

**Государственное бюджетное профессиональное образовательное
учреждение «Уральский медицинский колледж»**

Исследовательский проект

«КИБЕРгигиена - наш щит в цифровом мире»

Кочкина Валерия, Борисова Дарья
1 курс, группа Л2-25, специальность
31.02.01 «Лечебное дело»

Научный руководитель:
Шумкова Наталья Юрьевна, преподаватель
ГБПОУ «Уральский медицинский колледж»
Лысьвенский филиал

**Пермский край, г.Лысьва,
2025 г.**

Содержание

1.	Введение	3
2.	Основная часть	5
2.1.	Некоторые результаты исследований об использовании интернета жителями России	5
2.2.	Организация мероприятий по реализации исследовательского проекта: «КИБЕРгигиена - наш щит в цифровом мире»	6
2.3.	Реализация проекта	7
3.	Заключение	17
4.	Библиографический список	19
5.	Приложения	20

1.Введение

Актуальность проекта

Многие понимают значение гигиены тела и жилья. Знаем, что необходимо мыть руки, принимать душ, стричь ногти, следить за чистотой волос, одежда должна быть чистой и опрятной, а дома необходимо убираться и проветривать. Со всеми этими правилами мы знакомимся с самого детства.

Многие отмечают, что нахождение в сети Интернет занимает большую часть дня. Это не делает здоровье человека более крепким. К сожалению, в последнее время активизировались не только вирусы, но и киберпреступники. Как же может защитить себя в сети Интернет современный пользователь? Существуют ли правила гигиены при работе в сети Интернет?

Все это обуславливает актуальность выбранной темы исследовательского проекта: «КИБЕРгигиена - наш щит в цифровом мире».

Объект исследования: процесс формирования культуры безопасного поведения студентов в онлайн-пространстве.

Предмет исследования: влияние практических мероприятий по кибергигиене на уровень ответственности и защищенности студентов в Интернете.

Гипотеза: организация практических мероприятий по кибергигиене среди студентов приведет к более ответственному и защищенному поведению в онлайн-пространстве.

Цель проекта: повышение уровня осведомленности и формирование устойчивых навыков безопасной работы в Интернете среди студентов посредством организации и проведения практических мероприятий по вопросам кибергигиены.

Задачи:

Определить контрольную группу студентов (далее КГ) для реализации проекта;

- * Изучить данные о киберпреступности и рисках поведения в сети Интернет, а также о способах защиты – кибергигиене;
- * Выявить уровень настороженности студентов КГ к теме рисков и угроз сети Интернет, а также уровень владения культурой КИБЕРгигиены;
- * Провести занятие «Безопасная цифра и полезные цифровые привычки» по методу кейс-стади;
- * Организовать челлендж - марафон «#КИБЕРгигиена» среди студентов;
- * Организовать «Учебный день без телефона» среди студентов контрольной группы и провести опрос по его результатам;
- * Подготовить наглядные информационные материалы: стенгазеты, буклеты, чек – лист по Кибергигиене и безопасному поведению, распространить среди студентов, в социальной сети колледжа ВКонтакте;
- * Сформировать кейс материалов для дальнейшего использования;
- * Провести анализ и сделать выводы по проведенной работе.

Реализация проекта предусматривает организовать мероприятия в деятельностном режиме.

Сроки реализации проекта: 27.10.2025 – 27.11.2025

Целевая группа: студенты группы Л2-25 «Лечебное дело», 1 курс, ГБПОУ «Уральский медицинский колледж», по возможности – студенты 1 курса других групп.

Применяемые методы исследования: анкетирование, опрос, наблюдение, анализ результатов

2. Основная часть

При знакомстве с темой киберугроз, кибербезопасности и кибергигиены мы изучили последние данные об использовании всемирной сети и преступности.

2.1 Некоторые результаты исследований об использовании интернета жителями России:

По данным «**DataReportal**» сервиса, который занимается аналитикой мирового цифрового пространства, который ежегодно составляет и публикует отчёты по развитию цифровых технологий в мире[1]:

- В начале 2025 года в России было зарегистрировано **216 миллионов** мобильных подключений, что эквивалентно **150%** от общей численности населения
- По состоянию на январь 2025 года количество интернет-пользователей в России составило **133 миллиона** человек, а уровень проникновения интернета составил **92,2%**
- В начале 2025 года в России насчитывалось **106 миллионов** пользователей социальных сетей, это **73,4%** от общей численности населения
- По данным исследования, российские пользователи проводят в интернете более 8 часов в день. Основные причины этого: поиск информации (80,4%), отслеживание актуальных новостей и событий (66,1%), общение с семьёй и друзьями (65,6%), просмотр видео, ТВ-шоу и фильмов (64,0%)

Вместе с большим охватом растёт и уровень КИБЕР преступности.

