**УТВЕРЖДАЮ**

Директор ГОУ ДО ЯО ЦДЮТурЭк

_____А.Н. Логинова

«24» января 2020 г.

# ИНСТРУКЦИЯ

для обучающихся по обеспечению информационной безопасности
при использовании сети «Интернет»
в государственном образовательном учреждении дополнительного образования
Ярославской области «Центр детского и юношеского туризма и экскурсий»

## 1 Основные положения

1.1 Настоящий Инструкция устанавливает порядок работы обучающихся государственного образовательного учреждения дополнительного образования Ярославской области «Центр детского и юношеского туризма и экскурсий» (далее – ГОУ ДО ЯО ЦДЮТурЭк) в сети «Интернет».

1.2 Использование сети «Интернет» в ГОУ ДО ЯО ЦДЮТурЭк подчинено следующим принципам:

– соответствия образовательным программам;

– способствования гармоничному формированию и развитию личности;

– уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
приобретения новых навыков и знаний;

– расширения применяемого спектра учебных и наглядных пособий;

– социализации личности, введения в информационное общество.

## 2 Права, обязанности и ответственность пользователей

2.1 Пользователи сети «Интернет» имеют право:

– использовать сеть «Интернет» для работы с информационными ресурсами сети «Интернет» только в образовательных целях или для осуществления научных изысканий,

– выполнения гуманитарных и культурных проектов; любое нецелевое использование сети «Интернет» запрещено;

– производить поиск необходимой информации в сети «Интернет»;

– получать консультации по вопросам, связанным с использованием сети Интернет.

2.2 Пользователи сети «Интернет» обязаны:

– выполнять все требования преподавателя;

– сохранять оборудование в целости и сохранности;

– поставить в известность преподавателя при возникновении технических проблем.

2.3 Пользователям сети «Интернет» запрещается:

– осуществлять действия, запрещенные законодательством Российской Федерации;

– посещать сайты, содержащие информацию, запрещенную к распространению в Российской Федерации и/или не совместимую с задачами образования и воспитания в соответствии с утвержденными классификаторами;

– передавать информацию, представляющую коммерческую или государственную тайну;

– распространять информацию, порочащую честь и достоинство граждан;

– осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в локальной сети ГОУ ДО ЯО ЦДЮТурЭк, так и за его пределами;

– использовать возможности сети «Интернет» для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации;

– работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции;

– устанавливать какое-либо дополнительное программное обеспечение и/или вносить какие-либо изменения в программное обеспечение, установленное на рабочей станции;

– производить запись информации на жесткий диск рабочей станции;

– работать с объемными ресурсами (video, audio, chat, игры и др.);

– изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, фоновые рисунки рабочего стола, стартовые страницы браузеров);

– включать, выключать и перезагружать компьютер без согласования с преподавателем.

2.4 Пользователи сети «Интернет» несут ответственность:

– за содержание передаваемой, сознательно принимаемой и печатаемой информации;

– пользователи, не соблюдающие настоящую инструкцию, лишаются права работы в сети «Интернет»;

– при нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

# Информационная памятка для обучающихся государственного образовательного учреждения дополнительного образования Ярославской области «Центр детского и юношеского туризма и экскурсий» по обеспечению информационной безопасности при использовании сети «Интернет»

## 1 Защита от компьютерных вирусов

1.1 Компьютерный вирус – это вредоносная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. В большинстве случаев компьютерные вирусы распространяется через сеть «Интернет».

1.2 Для защиты от вредоносных программ необходимо:

– использовать современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;

– постоянно устанавливать обновления своей операционной системы. Рекомендуется включить автоматическое обновление операционной системы (если существует такой режим) либо скачивать обновления только с официального сайта разработчика операционной системы;

– работать на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ проникнуть в файловую систему;

– использовать антивирусное программное обеспечение известных производителей с автоматическим обновлением баз;

– ограничить физических доступ к компьютеру для посторонних лиц;

– использовать внешние носители информации (флеш-накопители или диски) только из доверенных источников и предварительно проверенные на наличие вредоносных программ;

– не открывать компьютерные файлы, полученные из недоверенных источников;

– не переходить по ссылкам и нажимать кнопки во всплывающих сообщениях, которые кажутся подозрительными.

## 2 Защита от фишинга

2.1 Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к логинам и паролям пользователей.

