Информационно-методический вестник «Я-профи»

ноябрь 2021

# Информационная безопасность в интернете

## СОДЕРЖАНИЕ

**Для педагогов**

- Информационная безопасность в Интернет-ресурсах
- Мини-игра по безопасность в интернете
- Памятка по использованию сотовых телефонов в профессиональной образовательной организации

**Для студентов:**

- Лайфхак для флеш-накопителя
- Кибербуллинг
- Полезные ссылки по информационной безопасности

**Календарь мероприятий**

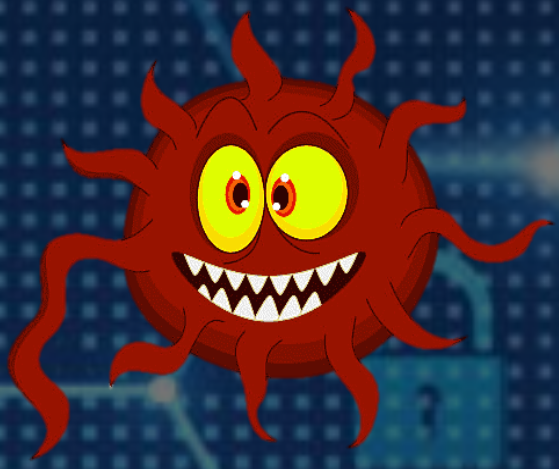
**Контакты**

Информационно-методический вестник «Я-профи»

ноябрь 2021

С каждым годом молодежи в интернете становиться больше, а студенты одни из самых активных пользователей. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Данная информация должна помочь безопасно находиться в сети.

***Компьютерный вирус*** – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.



**Методы защиты от вредоносных программ:**

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;

2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

5. Ограничь физический доступ к компьютеру для посторонних лиц;

6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;

7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Информационно-методический вестник «Я-профи»

ноябрь 2021


**Wi-Fi** — это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

**Советы по безопасной работе в общедоступных сетях Wi-Fi:**

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;

4. Не используй публичный Wi-Fi для передачи личных данных, например, для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводи именно «https://»;

6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Социальные сети** активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты.

Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.


**Основные советы по безопасности в социальных сетях:**

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Электронные деньги** — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и неанонимные. Разница в том, что анонимные — это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимные идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

**Основные советы по безопасной работе с электронными деньгами:**

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли —это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Электронная почта —** это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена.

Также кроме передачи простого текста, имеется возможность передавать файлы.

**Основные советы по безопасной работе с электронной почтой:**

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь, и кто первый в рейтинге;

2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Современные смартфоны и планшеты** содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало.

Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

**Основные советы для безопасности мобильного телефона:**

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в итоге?

3. Необходимо обновлять операционную систему твоего смартфона;

4. Используй антивирусные программы для мобильных телефонов;

5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

7. Периодически проверяй какие платные услуги активированы на твоем номере;

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Современные онлайн-игры –** это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

**Основные советы по безопасности твоего игрового аккаунта:**

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Информационно-методический вестник «Я-профи»

ноябрь 2021

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как **фишинг (от fishing — рыбная ловля, password — пароль).**

**Основные советы по борьбе с фишингом:**

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Цифровая репутация** — это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» — это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

**Основные советы по защите цифровой репутации:**

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;

3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Информационно-методический вестник «Я-профи»

ноябрь 2021


Современные студенты – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин **«интеллектуальная собственность»** относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

**Авторские права** – это права на интеллектуальную собственность на произведения науки, литературы и искусства.

Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание.

Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете. Использование «пиратского» программного обеспечения может привести ко многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

Кроме памятки, можно показать студентам видеоролик 10 глупых вопросов СПЕЦИАЛИСТУ ПО КИБЕРБЕЗОПАСНОСТИ [10 глупых вопросов СПЕЦИАЛИСТУ ПО КИБЕРБЕЗОПАСНОСТИ - YouTube]

Для студентов профессиональных образовательных организаций можно провести итоговую мини-игру для закрепления полученной информации.