По данным **МВД** [2], всего в январе-июле 2025 года зарегистрировано 425 тыс. преступлений, совершенных с использованием Интернет, количество несовершеннолетних, пострадавших от киберпреступлений за девять месяцев 2025 года, возросло на 120%, сообщило управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий в МВД [3]

Получив такие данные, мы пришли к выводу, что необходимо регулярно проводить работу по обучению пользователей безопасному поведению в сети Интернет.

2.2 Организация мероприятий по реализации исследовательского проекта: «КИБЕРгигиена - наш щит в цифровом мире»

Кибергигиена – это набор ежедневных привычек, знаний и навыков, которые позволяют существенно снизить риски работы в Интернете.

Некоторые из этих практик:

- **Регулярное обновление программного обеспечения.** Установка обновлений и патчей безопасности для операционных систем, приложений и устройств.
- **Использование сложных паролей.** Применение уникальных, сложных паролей для каждой учётной записи.
- **Многофакторная аутентификация (MFA).** Включение многофакторной аутентификации для всех учётных записей, где это возможно. Это добавляет дополнительный уровень защиты.
- **Регулярное резервное копирование данных.** Настройка автоматического резервного копирования данных на внешние носители или облачные хранилища.
- **Осторожное обращение с подозрительными сообщениями.** Не открытие вложений и не переход по ссылкам в письмах от неизвестных отправителей.
- **Использование антивирусного и защитного программного обеспечения.** Установка антивирусного ПО и регулярное его обновление.
- **Безопасное использование общедоступных сетей.** Избегание использования общедоступных Wi-Fi сетей для передачи конфиденциальной информации.

Всеми этими действиями должны владеть пользователи Интернет. Знать и применять их – значит защищать себя.

Для реализации проекта мы определили контрольную группу – студенты ГБПОУ «Уральский медицинский колледж» Лысьвенского филиала, группа Л1-25, специальность «Лечебное дело», в количестве 26 человек.

Выбор контрольной группы был обусловлен параметрами:

- это наши одноклассники, один возраст, общие интересы,
- с ними проще организовать мероприятия, зная расписание учебных занятий,
- желание организовать общую деятельность для сближения, лучшего узнавания друг друга;

2.3 Реализация проекта

1. **Вводное анкетирование – 29.10.2025 г** В группе 26 человек, приняли участие – 25 человек (один студент болел).

Итоги:

- ✓ О киберпреступлениях слышали 23 человека – (%),
- ✓ 5 (%) человек были жертвой киберпреступников один раз, 7 – 2 раза, 1- более двух раз, 12 человек не подвергались угрозам.
- ✓ 19 опрошенных пользуются антивирусным программным обеспечением, 3 из всех меняют пароли каждый месяц, 11 человек раз в полгода, 11 человек не меняют пароли
- ✓ Подозрительные сообщения игнорируют и удаляют – 100 % опрошенных
- ✓ Двухфакторную аутентификацию используют 21 студент (%) , 4 не используют
- ✓ Больше всего опрошенных беспокоят: кражи личных данных, взломы, вредоносное ПО
- ✓ 20 человек не используют общедоступные сети WI-FI при работе с личной безопасностью, т.к. знают о рисках

- ✓ Наиболее эффективными методами защиты считают: информирование и обучение – 15 человек, ответственность пользователей – 9 ответов, обновление законодательства – 5 ответов
- ✓ 18 человек считают, что на уроках достаточно говорят о кибербезопасности

Вывод: уровень настороженности студентов контрольной группы к теме рисков и угроз сети Интернет удовлетворительный, уровень владения культурой КИБЕРгигиены – достаточный. Однако:

- * Не все студенты серьезно относятся к надежности паролей,
- * Не все используют двухфакторную аутентификацию,
- * Не все интересуются тем, какие новые риски и угрозы появляются в последнее время, что может послужить опасностью.

2. Занятие «Безопасная цифра и полезные цифровые привычки» по методу кейс-стади – 08.11.2025

Участники – группа Л1-25, пригласили для участия студентов группы Л2-25. Общее количество – 43 студента. В основе разработка занятия «Разговоры о важном» от 23.01.2023 г «Медиаграмотность и цифровая гигиена» [4].

