интересного есть?» Это даст вам понимание его цифрового ландшафта.

Действуйте как команда: «Давай вместе разберемся, как настроить эту двухфакторную аутентификацию, я тоже хочу быть в безопасности».

Ваш ребенок учится брать ответственность за здоровье других людей. Давайте поможем ему научиться брать ответственность и за свою цифровую безопасность. Это неотъемлемая часть профессионализма современного медика.

Кибербуллинг: как распознать и что делать?

Сегодня нам с вами предстоит поговорить о тяжелой, но очень важной теме. Если буллинг (травля) – это рана, то кибербуллинг (травля в интернете) – это рана, которая никогда не затягивается. Она доступна круглосуточно, на виду у сотен и тысяч людей, а обидчик часто прячется за анонимностью. Для подростка, чья личность и самооценка только формируются, это может быть особенно разрушительно.

Ваша роль здесь неоценима. Вы можете стать тем самым «тихим портом», который поможет ребенку пережить этот шторм.

Как распознать, что ваш ребенок столкнулся с кибербуллингом?

Ребенок редко говорит прямо: «Меня травят в сети». Чаще его состояние говорит за него. Обратите внимание на эти тревожные «звоночки»:

1. Эмоциональные изменения: Резкие перепады настроения, подавленность, тревожность, раздражительность после использования телефона или компьютера. Нежелание идти в колледж, ограничивает встречи с друзьями. Возможны высказывания о собственной никчемности, ненависти к себе, нежелании «больше так жить».

2. Изменения в поведении: Ребенок неожиданно и надолго прекращает пользоваться соцсетями, удаляет свои аккаунты. Или наоборот, появляется навязчивая, нервная потребность постоянно проверять телефон, сопровождающаяся всплесками негативных эмоций. Определяются нарушения сна (нервная бессонница или постоянная сонливость), потеря аппетита или, наоборот, «заедание» стресса. Старается больше времени проводить в одиночестве, замыкается в себе, перестает делиться новостями из своей жизни.

Что делать? Алгоритм ваших первых, самых важных шагов.

Шаг 1: Обеспечьте поддержку и доверие. Это главное.

Подойдите и скажите: «Я заметил(а), что в последнее время ты выглядишь расстроенным. Мне кажется, с тобой что-то происходит. Я люблю тебя и хочу помочь. Ты не виноват(а) ни в чем, что бы ни случилось».

Выслушайте. Без критики, без немедленных советов, без фраз «сам(а) виноват(а)» или «не обращай внимания». Дайте ему выговориться и выпустить боль. Ваша задача показать, что вы на его стороне.

Шаг 2: Сохраните доказательства.

Спокойно объясните ребенку важность этого. Не удаляйте переписки, оскорбительные комментарии и скриншоты страниц. Сделайте скриншоты (желательно с захватом даты и времени). Это может понадобиться для обращения в администрацию соцсети, в колледж и/или в правоохранительные органы.

Шаг 3: Сообщите администрации социальной сети.

Практически все платформы имеют функцию «Пожаловаться» на оскорбительный контент, аккаунт или комментарий. Модераторы обязаны проверить жалобу и удалить нарушающий правила контент. Это самый быстрый способ остановить травлю в конкретном месте.

Шаг 4: Обратитесь за помощью в колледж.

Тьютор, педагог-психолог и социальный педагог – ваши первые союзники. Травля часто имеет продолжение в стенах колледжа. Образовательная организация обязана отреагировать и провести профилактическую работу с обидчиками.

Педагог-психолог колледжа окажет профессиональную поддержку вашему ребенку, поможет ему справиться с тревогой и восстановить самооценку.

Шаг 5: Не оставайтесь один на один с проблемой. Подключайте внешние ресурсы.

В России действуют специальные организации, которые профессионально помогают в таких ситуациях (на странице 11 представлена контактная информация).

Узнать больше о буллинге и способах как его преодолеть также можно на портале проекта «Вместе против буллинга». Его создали в 2021 году Департамент образования и науки города Москвы совместно с Департаментом труда и социальной защиты населения: <https://bullying.shkolamoskva.ru/#help> На портале собраны памятки, инструкции, тесты, статьи, книги, видео и даже комиксы от ведущих экспертов, которые занимаются профилактикой и борьбой со всеми видами травли.

Рекомендована к прочтению книга Натальи Цымбаленко, «Буллинг. Как остановить травлю ребенка».

Шаг 6: В серьезных случаях – обращайтесь в правоохранительные органы.

Если угрозы носят серьезный характер (угроза жизни, здоровью, распространение компрометирующих фото/видео), вы имеете полное право написать заявление в полицию или Следственный комитет РФ.

