ЦИФРОВАЯ КОМПЕТЕНТНОСТЬ

МЕДИАБЕЗОПАСНОСТЬ В СЕТИ

СЕТЕВОЙ ЭТИКЕТ

ЦИФРОВИЗАЦИЯ

- Правительство и органы управления
- Экономика
- Социально значимые институты

ЦИФРОВОЕ ГОСУДАРСТВО

– информационно-технологическая организация политико-правового взаимодействия граждан и органов публичной власти. Целью такого взаимодействия является обеспечение наиболее полных возможностей участия граждан в осуществлении власти и предоставления им услуг государства, реализуемых с использованием цифровых технологий.

ЗАЧЕМ?

- Быстрое получение услуг и информации;
- Отсутствие очередей;
- Единая площадка для получения всех услуг;
- Объединение банков данных различных структур;
- Прозрачность;
- Понятная и быстрая обратная связь.

ЦИФРОВАЯ КОМПЕТЕНТНОСТЬ

В отечественной модели цифровой компетентности, предложенной Г.У. Солдатовой и Е.И. Рассказовой, в структуре цифровой компетентности выделены четыре компонента:

1) информационная и медиакомпетентность;

2) коммуникативная компетентность;

3) техническая компетентность;

4) потребительская компетентность.

ИНФОРМАЦИОННАЯ И МЕДИАКОМПЕТЕНТНОСТЬ

Информационная и медиакомпетентность – знания, умения, мотивация и ответственность, связанные с поиском, пониманием, организацией цифровой информации, и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео).

КОММУНИКАТИВНАЯ КОМПЕТЕНТНОСТЬ

Коммуникативная компетентность – знания, умения, мотивация и ответственность,

необходимые для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) и с различными целями.

ТЕХНИЧЕСКАЯ КОМПЕТЕНТНОСТЬ

Техническая компетентность – знания, умения, мотивация и ответственность, позволяющие эффективно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.

ПОТРЕБИТЕЛЬСКАЯ КОМПЕТЕНТНОСТЬ

Потребительская компетентность – знания, умения, мотивация и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей

ЦИФРОВЫЕ КОМПЕТЕНЦИИ

- цифровые компетенции, связанные с достоверным поиском, пониманием, организацией, архивированием цифровой информации, ее критическим осмыслением;
- цифровые компетенции, необходимые для сотрудничества, онлайн-коммуникации в различных формах (веб-конференции, вебинары, электронная почта, чаты, блоги, форумы, социальные сети и др.);
- цифровые компетенции, необходимые для организации безопасной деятельности в сети Интернет (обеспечение безопасности данных и устройств в сети Интернет);
- цифровые компетенции, позволяющие решать с помощью компьютера повседневные задачи, предполагающие удовлетворение различных цифровых потребностей;
- цифровые компетенции, позволяющие эффективно и безопасно использовать компьютер и соответствующее ПО для решения различных технических задач.

ПРОСТЫМИ СЛОВАМИ

- Уметь искать информацию, понимать ее и использовать;
- Отличать реальные данные от фейков;
- Критически воспринимать новые данные и публикации;
- Уметь пользоваться электронными сервисами;
- Создавать свое в цифровом виде;
- Понимать, что такое безопасность, и быть осторожными;
- Осваивать новые сервисы и технологии.

ЧТО КАСАТЕЛЬНО БИБЛИОТЕКАРЕЙ?

Умение работать с информацией, верифицировать ее, систематизировать и хранить – базовые компетенции библиотекаря.

Умение работать с цифровыми сервисами – необходимость.

Безопасности нужно учиться.

БЕЗОПАСНОСТЬ

Информационная безопасность

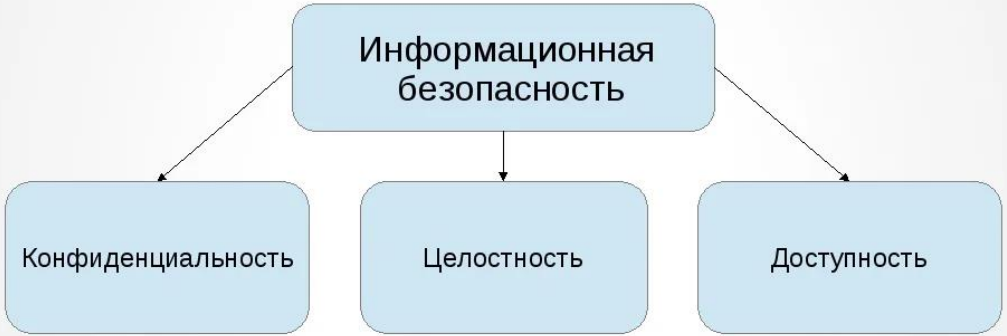
Медиабезопасность

Финансовая безопасность

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность

Информационная безопасность — это процесс обеспечения **конфиденциальности, целостности** и **доступности** информации.