Распределение участников по группам: 1. «Кибермошенники» 2. «Специалисты по безопасности» 3. «Эксперты».

Метод «Кейс-стади» предполагает следующие этапы:

- 1) интерактивная мини-лекция по теме мероприятия;
- 2) выдача ситуаций каждой команде и их решение на основании полученной информации и имеющегося у участников опыта;
- 3) защита решённой ситуации перед остальными участниками, подведение итогов, рефлексия.

В ходе мероприятия студенты решали кейс ситуаций с точки зрения «Кибермошенников» и «Специалистов по безопасности», обсуждали, заслушивали мнение «Экспертов». Также смотрели видеоролики по теме занятия.

Для повышения знаний в области кибергигиены был проведен мастер-класс «Поговорим о паролях», где мы рассказали о надёжных паролях и показали способы их составления.

ИТОГИ: Собрали отзывы о проведенном мероприятии, актуальности темы.

По отзывам – тема мероприятия актуальна, важна. Много положительных отзывов о том, что узнали, как составить надежный пароль.

Студенты получили домашнее задание – снять видеосюжет на тему кибербезопасности.

3. Челлендж - марафон «#КИБЕРгигиена» - 08.11-18.11. 2025

В течение 10 дней проводилась работа:

- ✓ съемка видеосюжетов на тему безопасного поведения в сети Интернет студентами;
- ✓ просмотр и выбор сюжетов для публикации в соц.сетях организаторами проекта. Требования: содержательность, творческий подход, эстетичность;
- ✓ публикация роликов с хештегами:

#МыАктивныеУМК#КИБЕРгигиена#ЧелленджМарафонУМК#ДорогамиДобра
ПК#ИнформационнаяКультураУМК#ЦифроваябезопасностьУМК

ИТОГ: В марафоне приняли участие 39 студентов, снято 29 роликов, размещены в социальной сети Контакте <https://vkvideo.ru/@club232357926> и на личных

страницах студентов. В видеороликах студенты рассказали о способах защиты данных, о безопасном поведении в сети Интернет, о полезных привычках.

4. Акция «Учебный день без телефона» среди студентов – 20.11.2025

Цель: привлечение внимания студентов к проблеме зависимости от технологий и стимулирование осознания ценности живого общения

Накануне проведения обсудили, что в любой день недели состоится акция, предупредили родителей в чате.

Телефоны были сданы на хранение куратору группы на время учебных занятий. Участникам было предложено отслеживать своё состояние в течение дня. В свободное время были организованы: настольные игры- шашки, ходилки, игра в теннис, раскрашивание антистрессовых раскрасок, общение. По окончании уроков проведен опрос.

ИТОГИ: участие приняли 24 студента, по результатам опроса:

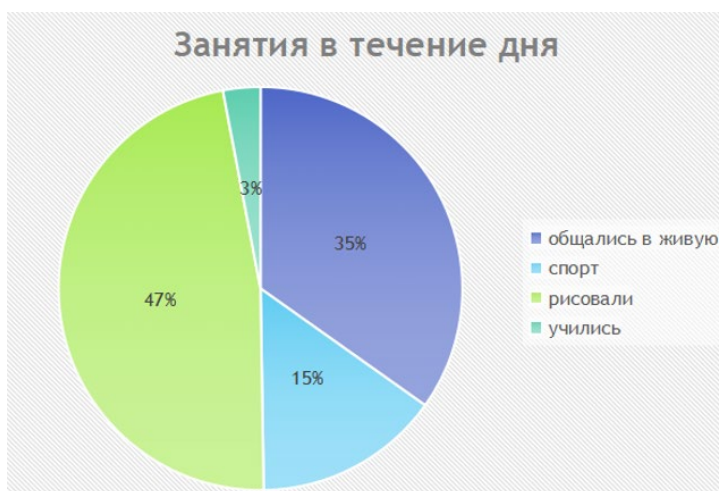
1. Моё обычное время в Интернете: 3-5 часов – 6 человек, 5-8 часов – 8 человек, более 8 часов -10 человек