1. Какие правила необходимо соблюдать, чтобы не заразить мобильное устройство вирусом?

   ***Ответ:***

- *Подключить себе на номер телефона услугу «Запрет контента», Черно-белые списки» и т.п. в зависимости от оператора, SIM-карту которого используете.*
- *Не переходить по сомнительным адресам в интернете.*
- *Не переходить по сомнительным ссылкам, особенно, если это рекламные баннеры с громкими заголовками.*
- *Не переходить по ссылкам в SMS с незнакомых номеров. Да и со знакомых тоже, до уточнения у отправителя, что именно вам прислали.*
- *При попытке сайта что-либо установить на телефон или при всплывающем окне с предложением что-либо скачать, свернуть все окна кнопкой «Home» и закрыть браузер через диспетчер запущенных приложений.*
- *Не качать приложения из сомнительных, неизвестных источников (иными словами, не из официального магазина приложений).*
- *Обновлять приложения только в официальном магазине приложений.*

2. Какие расширения могут быть опасны для скачивания из электронной почты? ***Ответ:*** *.docm, .xlsm и .pptm; расширения .js, .vbs, .msi и .reg; .exe, .scr, .bat, .com, .pif; Файлы с двойными расширениями.*

3. Как бесплатно скачать файлы, защищённые авторскими правами? ***(Никак).***

4. Какую практическую пользу, помимо украшения, имеет установка иконки на флэш-накопитель? ***(если на флешку попадет вирус, иконка пропадёт!).***

5. Что в первую очередь может смутить посетителя страницы? Как избежать обмана?

***Ответ:*** *Подозрительная, неправильная ссылка.*

***Ответ на второй вопрос:*** *Использовать «Закладки», «Избранное» и т.п. Проверять адрес сайта (vk.com, а не vkfrejhfhern.c0m). Безопасное соединение (https://, зелёная подсветка, замочек).*

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Памятка по использованию сотовых телефонов в профессиональной образовательной организации.**

(рекомендуется распечатать и повесить на информационном стенде)

**Нужен ли студенту сотовый телефон?**

Мобильные телефоны и устройства стали еще одной проблемой современной профессиональной образовательной организации. Мелодии, звучащие на занятиях, посылаемые SMS отвлекают студентов и мешают им. Кражи телефонов провоцируют конфликты и жалобы родителей. Излучение от сотовых оказывает вредное воздействие на здоровье растущего организма.

Частое использование мобильного телефона может стать причиной рака, но экспериментальных данных, подтверждающих или опровергающих влияние сотовых телефонов на юный организм, в России получено не было.

Нельзя сбрасывать со счетов различные учреждения о том, что мобильные телефоны могут вызвать доброкачественные опухоли, когнитивные расстройства и даже влиять на структуру ДНК.

Специалисты предостерегают родителей и преподавателей, а также рекомендуют не разрешать студентам чрезмерно часто пользоваться сотовыми телефонами.

**Правила пользования сотовыми телефонами в профессиональной образовательной организации.**

**Общие правила:**

• сотовый телефон, мобильное устройство является личной собственностью обучающегося;

• администрация колледжа и техникума не несет ответственности за личные вещи обучающихся;

• родители должны проинструктировать обучающегося о правилах пользования сотовым телефоном и мобильными устройствами;

• нельзя звонить с недостоверными сообщениями о подготовке к террористическим актам;

• с помощью сотовых и мобильных устройств нельзя передавать информацию, содержащую призывы к насилию и жестокости, суициду, террористической деятельности, распространению наркотиков, подготовке иных преступлений.