Такие действия могут подпадать под ст. 119 (Угроза убийством), ст. 110.1 (Склонение к самоубийству), ст. 128.1 (Клевета), ст. 138 (Нарушение тайны переписки), ст. 213 (Хулиганство).

Ваше заявление обязаны принять. Предоставьте собранные скриншоты как доказательства.

Чего делать НЕЛЬЗЯ:

1. Вестись на провокации и самим вступать в перепалку с обидчиком.
2. Игнорировать проблему в надежде, что само со временем уляжется.
3. Винить ребенка или лишать его доступа к интернету в качестве наказания. Это лишь усугубит его изоляцию и чувство вины.

Помните: ваше спокойствие, ваша любовь и ваши решительные, продуманные действия – это самая надежная защита для вашего ребенка. Вы не одни в этой борьбе.

Репутация будущего медика: все, что вы публикуете, может быть использовано против вас!

Дорогие наши студенты и уважаемые родители, выбранная вами профессия – одна из самых благородных и требовательных. Вы не просто получаете специальность; вы начинаете формировать профессиональную репутацию уже сегодня. В мире медицины, особенно в частных клиниках премиум-класса, таких как МЕДСИ, доверие пациента – это главная ценность. Это доверие строится не только на знаниях и навыках, но и на безупречной репутации и этике медицинского работника.

Важно понимать: для работодателя и пациентов ваши социальные сети не являются личным пространством, а становятся открытым резюме. Все, что вы публикуете сегодня, может быть использовано завтра для оценки вашей личности и профессионализма.

1. Врачебная тайна начинается в Колледже.

Это не просто юридический термин (ст. 13 ФЗ «Об основах охраны здоровья граждан»), это священный принцип профессии. Его нарушение – гарантия бесславного конца карьеры, еще не успевшей начаться.

Строжайшее табу: Никогда, ни при каких обстоятельствах нельзя выкладывать в общий доступ:

Любые данные пациентов. Даже если на фото лицо не видно, не видна фамилия. Не в коем случае нельзя публиковать фото истории болезни, назначений, экранов мониторов, табличек на дверях содержащие данные других людей.

Обсуждение случаев: Даже анонимные рассказы о «забавном» или «тяжелом» пациенте в пабликах, чатах или сторис без официального письменного согласия пациента - это грубейшее нарушение этики.

Почему это критично? Частная клиника, дорожающая своей репутацией, никогда не возьмет на работу человека, который пренебрегает конфиденциальностью. Один недоброжелательный пост может стать причиной многомиллионного иска клиники к сотруднику и повлечь уголовную ответственность.

2. Профессиональный имидж vs. личное мнение.

Будущий медик всегда на виду. Ваши взгляды и модели поведения должны соответствовать высокой.

Критика и негатив: Никогда не высказывайтесь публично в агрессивной или неуважительной форме о Колледже, преподавателях, одноклассниках, а в будущем о коллегах, Клинике или уж тем более пациентах. Работодатель справедливо решит: «Если он так говорит о других за спиной, то что же он говорит о нас и наших пациентах?».

Вредные привычки: Фотографии с алкоголем, сигаретами и другими нездоровыми атрибутами абсолютно недопустимы. Медик – это ролевая модель здорового образа жизни.

Экстремальный контент: Излишне эпатажные, провокационные фото и видео могут быть неверно истолкованы и вызвать недоверие у консервативной части пациентов.

3. Ваш профиль – это ваше лицо. Сделайте его своим союзником!

Социальные сети можно и нужно использовать с умом для построения позитивного профессионального образа.

Настройки приватности: Тщательно проверьте, кто видит ваши посты, фото списки друзей. Лучшая практика – разделение: создайте закрытый профиль для узкого круга друзей и публичный для профессионального общения.

Наполнение контентом: Наполните свой публичный профиль тем, что подчеркнет вашу увлеченность профессией. Используйте репосты новостей медицины (обязательно из официальных источников). Фото с образовательных мероприятий (конференций, семинаров). Пишите об участии в благотворительных акциях, донорстве. Давайте рекомендации по ЗОЖ (используйте только авторитетные источники).

Сетевой этикет: Общайтесь в сети уважительно, грамотно и вежливо. Это показывает вашу зрелость и культуру.

Практический совет педагога- психолога в рамках карьерного консультирования – проведите цифровой аудит прямо сейчас:

1. Введите свое имя и фамилию в поиске Google и/или Яндекс. Что увидят потенциальные работодатели?
2. Просмотрите свои социальные сети глазами руководителя отделения клиники МЕДСИ. Вы бы взяли на работу такого человека?
3. Удалите или скройте в настройках приватности всё, что может скомпрометировать вас как будущего медицинского работника.
4. Начинайте формировать свое профессиональное портфолио уже сейчас в ваших социальных сетях.

