

Что такое авторское право

Рекомендовано
Минобрнауки

Чтобы использовать возможности цифрового мира, нужно соблюдать права 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, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность – на произведения науки, литературы и искусства. Авторские права выступают как гарантия возможностей автора заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать или размещать в интернете.

«Пиратское» программное обеспечение несет в себе многие риски: от потери данных до блокировки устройства, где установлена нелегальная программа. Не забывайте, что в Сети можно найти легальные и бесплатные программы со сходным функционалом.

Как безопасно играть online

Рекомендовано
Минобрнауки

ONLINE-ИГРЫ объединяют людей по всему миру. Игроки покупают диск, оплачивают абонемент или дополнительные опции. На эти средства совершенствуются системы авторизации, закрываются уязвимости. В играх стоит опасаться кражи пароля.

- 1 Блокируй неадекватов.** Заблокируй в списке игроков того, кто ведет себя агрессивно по отношению к тебе или создает неприятности.
- 2 Пожалуйся администраторам игры на поведение агрессивного игрока.** Желательно приложить доказательства в виде скринов.
- 3 Будь осторожен.** Не указывай личную информацию в профайле игры.
- 4 Следи за своим поведением.** Уважай других участников игры.
- 5 Устанавливай проверенные утилиты.** Избегай неофициальных патчей и модов.
- 6 Берегись от взлома.** Используй сложные и разные пароли.
- 7 Не отключай антивирус во время игры.** Пока ты играешь, твой компьютер могут заразить.

Как безопасно пользоваться смартфоном, планшетом

Рекомендовано
Минобрнауки

- 1 Будь осторожен.** Когда тебе предлагают бесплатный контент, в нем могут быть скрыты платные услуги.
- 2 Думай, прежде чем отправить СМС, фото или видео.** Ты точно знаешь, где они окажутся в конечном итоге?
- 3 Обновляй операционную систему смартфона.** Это дополнительная защита.
- 4 Используй антивирусные программы для смартфонов.** Регулярно обновляй их.
- 5 Не загружай приложения от неизвестного источника.** Они могут содержать вредоносное программное обеспечение.
- 6 Зайди в настройки браузера и удали cookies.** Сделай это сразу после того, как ты выйдешь с сайта, где вводил личную информацию.
- 7 Проверь платные услуги на твоём номере.** Иногда могут активировать новые.
- 8 Не всем давай номер телефона.** Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
- 9 Выключай Bluetooth, когда не используешь его.** Иногда проверяй, не забыл ли выключить.

Как безопасно пользоваться электронной почтой

Рекомендовано
Минобрнауки

- 1 Выбери правильный почтовый сервис.** В интернете много бесплатных. Однако почту лучше заводить на популярном сервисе, которым уже пользуются твои знакомые.
- 2 Не пиши о себе в адресе почты.** Не указывай в почтовом адресе личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2018@» вместо «андрей2005@».
- 3 Используй двухэтапную авторизацию.** Для двухэтапной авторизации помимо пароля нужно вводить код, который присылают по СМС.
- 4 Выбери сложный пароль.** Для каждого почтового ящика должен быть свой сложный, устойчивый к взлому пароль.
- 5 Используй проверочный вопрос.** Придумай сам свой личный вопрос для идентификации, если сервис дает такую возможность.
- 6 Заведи несколько почтовых ящиков.** Первый для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не нужно использовать при регистрации на форумах и сайтах.
- 7 Не открывай вложения писем.** Не открывай файлы и другие вложения в письмах, даже если они пришли от друзей. Уточни у них, отправляли ли они тебе эти файлы.
- 8 Выходите из почты.** Не забывай нажимать «Выйти» после окончания работы на почтовом сервисе, перед тем как закрыть вкладку с сайтом.

Как защититься от компьютерных вирусов

Рекомендовано
Минобрнауки

КОМПЬЮТЕРНЫЙ ВИРУС – это программа, которая может создавать свои копии. Вирусы повреждают или уничтожают файлы на зараженном компьютере и всю операционную систему в целом. Чаще всего распространяются вирусы через интернет.

1

Загрузи современную операционную систему. Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.

2

Обновляй операционную систему. Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.

3

Используй права пользователя. Работай на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установиться.

4

Не рискуй. Используй антивирусные программные продукты проверенных производителей с автоматическим обновлением баз.

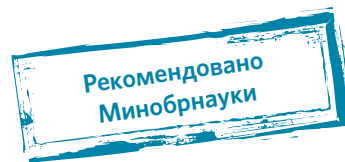
5

Ограничь доступ к своему компьютеру. Не разрешай посторонним пользоваться своим компьютером.

6

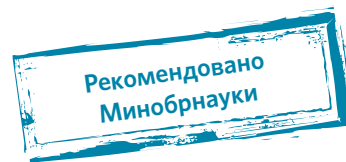
Выбирай тщательно источники. Копируй и загружай файлы только с проверенных съемных носителей или интернет-ресурсов. Не открывай файлы, которые получил из ненадежных источников. Даже те, которые прислал твой знакомый. Уточни у него, отправлял ли он тебе их.

Как безопасно общаться 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 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 то, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.
- 4 Не используй реальное имя.** Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительства, место учебы и прочее.
- 5 Не сообщай свое местоположение.** Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить местоположение.
- 6 Используй сложные пароли.** При регистрации пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.
- 7 Используй разные пароли.** Для социальной сети, почты и других сайтов создавай разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу.

Как безопасно пользоваться сетью Wi-Fi



Wi-Fi – это беспроводной способ передачи данных с помощью радиосигналов. В кафе, отелях, аэропортах часто можно бесплатно выйти в интернет через Wi-Fi. Но общедоступные сети Wi-Fi небезопасны.

- 1 Не передавай личную информацию через общедоступные сети Wi-Fi.** Желательно не вводить пароли доступа, логины и номера.
- 2 Используй и обновляй антивирусные программы и брандмауэр.** Так ты обеспечишь себя от загрузки вируса на устройство.
- 3 Отключи функцию «Общий доступ к файлам и принтерам» при использовании Wi-Fi.** Эта функция закрыта по умолчанию, однако некоторые пользователи активируют ее 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.** То есть при наборе веб-адреса вводи именно «https://».
- 6 Отключи функцию «Подключение к Wi-Fi автоматически» в мобильном телефоне.** Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.