Информационная памятка для обучающихся ГПОУ ЯО «Ярославский колледж культуры» 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;

2.3 Комиссия вводит название материала или адрес Интернет-ресурса в поле поиска любой поисковой системы, из предложенного поисковой системой списка Интернет-ресурсов открывает Интернет-ресурс, содержащий противоправный контент и выполняет следующие действия:

- в случае если материал отображается и с ним можно ознакомиться без дополнительных условий - фиксирует факт нарушения работы СКФ;
- в случае если Интернет-ресурс требует дополнительных условий (требуется регистрация, условное скачивание, переадресация и т.д.), при выполнении которых материал отображается - фиксирует факт нарушения работы СКФ;
- в случае если ознакомление с противоправным контентом при выполнении дополнительных условий невозможно - не фиксирует факт нарушения работы СКФ.

2.4 Комиссия составляет 3-4 запроса по заданной теме (экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т.д.) в любой поисковой системе, состоящих из слов, которые однозначно могут привести на запрещенные для несовершеннолетних детей ресурсы, например, «изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида» и т.д., из предложенного поисковой системой списка Интернет-ресурсов открывает 2-3 Интернет-ресурса, ознакамливается с полученными материалами, дает оценку материалам на предмет возможного нанесения ущерба физическому и (или) психическому здоровью обучающихся и выполняет следующие действия:

- в случае если обнаруженный материал признается условно противоправным - фиксирует факт нарушения;
- в случае если найденный материал нарушает законодательство Российской Федерации - направляет адрес Интернет-ресурса на проверку в единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

2.5 Комиссия проверяет работоспособность СКФ на всех компьютерах колледжа путем ввода в поле поиска любой поисковой системы ключевых слов из списка информации, запрещенной для просмотра учащимися, с последующими попытками загрузки сайтов из найденных. В том числе комиссия проверяет осуществляется ли загрузка информации, причиняющей вред здоровью и (или) развитию детей, не имеющей отношения к образовательному процессу, в социальных сетях.

2.6 Комиссия проверяет работоспособность журнала, фиксирующего адреса Интернет-ресурсов, посещаемых с компьютеров колледжа.

2.7 По итогам мониторинга комиссия формирует акт проверки СКФ в колледже.

2.8 Если по итогам мониторинга были выявлены Интернет-ресурсы, не включенные в Реестр безопасных образовательных сайтов, то комиссия указывает их в акте проверки СКФ в колледжа.

2.9 При выявлении компьютеров, подключенных к сети «Интернет» и не имеющих СКФ, производится одно из следующих действий:

немедленная установка и настройка СКФ;

- **немедленное программное и/или физическое отключение доступа к сети «Интернет» на выявленных компьютерах.**

- 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 сетях, 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.