Карьера в медицине сравнима с марафоном на длительную дистанцию. Не позволяйте сиюминутной глупости в социальных сетях перечеркнуть годы вашего труда и лишит вас возможности работать в лучших клиниках страны. Ваша репутация - это самый ценный актив, который у вас есть. Берегите её.

Куда обращаться за помощью? (горячие линии и ресурсы РФ)

В сложной ситуации важно помнить: вы не одни. В России существует развитая система бесплатной помощи детям и их родителям, столкнувшимся с любыми проблемами в цифровом пространстве. Все эти службы работают анонимно и конфиденциально.

Экстренная психологическая помощь:

Круглосуточная горячая линия «Ребенок в опасности»	8 (800) 707-70-22
Телефон экстренной психологической помощи	051 с городского, 8 (495) 051 с мобильного
Круглосуточный телефон доверия	8 (800) 2000 122 с городского, 124 с мобильного

Специализированная помощь по проблемам в интернете:

Горячая линия «Травли.NET»	8 (800) 500-44-14 (пн-пт 10:00 до 20:00)
Линия помощи «Дети онлайн»	8 (800) 250 00 15

Помощь в стенах Колледжа:

Педагог-психолог колледжа: Семенычева Алина Юрьевна

График приема: по средам с 10:00 до 17:00

Запись: +7 (993) 890 38 90, кабинет 749

Обращение за помощью – это признак силы и ответственности, а не слабости. Сохраните простой номер 124 службы доверия на своем мобильном устройстве. Лучше пусть он никогда не понадобится, но в критический момент вы будете знать, куда можно быстро позвонить и вас услышат.

Проверь свою цифровую защиту!

Прохождение практики начинается с самого себя. Прежде чем помогать другим, важно обеспечить собственную безопасность. Пройди этот чек-лист вместе с родителями, чтобы твоя цифровая гигиена была безупречной!

Инструкция: Обсуди каждый пункт с родителем. Поставь галочку, когда договоритесь и выполните необходимое.

✓ Блок 1: МОЙ НАДЕЖНЫЙ ТЫЛ

«Код красный»: Мы договорились, что в любой непонятной или пугающей ситуации в сети мой первый шаг – это сказать тебе: «Мне нужна помощь». Я знаю, что ты не будешь ругать меня, а pomoжешь разобраться. Доверие – наше оружие: Мы обсудили, что можно рассказывать друг другу о новых знакомых в сети и подозрительных предложениях, не боясь осуждения.

✓ Блок 2: КЛЮЧИ ОТ ЦИФРОВОЙ КРЕПОСТИ

Двойной замок: Мы с тобой проверили и включили двухфакторную аутентификацию (2FA) на моей почте, в социальных сетях (ВК, Telegram) и других важных аккаунтах. Теперь мой аккаунт защищен как сейф! Я использую для каждого важного сайта разные сложные пароли. Мы установили и настроили менеджер паролей, чтобы их не забыть.

✓ Блок 3: БДИТЕЛЬНОСТЬ У ОПЕРАЦИОННОГО СТОЛА

Правило «Не кликай!»: Я знаю, что нельзя переходить по подозрительным ссылкам из писем, сообщений от незнакомцев или с надписью «Срочно!». Я всегда проверю информацию через официальные каналы. Никакой фишинг не поймает нас на крючок.

✓ Блок 4: ЧИСТОТА МЕДИЦИНСКОЙ МАНТИИ

Врачебная тайна – свята: Я твердо усвоил(а): НИКАКИХ фото и видео пациентов (даже их спин!) и медицинских документов. Моя будущая репутация дороже лайков. Мой цифровой след – мое резюме. Я понимаю, что работодатели (например, из сети клиник МЕДСИ) смотрят социальные сети. Я проверю свои профили и удалю или скрою всё, что может испортить мнение о мне как о профессионале.

✓ Блок 5: ПЛАН СПАСЕНИЯ НА СЛУЧАЙ ЧП

Скриншот является доказательством. Я знаю, что если меня травят или шантажируют, первым делом сделать скриншот, а не удалять переписку. У меня в телефонной книге есть номер 124. Я знаю, что наша команда – это еще и тьютор, педагог-психолог и социальный педагог колледжа, и мы не боимся к ней обратиться.

Все пункты пройдены? Поздравляю! Ты не только заботишься о своем здоровье, но и обеспечиваешь безопасность своей будущей профессии.

Цифровая гигиена – это навык настоящего профессионала!