

Безопасность в цифровом мире — приветствие

*Прасолова Людмила Сергеевна,
МАОУ СШ №9,
учитель математики*

Интернет и информационная безопасность: основы

Интернет — глобальная сеть, объединяющая миллиарды пользователей. Информационная безопасность защищает конфиденциальность, целостность и доступность данных на техническом, организационном и поведенческом уровнях.

Информационная безопасность — комплекс специально разработанных мер и процессов, направленных на защиту информации от изменения, уничтожения, незаконного доступа.



Главные угрозы в сети



Фишинг

Фишинговые письма имитируют легитимные сервисы и требуют учётных данных или денег; большинство атак начинается с электронной почты.



Вредоносные ссылки

Ссылки в сообщениях и соцсетях могут вести на фальшивые сайты или запускать скачивание вредоносного ПО без явного уведомления пользователя.



Утечки данных

Компрометация баз данных приводит к раскрытию личной информации клиентов и сотрудников, что увеличивает риск мошенничества и взломов.



Социальная инженерия

Манипуляции с людьми — запросы паролей или кодов под видом службы поддержки или знакомых, приводящие к потере доступа.





Преимущества цифровой среды

Доступ и удобство

Интернет расширяет доступ к образованию, банковским услугам и коммуникациям. Он ускоряет работу и делает сервисы доступными в любое время суток.

Инструменты защиты

Ключевые инструменты — HTTPS, антивирусы и 2FA. Комбинация технологий и осознанного поведения существенно снижает вероятность успешной атаки.

Способы защиты данных в Интернете

Защита соединения: проверять HTTPS и сертификаты сайтов, избегать публичного Wi-Fi для конфиденциальных операций; при необходимости использовать VPN, обновлять роутер и включать брандмауэр и мобильные устройства.

Создание и хранение надёжных паролей: использовать уникальные длинные фразы, включать буквы, цифры, символы; применять менеджер паролей и двухфакторную аутентификацию для защиты учётных записей и устройств.

Обновления, резервное копирование и внимательность: регулярно обновлять ОС и приложения, устанавливать антивирус, настраивать автоматические бэкапы, проверять ссылки и подозрительные письма перед переходом и сохранять копии в облаке.

Правила информационной безопасности в сети

Не раскрывайте личные данные: имя, адрес, номер телефона, пароли и финансовую информацию нельзя сообщать незнакомым людям или на сомнительных сайтах; проверяйте подлинность запроса и источник.

01

Осторожно относитесь к ссылкам и вложениям: не переходите по подозрительным адресам, проверяйте URL и отправителя, используйте безопасные закладки и проверочные сервисы перед загрузкой файлов на устройство.

03

Используйте сложные уникальные пароли для каждой учётной записи, сочетая буквы, цифры и символы; включайте двухфакторную аутентификацию и регулярно обновляйте пароли и программное обеспечение на устройствах.

02

Устанавливайте и обновляйте антивирусы, брандмауэры и официальные обновления системы; делайте резервные копии важных данных и учитесь распознавать фишинг, социальную инженерию, сообщения и поддельные сайты.

04

Викторина: вопросы и ответы

Вопросы для закрепления цифровой гигиены.

Понятные правила позволяют быстро принимать безопасные решения в большинстве ситуаций.

Вопрос

Кто-то просит твои личные данные в сети Интернет. Как поступить?

Ты нашел интересный сайт, но там очень много рекламы и различных сообщений, стоит ли туда заходить?

Почему важно придумывать сложные пароли?

Нужен ли антивирус?

Друг скинул ссылку на канал, но тебя смущает его ссылка, т.к. она содержит в себе кучу непонятных символов, будешь ли ты переходить по ней?

Создание надёжного пароля — практические шаги

Применяйте фразы-пароли или генератор в менеджере паролей; пример безопасного варианта сочетает символы и буквы разных регистров.

Используйте длину минимум 12 символов и сочетание заглавных, строчных букв, цифр и спецсимволов; избегайте словарных слов и очевидных замен.

Храните пароли в менеджере (например, Bitwarden или 1Password) и меняйте их при подозрении на компрометацию, обычно каждые 6–12 месяцев.



Как отличить безопасную ссылку от опасной

Безопасные ссылки: домен соответствует ожидаемому, используется HTTPS, адрес короткий и читабелен; проверяйте сертификат сайта при сомнении.

Опасные признаки: длинные строки с непонятными символами, подозрительные поддомены и сокращатели без предварительной проверки; пример подозрительного домена — `bank-secure.example.com`.



По каким ссылкам будем переходить, а по каким нет?

1. <http://178.248.232.27>.
2. <https://1ps.ru/blog/dirs/kakie-ssyilki-sejchas-rabotayut/>
3. <https://360.yandex.ru/>
4. <https://mts-ru.com/>

1. <https://bank.ru/rd.php?go=https://zlo.ru>.
2. <httpsbank.ru>
3. <http://bank.ru@zlo.ru>.
4. <https://www.kaspersky.ru/blog/link-shorteners-privacy-security/35948/>

Итоги и конкретные шаги

Мы обсудили основы Интернета и ИБ, ключевые угрозы и практические навыки. Сделайте три шага: смените слабые пароли, включите 2FA и проверяйте ссылки перед кликом.