

Информационная памятка для обучающихся о безопасности в информационно-телекоммуникационной сети «Интернет»

Размещено в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»

С каждым годом число молодых пользователей сети «Интернет» неуклонно растёт. Студенты организаций среднего профессионального образования являются одной из наиболее активных категорий пользователей российского сегмента сети. Наряду с широкими возможностями для обучения, общения и саморазвития, интернет-пространство несёт и серьёзные угрозы. Настоящая памятка разработана с целью формирования у обучающихся навыков безопасного и ответственного поведения в цифровой среде, а также защиты их персональных данных в соответствии с действующим законодательством Российской Федерации.

Компьютерные вирусы и вредоносное программное обеспечение

Компьютерный вирус — это разновидность вредоносных программ, ключевой особенностью которых является способность к саморазмножению. Помимо этого, вирусы способны повредить или полностью уничтожить файлы и данные пользователя, а также вывести из строя операционную систему. Основным канал распространения вирусов — сеть «Интернет».

Меры защиты от вредоносных программ:

- Используйте современные операционные системы с высоким уровнем встроенной защиты.
- Своевременно устанавливайте патчи (цифровые обновления, автоматически дорабатывающие программу) и другие обновления операционной системы. Загружайте их только с официального сайта разработчика. При наличии режима автоматического обновления — активируйте его.
- Работайте за компьютером под учётной записью пользователя, а не администратора. Это существенно снижает риск установки вредоносного ПО.
- Применяйте антивирусные программные продукты известных производителей с функцией автоматического обновления баз.

- Ограничьте физический доступ посторонних лиц к вашему компьютеру.
- Используйте внешние носители информации (флеш-накопители, диски, файлы из сети) только из проверенных источников.
- Не открывайте файлы, полученные из ненадёжных источников. Даже если файл прислан знакомым — уточните у отправителя, действительно ли он его направлял.

Безопасность при работе в общедоступных сетях Wi-Fi

Wi-Fi — это не технология передачи данных, а зарегистрированный товарный знак. В 1991 году нидерландская компания зарегистрировала бренд «WESA», что означало «Wireless Fidelity» — «беспроводная точность». В дальнейшем появилась аббревиатура «Wi-Fi», созвучная стандарту высококачественного звука Hi-Fi («высокая точность»).

Бесплатный доступ к сети в кафе, гостиницах и аэропортах предоставляет широкие возможности, однако, по оценкам специалистов, общедоступные Wi-Fi-сети не являются безопасными.

Рекомендации по безопасности в общедоступных Wi-Fi-сетях:

- Не передавайте персональные данные через общедоступные Wi-Fi-сети. Воздержитесь от ввода паролей, логинов и номеров.
- Используйте и своевременно обновляйте антивирусные программы и брандмауэр — это защитит устройство от загрузки вредоносного ПО.
- При подключении к Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». По умолчанию она отключена, однако некоторые пользователи активируют её для удобства.
- Не используйте публичный Wi-Fi для передачи личных данных, в том числе для входа в социальные сети или электронную почту.
- Используйте только защищённое соединение HTTPS (а не HTTP) — при вводе веб-адреса указывайте «https://».
- На мобильном устройстве отключите функцию автоматического подключения к Wi-Fi. Не допускайте соединения устройства с сетями без вашего согласия.

Безопасность в социальных сетях

Социальные сети прочно вошли в повседневную жизнь. Многие пользователи не осознают, что размещённая ими информация может быть найдена и использована третьими лицами, в том числе с противоправными намерениями.

Основные рекомендации по безопасности в социальных сетях:

- Ограничьте список друзей. В нём не должно быть случайных и незнакомых людей.
- Защищайте частную жизнь. Не указывайте пароли, номера телефонов, адреса, дату рождения и иную личную информацию. Злоумышленники могут использовать даже сведения о планируемом отдыхе.
- Берегите репутацию — задавайте себе вопрос: хотели бы вы, чтобы ваши публикации увидели другие? Подумайте, прежде чем что-либо опубликовать или загрузить.
- При общении с незнакомыми людьми не используйте реальное имя и личные данные: имя, место жительства, место учёбы и прочее.
- Избегайте публикации фотографий, по которым можно определить ваше местоположение.
- При регистрации в социальной сети используйте сложные пароли из букв и цифр, не менее 8 знаков.
- Для социальных сетей, электронной почты и других сайтов используйте разные пароли. В случае взлома злоумышленники получают доступ только к одному ресурсу, а не ко всем сразу.