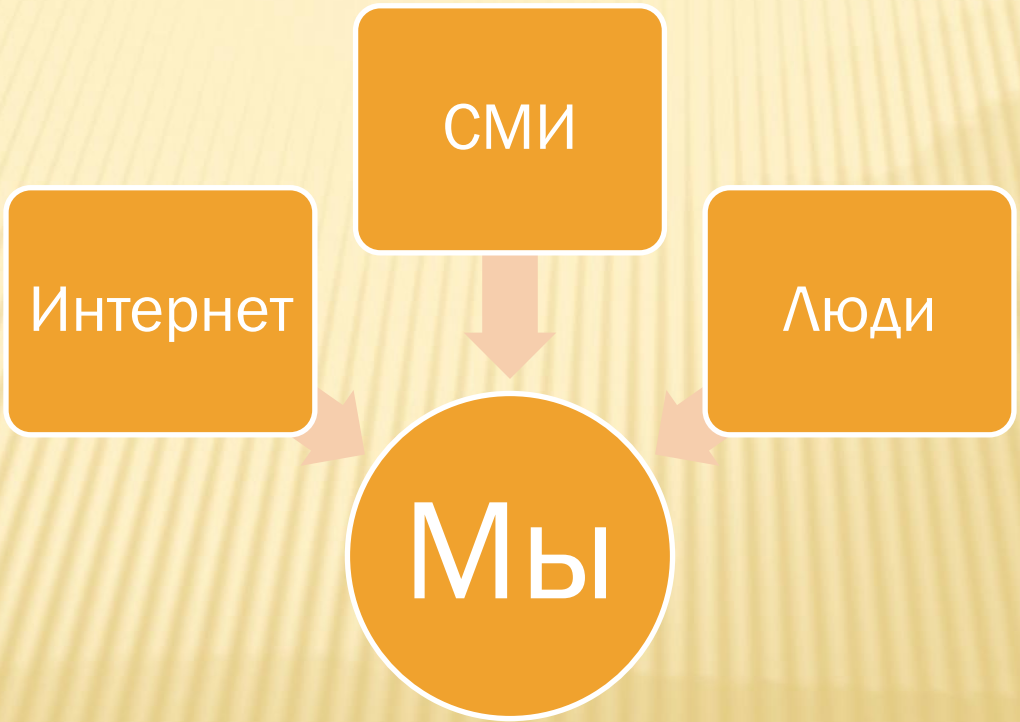


Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.

Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.

Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

МЕДИАБЕЗОПАСНОСТЬ

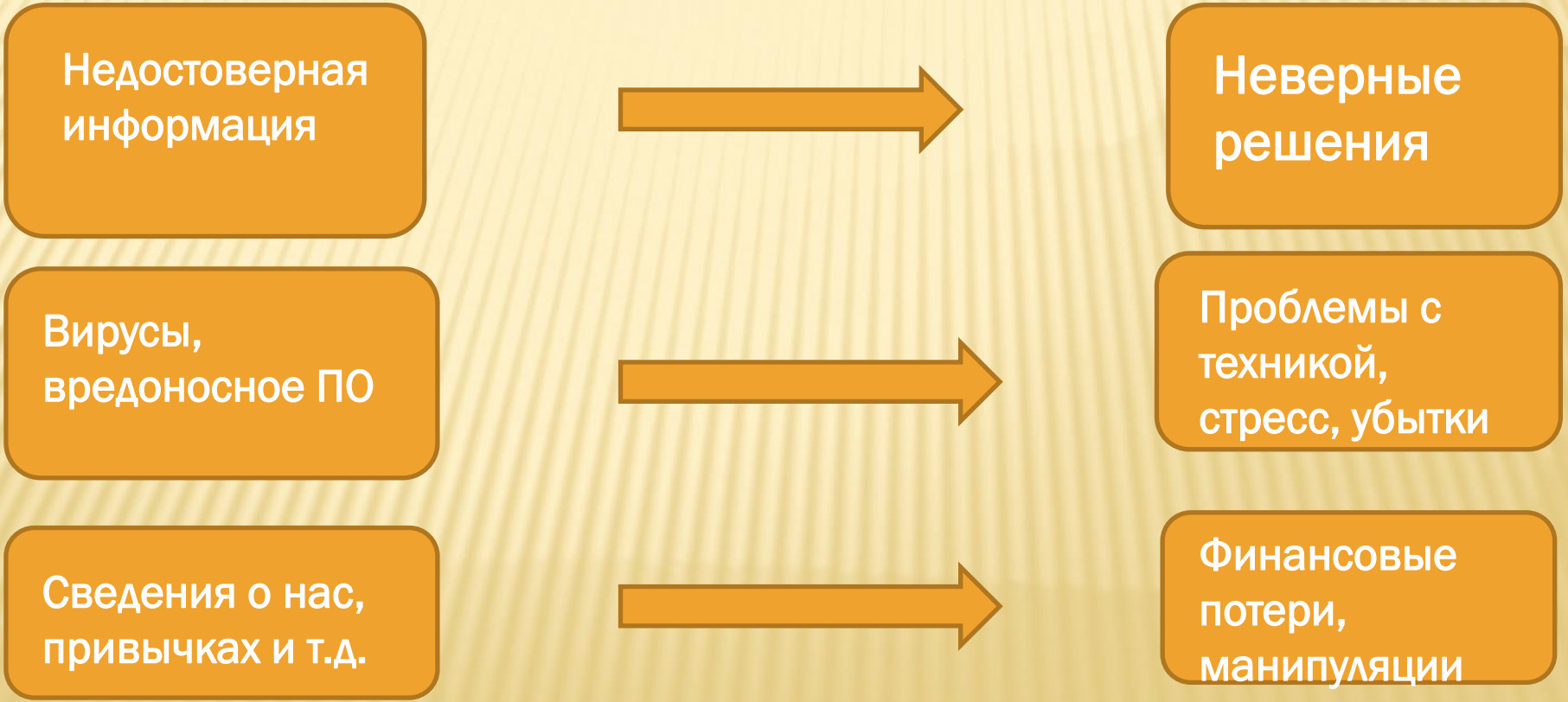



И чем же это плохо?

ОПАСНОСТИ МЕДИАСРЕДЫ

- Информационная
- Техническая
- Персональные данные
- Финансы

ИНФОРМАЦИОННАЯ ОПАСНОСТЬ



РЕШЕНИЯ, КОТОРЫЕ МЫ ПРИНИМАЕМ:

- Учеба
- Трудоустройство
- Покупка на крупную сумму
- Кредит
- Личные решения

ЗАВИСЯТ ОТ НАШЕЙ ИНФОРМИРОВАННОСТИ.