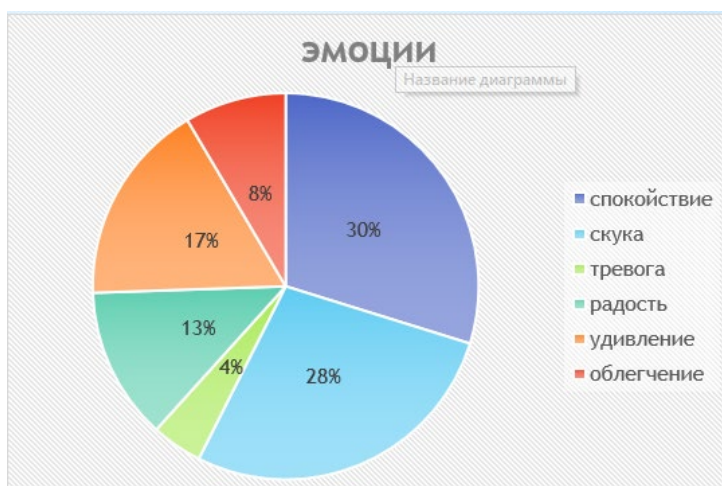
2. Интернет-сервисы, которые я посещаю: соц.сети – 19 человек, мессенджеры – 18 человек, онлайн-магазины- 6 человек, новостные сайты – 3 человека



3. Чем занимались в течение этого дня: рисовали – 47%, общались «в живую» - 35%, занимались спортом- 15%, учились без телефона – 3 %



4. Какие эмоции вы испытали: - спокойствие без телефона -30%, скука – 28 %, удивление – 17%, радость от того, что не отвлекает ничего – 13%, облегчение – 8%, тревога – 4%

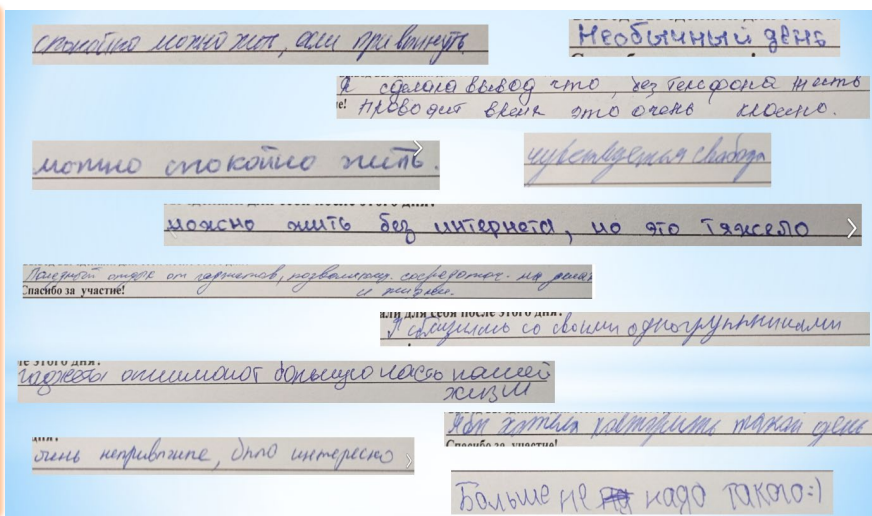


5. Какие сложности вы отметили, находясь без телефона:

Отсутствие связи с друзьями/родными – 11 человек, невозможность получить информацию – 7, нехватка развлечений – 8, трудности с учебной -1, ощущение оторванности от мира – 3, никаких - 4

6. Что понравилось: больше времени для общения – 16 ответов, отдых для глаз и мозга – 12 ответов, чувство свободы от гаджетов – 9, возможность сосредоточиться на делах -7, новые занятия – 5.

7. Нужно ли повторить этот опыт: да - 5 ответов, иногда надо – 12, нет – 7 ответов



ВЫВОД: большая часть студентов тратит более 8 часов в день на свой телефон. Их основное занятие – переписка в мессенджерах и посещение соцсетей, либо покупки в онлайн-магазинах. При проведении «Дня без телефона» они испытали тревогу, что не справятся с заданиями на уроке, т.к. не будет возможности посмотреть, при этом большинство отметило, что этот день дал возможность живого общения, занятий спортом, сплочения. Те, кто проводит с телефоном почти весь день испытывали стресс, нервничали, ощутили состояние потери во времени, т.к. у них отсутствовали часы. Большинство студентов считает, что такой опыт нужно иногда повторять – 1-2 раза в месяц, но в тот день, когда по расписанию стоит 2 пары занятий.

Считаем, что мероприятие «задело за живое» группу, оставило впечатления и привлекло внимание к тому, сколько времени тратится на пребывание в Интернете.

5. Подведение итогов, работа по заполнению чек-листа по безопасному поведению в сети Интернет, беседа о правах и ответственности – 21.11.2025 г.