Безопасность при работе с электронными деньгами

Электронные деньги — удобный способ платежей, однако существуют мошенники, стремящиеся получить эти средства. Электронные деньги появились сравнительно недавно, и в ряде государств до сих пор не урегулированы законодательно. В Российской Федерации они функционируют и закреплены в законе, где разделяются на анонимные и неанонимные. В анонимных допускается проведение операций без идентификации пользователя, в неанонимных идентификация обязательна.

Также различают электронные фиатные деньги (равные государственным валютам) и электронные нефиадные деньги (не равные государственным валютам).

Основные рекомендации по безопасной работе с электронными деньгами:

- Привяжите к счёту мобильный телефон — это наиболее удобный и быстрый способ восстановить доступ к счёту.
- Используйте одноразовые пароли. После перехода на усиленную авторизацию кража или перехват платёжного пароля становятся невозможными.
- Выберите сложный пароль. Надёжный пароль содержит не менее 8 знаков, включает строчные и прописные буквы, цифры и специальные символы. Например: \$tR0ng!;;
- Не вводите личные данные на сайтах, которым не доверяете.

Безопасность при работе с электронной почтой

Электронная почта — это технология и услуги по пересылке и получению электронных сообщений в компьютерной сети. Адрес электронной почты обычно имеет вид: имя_пользователя@имя_домена. Помимо текстовых сообщений, возможна передача файлов.

Основные рекомендации по безопасной работе с электронной почтой:

- Выбирайте надёжный почтовый сервис. В сети представлено множество бесплатных сервисов, однако предпочтение следует отдавать проверенным и авторитетным.
- Не указывайте в адресе почты личную информацию. Лучше выбрать «музыкальный_фанат@» или «рок2013», чем «тема13».
- Используйте двухэтапную авторизацию — когда помимо пароля требуется ввод кода, направляемого по SMS.
- Выберите сложный пароль. Для каждого почтового ящика должен быть свой надёжный, устойчивый к взлому пароль.
- При наличии возможности задать собственный контрольный вопрос — воспользуйтесь ею.
- Используйте несколько почтовых ящиков. Первый — для частной переписки с доверенными адресатами; его не следует использовать при регистрации на форумах и сайтах.
- Не открывайте файлы и вложения в письмах, даже если они пришли от друзей. Уточните у отправителя, направлял ли он эти файлы.

- По завершении работы с почтовым сервисом нажмите «Выйти» перед закрытием вкладки.

Кибербуллинг (виртуальное издевательство)

Кибербуллинг — это преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с использованием различных интернет-сервисов.

Основные рекомендации по противодействию кибербуллингу:

- Не вступайте в конфликт. Оптимальный вариант — посоветоваться, как себя вести; если обратиться не к кому — сначала успокоиться. Ответные оскорбления лишь усугубят конфликт.
- Управляйте своей киберрепутацией.
- Анонимность в сети мнимая. Существуют способы установить, кто стоит за анонимным аккаунтом.
- Не ведите хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их; удалить их впоследствии крайне затруднительно.
- Соблюдайте виртуальную честь смолоду.
- Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать — обычно агрессия прекращается на начальной стадии.
- Блокируйте агрессора. В программах обмена мгновенными сообщениями и социальных сетях предусмотрена возможность блокировки.
- Если вы стали свидетелем кибербуллинга: выступите против преследователя, покажите ему, что его действия оцениваются негативно, поддержите жертву, сообщите взрослым о факте агрессивного поведения в сети.

Безопасность мобильного телефона

Современные смартфоны и планшеты обладают функционалом, сопоставимым со стационарными компьютерами. Однако средств защиты для таких устройств пока недостаточно. Тестирование и поиск уязвимостей в них проводятся менее интенсивно, чем для ПК; то же касается мобильных приложений. Современные мобильные браузеры практически догнали

настольные аналоги, однако расширение функционала влечёт большую сложность и меньшую защищённость. Не все производители выпускают обновления, закрывающие критические уязвимости.

Основные рекомендации по безопасности мобильного телефона:

- Ничего не является по-настоящему бесплатным. При предложении бесплатного контента могут быть скрыты платные услуги.
- Обдумывайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они окажутся в конечном итоге?
- Своевременно обновляйте операционную систему смартфона.
- Используйте антивирусные программы для мобильных устройств.
- Не загружайте приложения из неизвестных источников — они могут содержать вредоносное ПО.
- После выхода с сайта, где вводились личные данные, удалите cookies в настройках браузера.
- Периодически проверяйте, какие платные услуги активированы на вашем номере.
- Сообщайте номер мобильного телефона только проверенным лицам.
- Отключайте Bluetooth, когда он не используется.