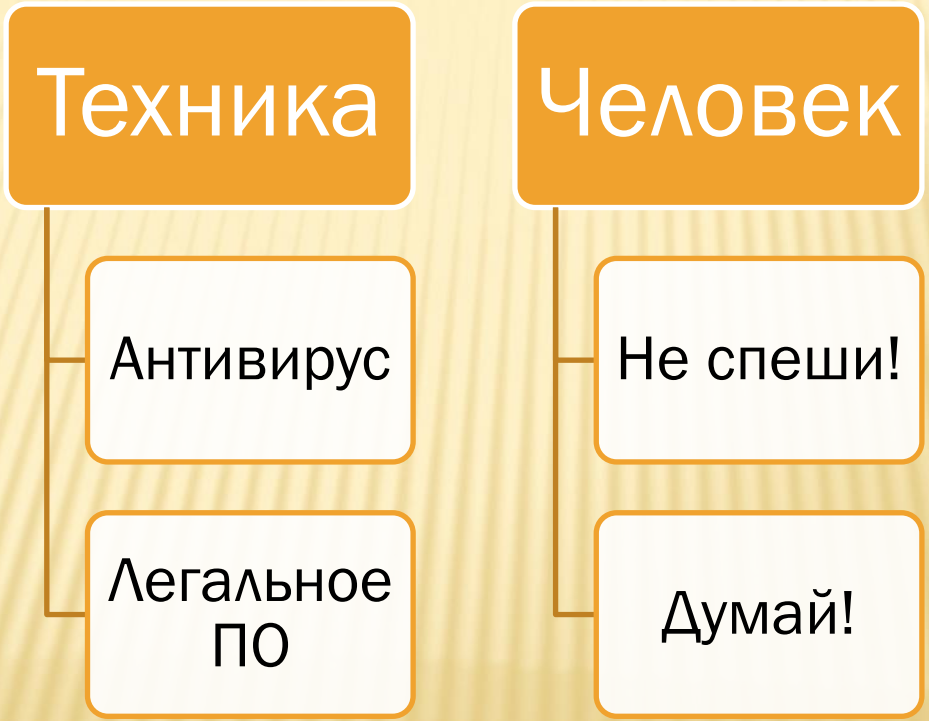
ПРАВОВОЙ АСПЕКТ

- N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»
- N 5485-1 «О государственной тайне»
- N 98-ФЗ «О коммерческой тайне»
- Ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан»
- Ст. 207.2. УК РФ «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия»
- Ст. 13.14.1. Кодекса об административных правонарушениях «Незаконное получение информации с ограниченным доступом»

И НЕ О ПРАВЕ

По данным компании Proofpoint, производящей решения для безопасности электронной почты, менее 1% всех атак эксплуатируют уязвимости систем. Остальные используют человеческий фактор.

ЧТО ДЕЛАТЬ?



ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ

- На всех гаджетах, с которых мы выходим в интернет, должен стоять антивирус.
- Все программы нужно регулярно обновлять, особенно антивирус и ОС.
- Не скачивать и не устанавливать пиратское ПО, «сломанные программы».

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ

- Не надеяться на авось.
- Не вводить личных данных и тем более платежных данных где попало.
- Думать, что и зачем вы пишете в интернете.
- Не публиковать фото карт, билетов, документов; фото машин и дома – только в закрытых альбомах.
- Следить, какие разрешения требуют приложения на телефоне и компьютере (зачем игре доступ к телефонной книге?).

СЕТИ WI-FI

- Выбирайте официальные точки доступа wi-fi (в госучреждениях, библиотеках, Макдональдс).
- Незапароленные сети, требующие в обмен на доступ номер телефона, e-mail, лучше не использовать (угроза спама, взлома).
- Бесплатная сеть без пароля – скорее всего, ловушка для попытки взломать и использовать ваше устройство.

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

Складывается из умения сберегать финансы (не сообщать свои данные, обезопасить свои банковские приложения, не переводить деньги с помощью сетей wi-fi, не переходить по ссылкам сомнительного вида, не участвовать в сомнительных схемах и т.д.) и умения здраво подходить к вопросу приумножения (вдумчиво изучить вопрос инвестирования и т.д.).

КОМУ НУЖНЫ МОИ ДАННЫЕ?

- Государство
- Бизнес
- Злоумышленники

ГОСУДАРСТВО

- Контроль
- Учет
- Управление
- Планирование
- Предупреждение и раскрытие преступлений

ЗЛОУМЫШЛЕННИКИ

- Кража денег
- Мошенничество
- Использование уязвимости устройства для внедрения различных программ
- Шантаж
- Использование чужих аккаунтов для противоправной деятельности