При подведении итогов мы провели обсуждение со студентами и предложили заполнить Чек-лист по Кибергигиене, который был составлен нами заранее.

ЧЕК-ЛИСТ ПО КИБЕРГИГИЕНЕ

- ☐ 1. Использую двухфакторную аутентификацию - помимо классического пароля при каждом входе в систему требуется ввести дополнительный код, который придет на почту или телефон.
- ☐ 2. Надежный пароль - не только цифры, еще и буквы и знаки пунктуации, количество 10-12
- ☐ 3. Не даю себя обмануть: фишинговые сайты - точные копии известных оригиналов, но основное отличие состоит в доменном имени, в которое вносятся коррективы. Внимательно проверяю адресную строку!
- ☐ 4. Имею запасной почтовый ящик для регистрации на сайтах, вызывающих сомнения.
- ☐ 5. Я осторожен с общественным Wi-Fi.
- ☐ 6. Устанавливаю антивирусные программы.
- ☐ 7. Не пренебрегаю резервным копированием. Создаю резервную копию важных данных на съемном носителе или в облаке.
- ☐ 8. Не публикую в социальных сетях личную информацию: домашний адрес, личные фотографии, номер телефона, номера кредитных карт, билеты, фото с видом из окна.

☐9. Перед утилизацией или продажей компьютера, планшета или смартфона, выполняю очистку жесткого диска, чтобы не допустить доступ третьих лиц к персональным данным.

☐10. Меняю пароль каждые 3 месяца

ИТОГИ: По отзывам студентов, на сегодняшний день они:

- не меняют пароль каждые 3 месяца, считают, что это не обязательно;
- не создают резервных копий своих файлов, т.к. не сталкивались с потерей данных;
- не создают запасной почтовый ящик для регистрации на сайтах, вызывающих сомнения.

Остальные правила гигиены студенты соблюдают.

ВЫВОД: В настоящий момент студенты знают о способах кибергигиены, но пользуются не всеми ресурсами. **Приучать себя к выполнению полезных привычек поведения в сети Интернет нужно постоянно.**

Беседа о правах и ответственном поведении

Очень важно знать свои права при пользовании ресурсами сети Интернет, а также не забывать об ответственности.

Право на конфиденциальность — защита личных данных, таких как переписки, фото и финансовая информация.

☐**Право на доступ к информации** — возможность свободно получать информацию из интернета.

☐**Право на свободу самовыражения** — возможность делиться своими мыслями и идеями в интернете, соблюдая правила платформы.

☐**Право на безопасность** — защита от киберугроз, таких как взлом или кража данных.

Ответственность за киберпреступления в России предусмотрена главой 28 Уголовного кодекса РФ.

Также за нарушения в сфере информационных технологий может наступить административная ответственность.

□ К уголовной ответственности привлекаются лица, достигшие 16 лет.

Статья 272 — неправомерный доступ к охраняемой законом компьютерной информации, если деяние повлекло уничтожение, блокирование, модификацию или копирование информации. Наказание — штраф, исправительные работы, ограничение свободы или лишение свободы.

□ Статья 273 — создание, использование и распространение вредоносных компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации или копирования информации. Наказание — ограничение свободы, принудительные работы или лишение свободы.

□ Статья 274 — нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшее уничтожение, блокирование, модификацию или копирование информации. Наказание — штраф, исправительные работы, ограничение свободы или лишение свободы.

Административная ответственность

□ Статья 13.12 — нарушение правил защиты информации, например, использование несертифицированных информационных систем, баз и банков данных. Наказание — административный штраф и др.

Также мы попросили студентов посмотреть свои подписки и удалить те группы, которыми они не пользуются. Сделки с группами через биржи-посредники могут быть связаны с мошенничеством, например, с подделкой статистики сообщества

или недобросовестными гарантами. Для того, чтобы обезопасить себя - лучше раз в месяц отписываться от сообществ, которые не актуальны.

6. Изготовление наглядных информационных материалов

Чтобы распространить знания по Кибергигиене, мы изучили данные о пользе и вреде работы на компьютере. Отсортировав самое важное, мы оформили буклет с советами «Как не испортить здоровье при работа за компьютером».

В результате проведения работы по реализации проекта был подготовлен кейс материалов, который может быть использован педагогами или студентами для проведения мероприятий.

3. Заключение

Проведенное исследование было посвящено изучению влияния организации практических мероприятий по кибергигиене на формирование устойчивого и ответственного поведения студентов в онлайн-пространстве.