• нельзя фотографировать и распространять информацию о студентах, преподавателях, сотрудниках колледжа и техникума без их согласия; нельзя снимать и распространять постановочные сцены насилия, жестокости и т.п. в стенах колледжа и техникума;

**На занятиях:**

• во время пары звуковой сигнал сотового телефона необходимо отключить;

• обучающимся во время пары запрещается пользоваться сотовым телефоном и мобильными устройствами;

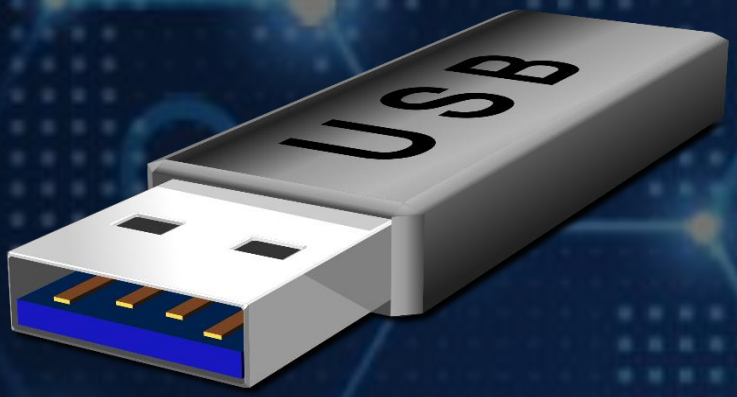
• во время пары педагог не имеет права брать на хранение сотовые телефоны обучающихся и не несет ответственности за их сохранность.

• родители не должны звонить обучающимся во время пар.

Информационно-методический вестник «Я-профи»

ноябрь 2021

Существует интересный лайфхак, который поможет вам одновременно украсить свой флэш-носитель и проверить его на наличие вирусов.




**Инструкция:**

**1 шаг.** Создать на флэш-накопителе текстовый файл. Затем переименовать его в autorun.inf. Важно! Если у вас не отражается расширение файла, например (avi, txt), вам нужно поставить в "свойствах папки", на вкладке "вид" убрать галочку с пункта "скрывать расширение".

**2 шаг.** Найти красивую иконку в Интернете с разрешением 64x64.

**3 шаг.** Открыть autorun.inf и написать в нем следующий текст:

[autorun]

icon=1.ico (название иконки с расширением файла)

**4 шаг.** Вытащить и заново вставить флэш-накопитель. Теперь в окне "мой компьютер" на месте стандартного значка флэш-накопителя будет отображаться новая иконка. Если на ваш флэш-носитель попадет вирус, то он перепишет файл autorun.inf и ваша иконка не будет отображаться — это и будет признаком вируса.

Попытаться получить доступ к файлам можно следующим образом. В заголовке окна во вкладке «Вид» необходимо включить отображение скрытых файлов, где, скорее всего, будет находиться папка с непримечательным простым названием (чаще всего вместо названия используется символ нижнего подчёркивания). Из папки необходимо скопировать все файлы на компьютер, а затем отформатировать флэш-носитель. Скопированные файлы необходимо проверить средствами антивирусной защиты.

Информационно-методический вестник «Я-профи»

ноябрь 2021

**Кибербуллинг** — это травля в интернете. Тех, кто ею занимается, называет троллями. Обычно кибербуллингом называют назойливую травлю, которая повторяется и продолжается долгое время, но в последнее время любые нападки в сети могут попасть под это определение.

**О кибербуллинге важно помнить две вещи:**

1. Никогда не начинайте и не участвуйте в травле сами. Даже один неприятный комментарий может обидеть и оскорбить человека. Тем более неприятно может быть, если такие комментарии оставит много людей или если они повторяются. Когда вы хотите написать о человеке что-то неприятное, подумайте, хотели бы вы сами прочитать что-то подобное о себе.

2. Вы должны помнить, что ничто не делает вас исключительным и защищенным от травли. Жертвой травли может стать абсолютно любой человек, поскольку травля может начаться из-за одной единственной неудачной фразы или фотографии, ее может начать кто-то, кто завидует тебе или почему-то не любит тебя. То, что ты стал жертвой травли, не значит, что ты плохой; это значит, что тем, кто тебя травит, не хватает воспитания, чтобы нормально вести себя в сети.