Безопасность в онлайн-играх

Современные онлайн-игры — красочные и захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют виртуальные миры, общаются, выполняют задания, сражаются с противниками и получают опыт. За удовольствие они платят: приобретают диск, оплачивают абонемент или покупают опции. Эти средства идут на поддержание и развитие игры, а также на безопасность: совершенствуются системы авторизации, выпускаются новые патчи, закрываются уязвимости серверов. В подобных играх следует опасаться не столько соперников, сколько кражи пароля, на котором основана система авторизации.

Основные рекомендации по безопасности игрового аккаунта:

- При недостойном поведении другого игрока — заблокируйте его в списке игроков.
- Пожалуйтесь администраторам игры на плохое поведение, приложив доказательства (скриншоты).

- Не указывайте личную информацию в профайле игры.
- Уважайте других участников игры.
- Не устанавливайте неофициальные патчи и моды.
- Используйте сложные и разные пароли.
- Не отключайте антивирус во время игры — компьютер может быть заражён.

Фишинг (кража личных данных)

С развитием интернет-технологий злоумышленники переместились в сеть. Так появилась угроза **фишинга** — интернет-мошенничества, главная цель которого — получение конфиденциальных данных пользователей: логинов и паролей. Термин происходит от английского phishing (от fishing — рыбная ловля, password — пароль).

Основные рекомендации по противодействию фишингу:

- Следите за своим аккаунтом. При подозрении на взлом — заблокируйте анкету и незамедлительно сообщите администраторам ресурса.
- Используйте безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.
- Используйте сложные и разные пароли. В случае взлома злоумышленники получают доступ только к одному профилю, а не ко всем.
- При взломе — предупредите знакомых из списка друзей о возможной рассылке спама и ссылок на фишинговые сайты от вашего имени.
- Установите надёжный пароль (PIN) на мобильный телефон.
- Отключите сохранение пароля в браузере.
- Не открывайте файлы и вложения в письмах, даже если они пришли от друзей. Уточните у отправителя.

Цифровая репутация

Цифровая репутация — это совокупность позитивной или негативной информации о человеке в сети. Компрометирующая информация, размещённая в интернете, может серьёзно отразиться на реальной жизни. Цифровая репутация формируется из информации о вас в сети: место

жительства, учёбы, финансовое положение, особенности характера, рассказы о близких.

Многие подростки легкомысленно относятся к публикации личной информации, не осознавая возможных последствий. Фотография, размещённая несколько лет назад, может стать причиной отказа в трудоустройстве. Комментарии и публикации могут сохраниться даже после удаления. Вы не знаете, кто сохранил информацию, попала ли она в поисковые системы и что подумают о вас окружающие. Найти информацию спустя много лет сможет любой — как из добрых побуждений, так и с намерением причинить вред.

Основные рекомендации по защите цифровой репутации:

- Обдумывайте, прежде чем что-либо опубликовать в блоге или социальной сети.
- В настройках профиля установите ограничения на просмотр — сделайте его доступным только «для друзей».
- Не размещайте информацию, которая может кого-либо оскорбить или обидеть.

Авторское право

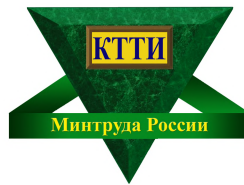
Современные обучающиеся — активные пользователи цифрового пространства. Однако не все осознают, что использование многих возможностей цифрового мира требует соблюдения прав на интеллектуальную собственность.

Интеллектуальная собственность — это результаты творческой деятельности человека: изобретения, знаки собственности на продукты и услуги, книги, фотографии, кинофильмы, музыкальные произведения. **Авторские права** — это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права гарантируют, что творческий труд автора не будет напрасным, обеспечат справедливые возможности для заработка, известности и признания. Без разрешения автора никто не вправе воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать в эфире или размещать в интернете.

Использование «пиратского» программного обеспечения влечёт риски: от потери данных к аккаунтам до блокировки устройства, где установлена

нелегальная программа. Следует помнить, что существуют легальные и бесплатные программы, доступные в сети.

Соблюдение изложенных рекомендаций позволит минимизировать риски при работе в сети «Интернет» и обеспечит защиту ваших персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных».



Подписано цифровой подписью:
ФЕДЕРАЛЬНОЕ КАЗЕННОЕ
ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ
ТЕХНИКУМ-ИНТЕРНАТ" МИНИСТЕРСТВА
ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Дата: 2026.09.17 16:51:32 +03'00'