Объектом исследования являлся процесс формирования культуры безопасного поведения студентов в сети Интернет, предметом изучения стало воздействие конкретных мероприятий на уровень защиты и ответственность пользователей.

В ходе реализации проекта была достигнута **поставленная цель**: повышение уровня осведомленности и формирование устойчивых навыков безопасной работы в Интернете среди студентов посредством организации и проведения практических мероприятий по вопросам кибергигиены.

Основные выводы заключаются в следующем:

1. Проведение регулярных практических занятий, акций, мероприятий существенно повысило уровень информированности студентов о рисках и угрозах, существующих в цифровом пространстве, что было выявлено при опросах, анкетировании и устных отзывах участников.
2. Участники мероприятий продемонстрировали значительное улучшение понимания принципов безопасного пользования сетью Интернет, включая защиту персональных данных, грамотное использование паролей и антивирусных решений, эти данные были получены при заполнении итогового Чек-листа по кибергигиене.
3. Практическое применение полученных знаний позволило сформировать устойчивые привычки и навыки ответственного поведения в виртуальной среде. Студенты смогли поделиться своими знаниями в снятых ими клипах на тему Кибербезопасности. При организации акции «Учебный день без телефона» было акцентировано внимание на проблемы ухода в виртуальное общение взамен

живого взаимодействия. Участники отметили важность проведения акции 1-2 раза в месяц.

Таким образом, проект подтвердил эффективность предложенных методов повышения кибергигиены среди студенческой аудитории.

Деятельностный характер проекта позволил вовлечь 26 студентов контрольной группы и 22 студента смежной группы в процесс реализации, предоставил возможность применять знания на практике, способствовал развитию личностных качеств - умение работать в команде, проявлять творческий подход, развивал критическое мышление участников, сплотил коллектив. Все мероприятия, акции были направлены на повышение уровня информационной культуры.

Выдвинутая гипотеза доказана: организация практических мероприятий по кибергигиене среди студентов приводит к более ответственному и защищенному поведению в онлайн-пространстве.

Полученный опыт реализации проекта может служить основой для разработки дальнейших образовательных инициатив, направленных на обеспечение информационной безопасности молодёжи. Разработанные и собранные нами мероприятия можно реализовать на любой студенческой группе.

Результаты проведённого исследования представляют ценность для педагогов, заинтересованных в формировании компетентных пользователей цифровых технологий.

Библиографический список

Используемые интернет-ресурсы:

1. https://www.web-canape.ru/business/statistika-interneta-i-socialnyh-setej-rossii-na-2025-god-glavnye-trendy-i-cifry/?ysclid=mi986hi9t368153984&utm_referrer=https%3a%2f%2fya.ru%2f
2. <https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd/?ysclid=mi98evxryv816104166>
3. <https://www.rbc.ru/rbcfreenews/68fe33d49a79474834407c53?ysclid=mi98rwv eii632881091>
4. <https://разговорыоважном.рф/?ysclid=mi99os1yd4780600813>

Приложение 1

Опрос «День без интернета»

Цель опроса: изучить эмоциональный и поведенческий опыт участников после проведения одного дня без доступа к интернету.

Инструкция: ответьте на все вопросы, выбрав подходящий вариант или написав свой ответ. Ваше мнение очень важно!

1. Сколько часов в обычный день вы проводите в интернете?

менее 1 часа; 1–3 часа; 3–5 часов; 5–8 часов; более 8 часов.

2. Какие интернет-сервисы вы используете чаще всего? (можно выбрать несколько)

социальные сети; мессенджеры; онлайн-магазины; новостные сайты; образовательные платформы; рабочие/учебные сервисы; другое (укажите): _____.

3. Что вы делали в течение дня без интернета? (выберите основные занятия)

общались с близкими вживую; занимались спортом; рисовали; учились без онлайн-ресурсов; другое (укажите): _____.

4. Какие эмоции вы испытывали в течение дня без интернета? (можно выбрать несколько)

спокойствие; скуку; тревогу; радость; раздражение; удивление; облегчение; другое (укажите): _____.

5. Что было самым сложным в этот день?

отсутствие связи с друзьями/родителями; невозможность получить нужную информацию; нехватка развлечений; трудности с учёбой; ощущение оторванности от мира; другое (укажите): _____.

6. Что вам понравилось в этом дне?

больше времени для живого общения; возможность сосредоточиться на делах; отдых для глаз и мозга; открытие новых занятий; чувство свободы от гаджетов; другое (укажите): _____.