**Если ты стал жертвой кибербуллинга, соблюдай следующие правила:**

- Никогда не отвечай троллям, это только раззадорит их.
- Расскажи своим близким, но ни в коем случае не проси их вступиться за тебя — это еще хуже, чем отвечать самому. Если ты будешь проводить с ними больше времени и ощущать их поддержку, это поможет сгладить переживания из-за травли.
- Заблокируй обидчиков с помощью настроек социальной сети, если травля становится навязчивой.

# Полезные ссылки по информационной безопасности

1) Единый Реестр запрещённых сайтов: http://eais.rkn.gov.ru/
2) Лига безопасных сайтов: http://ligainternet.ru/encyclopedia-of-security/included-white-list.php
3) Энциклопедия безопасности: http://www.ligainternet.ru/encyclopedia-of-security/
4) Информационно-аналитический сайт по ИБ, основная тема - антивирусы и их исследования: https://www.anti-malware.ru/
5) Обучение по информационной безопасности, сертификация, тестирование, аналитика, лучшие практики, документы: https://cccure.education/
6) Лучшие практики, исследования, отчеты, методологии: https://www.securityforum.org/
7) Новости, информация об угрозах и уязвимостях, статьи, средства обеспечения и анализа безопасности: https://www.securitylab.ru/
8) Открытая библиотека документов по информационной безопасности: http://securitypolicy.ru/
9) Рекомендации, обновления, средства обеспечения и анализа безопасности. Центр безопасности: https://technet.microsoft.com/ru-ru/ms376608.aspx

## КАЛЕНДАРЬ МЕРОПРИЯТИЙ

| Мероприятие | Время |
|---|---|
| Акция «Стоп ВИЧ/СПИД» в рамках программы по формированию здорового образа жизни обучающихся профессиональных образовательных организаций Калужской области «ProЗдоровье» | С 29 ноября по 3 декабря |
| Виджет по здоровому образу жизни «Будь здоров!» в рамках программы по формированию здорового образа жизни обучающихся профессиональных образовательных организаций Калужской области «ProЗдоровье» | Декабрь |
| Акция «После пары» в рамках программы адаптации первых курсов профессиональных образовательных организаций Калужской области «Зачет» | 1-15 декабря |
| Итоговая конференция рейтинга учета активности профессиональных образовательных организаций Калужской области в мероприятиях, проводимых ГБУ КО «Областной молодежный центр» | 8 декабря |
| Итоговая конференция ежегодного областного проекта по добровольчеству «Важное дело» по профилактике правонарушений, наркомании и асоциальных явлений среди молодёжи Калужской области | 8 декабря |
| Конкурс СТЭМ в рамках областного фестиваля художественного творчества обучающихся и работников профессиональных образовательных организаций Калужской области «Я вхожу в мир искусств» | 13 декабря |
| Конкурс чтецов «Литературное кафе приглашает в рамках областного фестиваля художественного творчества обучающихся и работников профессиональных образовательных организаций Калужской области «Я вхожу в мир искусств» | 15 декабря |
| Координационный совет обучающихся профессиональных образовательных организаций Калужской области «Шаг вперед» | 14 декабря |
| Областной турнир «Зимняя игротека» среди обучающихся профессиональных образовательных организаций Калужской области | 17 декабря |

# КОНТАКТЫ

**ГБУ КО «ОБЛАСТНОЙ МОЛОДЁЖНЫЙ ЦЕНТР»**

**НАШ АДРЕС:**

**248001, г. Калуга, ул. Ленина, 74, оф. 307.**

**E-mail: osm.klg@gmail.com**

**Группа ВК: https://vk.com/spo_omz**

**Инстаграм: https://www.instagram.com/spokaluga/**

## СОТРУДНИКИ ОТДЕЛА

**Белкина Юлия Витальевна**

**Денисенко Максим Сергеевич**

**Гаврилова Виктория Андреевна**

**Егорова Ирина Сергеевна**

**Егоров Юрий Борисович**

**Новосад Ирина Сергеевна**

**Тел. 8 (4842) 56-21-10**