БИЗНЕС

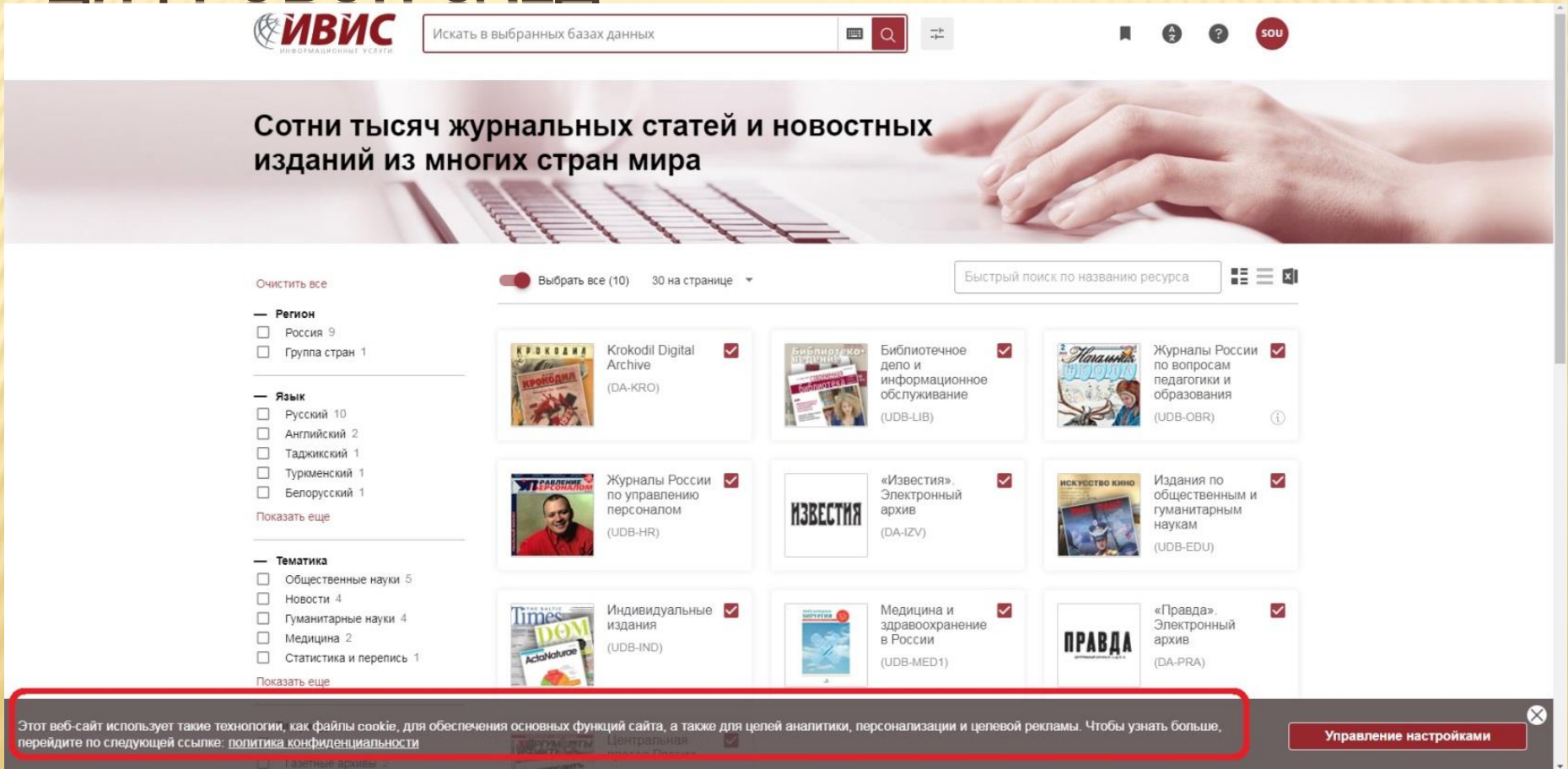
- Что покупатель хочет?
- Как он принимает решение о покупке?
- Что сильнее влияет на его решения?
- Нельзя ли заставить его хотеть то, что бизнес продает?
- Что будет, когда все покупатели уже купят то, что бизнес продает?

ЦИФРОВОЙ СЛЕД

Цифровой след

- совокупность информации о посещениях и вкладе пользователя во время пребывания в цифровом пространстве
- оказывает влияние на:
  - ✓Конфиденциальность информации
  - ✓Доверие
  - ✓Безопасность
  - ✓Цифровую репутацию

ЦИФРОВОЙ СЛЕД



ЦИФРОВОЙ СЛЕД

Веб-сайты сохраняют и аккумулируют информацию о каждом обращении к ним. С какого устройства, с какой ОС, с какого IP заходил пользователь, сколько времени провел на сайте, как перемещался по страницам сайта, какие товары его интересовали больше, какие меньше.

ОБОЮДНАЯ ВЫГОДА?

По идее, когда бизнес понимает закономерности поведения потребителя (каждого из нас), он может повлиять на это поведение в своих интересах. Будет ли это выгодно и нам тоже?

К примеру, мы можем сообщать свое местоположение сотовой компании в обмен на возможность ставить геотеги и получать прогноз погоды.

ЧТО ДЕЛАТЬ?

- Оценивать выгоду от предоставления данных для себя и только для себя.
- Отказываться от сервисов, которые требуют избыточные данные.
- Использовать все технические возможности для защиты своих данных и гаджетов.
- Не подключаться к публичным сетям wi-fi без острой необходимости.
- Учить безопасному поведению родственников, читателей и детей.