2.2 Для защиты от фишинга необходимо:

– следить за своим аккаунтом, если есть подозрение, что аккаунт был взломан, необходимо заблокировать его и сообщить об этом администраторам ресурса;

– использовать только безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем;

– перед тем как вводить логин и пароль, нужно проверять, защищено ли соединение. Если перед адресом сайта есть префикс https, то все в порядке;

– использовать сложные и разные пароли, в этом случае если аккаунт будет взломан, то злоумышленники получат доступ только к одному аккаунту, а не ко всем;

– если аккаунт был взломан, об этом необходимо предупредить всех знакомых. Возможно от вашего имени будет рассылаться спам и ссылки на фишинговые сайты;

– отключить сохранение пароля в браузере;

– не открывать подозрительные файлы и другие вложения в письмах, даже если письмо или сообщение пришло от лучшего друга или официальных организаций.

## 3 Безопасное использование публичной сети Wi-Fi

3.1 Wi-Fi – это беспроводной способ передачи данных, использующий радиосигналы. Wi-Fi – аббревиатура от английского словосочетания «Wireless Fidelity», которое можно дословно перевести как «беспроводная привязанность». Бесплатный Интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в сеть «Интернет». Но общедоступные сети Wi-Fi не являются безопасными.

3.2 Правила безопасного использования Wi-Fi:

– запрещено использовать Wi-Fi для выхода в социальные сети или в электронную почту, а также передавать свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины, данные банковских карт и т.д.;

– необходимо использовать и обновлять антивирусное программное обеспечение. Тем самым можно обезопасить устройство от заражения вирусом;

– при использовании Wi-Fi необходимо отключить функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

– необходимо использовать только защищенное соединение: перед адресом сайта должен быть префикс https;

– в мобильном телефоне необходимо отключить функцию «Подключение к Wi-Fi автоматически».

## 4 Безопасное общение в социальных сетях

4.1 Социальная сеть — онлайн-платформа, которую люди используют для общения, создания социальных отношений с другими людьми, которые имеют схожие интересы или офлайн-связи. Чаще всего в социальной сети для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещенная ими в социальных се-

тях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

4.2 Правила безопасности в социальных сетях:

– необходимо ограничь список друзей. В друзьях не должно быть случайных и незнакомых людей;

– необходимо защищать свою частную жизнь: не указывать пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о планах на каникулы;

– необходимо защищать свою репутацию: держать ее в чистоте и думать прежде, чем что-то опубликовать, написать и загрузить;

– при разговоре с незнакомыми людьми лучше не использовать свое реальное имя и другую личную информацию: место жительства, место учебы и прочее;

– необходимо избегать размещения фотографий в сеть «Интернет», где изображена местность, по которой можно определить местоположение;

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

– для социальной сети, электронной почты и других сайтов необходимо использовать разные пароли. В этом случае если аккаунт будет взломан, то злоумышленники получат доступ только к одному аккаунту, а не ко всем.

## 5 Безопасное использование электронной почты

5.1 Электронная почта – это технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе — сети «Интернет»).

5.2 Правила безопасной работы с электронной почтой:

– необходимо выбрать правильный почтовый сервис. В сети «Интернет» есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кто первый в рейтинге;

– необходимо выбрать правильное название почтового ящика, которое не должно содержать личную информацию;

– необходимо использовать двухэтапную авторизацию: помимо пароля нужно вводить код, присылаемый по SMS;

– необходимо выбрать сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

– необходимо использовать несколько почтовых ящиков. Первый для частной переписки с адресатами. Этот электронный адрес не надо использовать при регистрации на сайтах;

– запрещено открывать файлы и другие вложения в письмах, даже если письмо пришло от лучшего друга или официальных организаций;

– после окончания работы в почтовом сервисе перед закрытием вкладки с сайтом необходимо нажать на «Выйти».

## 6 Безопасное использование мобильных устройств

6.1 Правила безопасного использования мобильных устройств:

– необходимо обновлять операционную систему мобильных устройств;

– необходимо использовать антивирусные программы для мобильных устройств;

– запрещено загружать приложения от неизвестного источника: они могут содержать вредоносное программное обеспечение;

– необходимо периодически проверять, какие платные услуги подключены на номере мобильного телефона;

– номер мобильного телефона можно давать только знакомым людям;

– необходимо всегда выключать Bluetooth после использования.