7. Хотели бы вы повторять такой опыт?

да, регулярно (например, раз в месяц); иногда, время от времени; нет; затрудняюсь ответить.

8. Какой вывод вы сделали для себя после этого дня?

Спасибо за участие!

Приложение 2

ЧЕК-ЛИСТ ПО КИБЕРГИГИЕНЕ



- ✓ 1. Использую двухфакторную аутентификацию - помимо классического пароля при каждом входе в систему требуется ввести дополнительный код, который придет на почту или телефон.
- ✓ 2. Надежный пароль - не только цифры, еще и буквы и знаки пунктуации, количество 10-12
- ✓ 3. Не даю себя обмануть: фишинговые сайты - точные копии известных оригиналов, но основное отличие состоит в доменном имени, в которое вносятся коррективы. Внимательно проверяю адресную строку!
- ✓ 4. Имею запасной почтовый ящик для регистрации на сайтах, вызывающих сомнения.
- ✓ 5. Я осторожен с общественным Wi-Fi.
- ✓ 6. Устанавливаю антивирусные программы.
- ✓ 7. Не пренебрегаю резервным копированием. Создаю резервную копию важных данных на съемном носителе или в облаке.
- ✓ 8. Не публикую в социальных сетях личную информацию: домашний адрес, личные фотографии, номер телефона, номера кредитных карт, билеты, фото с видом из окна.
- ✓ 9. Перед утилизацией или продажей компьютера, планшета или смартфона, выполняю очистку жесткого диска, чтобы не допустить доступ третьих лиц к персональным данным.
- ✓ 10. Меняю пароль каждые 3 месяца
- ✓

БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ С МЕНЯ!!!!

Приложение 3. Буклет

Наша команда



Наталья Юрьевна Шумкова
Преподаватель, советник директора по воспитанию, куратор группы Л2-25



Дарья Борисова
Студент группа Л2-25
Лечебное дело



Валерия Кочкина
Студент группа Л2-25
Лечебное дело

Положительные и отрицательные аспекты влияния персонального компьютера (ПК):

****Положительные аспекты влияния ПК:****

- Повышение технической грамотности;
- Развитие логического мышления;
- Увеличение скорости реакции и принятия решений;
- Улучшение памяти;
- Повышение концентрации внимания;
- Развитие визуального восприятия объектов;
- Возможность общения с друзьями, живущими далеко;
- Улучшение навыков поиска и получения разнообразной информации.

****Отрицательные аспекты влияния ПК:****

- Электромагнитное излучение;
- Проблемы со зрением и осанкой;
- Малоактивный образ жизни;
- Вредная и непроверенная информация из Интернета;
- Развитие компьютерной зависимости;
- Сильное нервное напряжение;
- Быстрая утомляемость;
- Эмоциональные стрессы.

Таким образом, ПК оказывает как положительное, так и отрицательное влияние на человека, и важно использовать его с умом, чтобы минимизировать негативные последствия.



ГБПОУ
"УРАЛЬСКИЙ
МЕДИЦИНСКИЙ
КОЛЛЕДЖ"

КИБЕРГИГИЕНА НАШ ЩИТ В ЦИФРОВОМ МИРЕ



Пермский край, г.Лысьва
2025 год

Опасные и вредные факторы при работе с компьютером

- **Повышенный уровень рентгеновского, ультрафиолетового и инфракрасного излучения****
Эти виды излучения могут вызывать повреждения тканей организма, включая кожу и глаза, а также повышать риск развития различных заболеваний, включая онкологические.
- **Запыленность воздуха рабочего пространства****
Высокая концентрация пыли в воздухе может привести к заболеваниям дыхательных путей, аллергиям и ухудшению общего самочувствия.
- **Неравномерное распределение яркости в поле зрения****
Может вызывать зрительное напряжение, усталость глаз, снижение работоспособности и повышать риск ошибок при выполнении задач.
- **Повышенный уровень пульсации светового потока****
Мерцание света (пульсация) негативно влияет на зрение, вызывает головные боли, усталость и снижает концентрацию.
- **Возможность поражения статическим электричеством****
Статическое электричество может привести к неприятным ощущениям, а в некоторых случаях — к повреждению электронного оборудования или даже к возгоранию.
- **Повышенный уровень напряжения в электрической цепи, замыкание которой может пройти через тело пользователя****
Представляет серьезную опасность поражения электрическим током, что может привести к травмам или смерти.