ПОЛЕЗНЫЕ РЕСУРСЫ

- ЦИФРАтека – библиотека материалов по безопасности в цифровой среде для детей (https://cifrateka.ru/)
- База знаний РОЦИТ – подборка материалов по безопасному поведению в цифровой среде для детей и взрослых, о цифровых сервисах и услугах, о мошенничестве и способах ему противостоять (https://rocit.ru/knowledge_base/)
- Учебник по информационной безопасности (https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf?ysclid=lu881p5teg76050136)

ЦИФРОВОЙ ЭТИКЕТ

Деловой и светский этикет помогает строить общение эффективно и безопасно. Мы знаем, что в деловой среде в начале встречи принято пожимать руки и представляться — это создает атмосферу доверия и помогает выстраивать рамки общения. Цифровой этикет выполняет ту же функцию в онлайн-пространстве.

ЦИФРОВОЙ ЭТИКЕТ

Цифровой этикет основан на тех же принципах, что и этикет в личном общении:

- соблюдение личных границ;
- экономия ресурсов;
- демонстрация уважения.

ЛИЧНЫЕ ГРАНИЦЫ

Цифровая коммуникация позволяет нам быть на связи абсолютно всегда. Некоторые злоупотребляют технологиями: если раньше мы бы трижды подумали, стоит ли звонить человеку после 20:00, то теперь многие готовы отправить рабочее сообщение даже ночью. Если вы не договорились с собеседником о том, насколько это поведение приемлемо, делать так не следует.

ЭКОНОМИЯ РЕСУРСОВ

- Договаривайтесь о звонках заранее;
- Важные моменты лучше обсуждать в переписке, где легко найти все моменты по ключевым словам;
- Не используйте голосовые сообщения без договоренности;
- Если переписка происходит в мессенджере, не дробите сообщения без нужды.

ДЕМОНСТРАЦИЯ УВАЖЕНИЯ

Обращайтесь к собеседнику так, как он вам представился: используйте форму имени или имя с отчеством. Сохраняйте необходимую дистанцию в общении, благодарите собеседника, если он выполнил вашу просьбу и ответил на вопрос.

Некоторые формулировки в устной речи звучат доброжелательно благодаря интонации и мимике, но на письме могут выглядеть как слишком строгие, неприветливые и даже агрессивные. Смягчайте их, чтобы ненароком не обидеть собеседника.

ВЫСТРАИВАЕМ ГРАНИЦЫ

- Определите основной канал связи;
- Определите резервный канал связи;
- Договоритесь о времени связи;
- Настройте автоответ в нерабочее время.

ГЛАВНЫЕ ПРИНЦИПЫ СЕТЕВОГО ЭТИКЕТА В ПЕРЕПИСКЕ

- Начинайте диалог с приветствия. Сообщите собеседнику, кто вы и почему пишете сообщение.
- Делите сообщения на абзацы. Одна мысль — один абзац. Так собеседнику будет проще воспринимать текст, а еще он не потеряет нужные мысли.
- Указывайте тему письма. Если пишете на почту, не забудьте написать тему письма, иначе оно может затеряться среди других.
- Благодарите собеседника, если он ответил на вопрос или выполнил просьбу.
- Пишите грамотно — перечитывайте письмо и перепроверяйте, если не знаете, как пишется слово.
- Не отправляйте неинформативные письма, например эмоджи или стикеры. Это отвлекает собеседника.

ЧТО ДЕЛАТЬ, ЕСЛИ НАРУШИЛИ?

Универсальный совет: проговорите сразу. Неважно, требует ли ошибка немедленных извинений, или достаточно просто проговорить, что случилось, и что вы осознаете ошибку.

ОБЯЗАТЕЛЬНО ТРЕБУЮТ ИЗВИНЕНИЙ:

- Ошибка в имени адресата;
- Ошибка в адресе.

Все, что мы проявляем в цифровой коммуникации, становится частью репутации! Все, что появляется в интернете, там и остается!

ДОМАШНЕЕ ЗАДАНИЕ

Оцените свое поведение в интернете, в публикациях в социальных сетях, сделайте выводы: достаточно ли вы заботитесь о своей безопасности, нужно ли вам уменьшить свой цифровой след? Кратко аргументируйте.

Спасибо за внимание!

Сизова А.В.
главный библиограф
отдела электронных ресурсов
ГАУК СОУНБ им. В.Г. Белинского
z_inf@uraic.ru