Как не испортить здоровье за работой за компьютером

- Правильная организация рабочего места**
 - Используйте удобное кресло с поддержкой спины.
 - Расположите монитор на уровне глаз, чтобы не наклонять голову.
 - Держите клавиатуру и мышь на удобной высоте, чтобы не напрягать запястья.
- Регулярные перерывы**
 - Каждые 45-60 минут делайте короткий перерыв на 5-10 минут.
 - Вставайте, разминайтесь, делайте простые упражнения для глаз и тела.
- Упражнения для глаз**
 - Следуйте правилу 20-20-20: каждые 20 минут смотрите на объект, находящийся на расстоянии около 6 метров в течение 20 секунд.
 - Моргание помогает увлажнять глаза и снижать усталость.
- Правильное освещение**
 - Избегайте бликов на экране, расположив источник света сбоку.
 - Используйте мягкое, рассеянное освещение.
- Поддержание правильной осанки**
 - Сидите прямо, не сутультесь.
 - Стопы должны полностью стоять на полу или на подставке.
 - Избегайте скрещивания ног.
- Гидратация и питание**
 - Пейте достаточно воды в течение дня.
 - Старайтесь питаться сбалансировано, чтобы поддерживать энергию и здоровье.
- Ограничение времени работы**





Основные негативные факторы, связанные с работой за компьютером, и их влияние на организм:

- **Длительное сидячее положение****
 - Напряжение мышц шеи, головы, рук и плеч
 - Остеохондроз
 - Возможный сколиоз у детей и подростков
 - Застой крови в тазовых органах
 - Риск ожирения из-за малоподвижного образа жизни
- **Электромагнитное излучение****
 - Монитор излучает различные виды электромагнитного излучения, что может оказывать негативное воздействие на организм
- **Нагрузка на зрение****
 - Восприятие мельчайших вибраций текста и мерцания экрана
 - Постоянное напряжение мышц глаза, управляющих хрусталиком
 - Потеря остроты зрения
- **Стресс при потере информации****
 - Эмоциональное напряжение и переживания, вызванные потерей или повреждением данных
- **Перегрузка суставов кистей рук****
 - Может привести к синдрому запястного канала
- **Возможность заболеваний органов дыхания и аллергии****
 - связано с пылью, кондиционированием воздуха и другими факторами в помещении

Приложение 4. Входная диагностика

ФИ

1. Слышали ли Вы о киберпреступлениях? Да Нет
2. Как Вы оцениваете свой уровень знаний о киберпреступлениях Высокий Средний Низкий
3. Какие виды киберпреступлений Вам известны? (выберите все подходящие варианты)
Фишинг Взлом аккаунтов Вирусы и вредоносное ПО Кража личных данных Другие
4. Используете ли Вы антивирусное программное обеспечение? Нет Да
5. Как часто Вы меняете пароли для своих онлайн-аккаунтов?
Каждый месяц Каждый квартал Раз в полгода Не меняю
6. Знаете ли вы, что такое фишинг? Да Нет
7. Как Вы обычно реагируете на подозрительные электронные письма?
Игнорирую Удаляю Открываю и просматриваю
8. Используете ли Вы двухфакторную аутентификацию в своих аккаунтах? Да Нет
9. Какой вид киберпреступлений Вас больше всего беспокоит? Кража личных данных Взлом аккаунтов Онлайн-мошенничество Вредоносное ПО
10. Достаточно ли информативны для Вас уроки по кибербезопасности в учебном заведении? Да Нет
11. Используете ли Вы общедоступные Wi-Fi сети для работы с личной информацией?
Да Нет
12. Знаете ли Вы о рисках, связанных с использованием общедоступных Wi-Fi сетей?
Да Нет
13. Сколько раз Вы становились жертвой киберпреступления?
Ни разу Один раз Два раза Более двух раз
14. Как бы Вы описали свои знания о безопасном обращении с личными данными?
Хорошие Удовлетворительные Плохие
15. Интересуетесь ли Вы карьерой в области кибербезопасности? Да Нет
16. Что было бы наиболее эффективным методом защиты от киберпреступлений?
Образование и информирование Технологические меры Законодательство Социальная ответственность
17. Пользуетесь ли Вы VPN-сервисами для повышения безопасности в интернете? Да Нет
18. Слышали ли Вы о GDPR и его значении для кибербезопасности? Да Нет
19. Как Вы относитесь к вопросам приватности в интернете?
Очень серьезно Умеренно Не беспокоюсь