Безопасность в сети Интернет

Методист отдела внедрения ИКТ

Корниевич А.И.

Цель

сформировать и расширить компетенции при работе в сети Интернет для обеспечения безопасного поведения детей и взрослых

План

Знакомство с нормативной правовой документацией по вопросам информационной безопасности.

Презентация совместного проекта МТС и Детского фонда ООН (ЮНИСЕФ) по профилактике кибербуллинга среди детей и подростков.

Совершенствование знаний по вопросам формирования безопасной информационно-образовательной среды, безопасному использованию сети Интернет и профилактики киберпреступности.

Интернет сегодня - важнейший институт социализации человека в современном обществе

Копия реальности

Гибридизация

Способность к воспроизведению всего спектра повседневных ощущений

Метафоричность

Анонимность

Понятия и их определения

Компьютерная безопасность меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет. **Источник**

Цифровая безопасность представляет собой сочетание инструментов и привычек, которые пользователи могут использовать, во избежание контроля над их действиями в Интернете, доступа или вмешательства в их электронную информацию и вмешательства в их электронные устройства и программы. **Источник**

Цифровая грамотность – набор компетенций, связанных с квалифицированным использованием компьютеров и информационных технологий. **Источник**

Цифровая гигиена – это свод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет. Относится к сфере знаний о цифровой безопасности. **Источник**

Понятия и их определения

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз. **Источник**

Кибербуллинг – это травля с использованием цифровых технологий. **Источник**

Тро́ллинг — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации. **Источник**

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. **Источник**

Нежелательный контент – это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, но и различные вредоносные и шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством. **Источник**

Понятия и их определения

Фишинг – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, интернет-банкингу и т.д.). **Источник**

Вишинг – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль, вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой. **Источник**

Смишинг – вид мошенничества, целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения. **Источник**

Сваттинг – тактика домогательства, которая реализуется посредством направления ложного вызова той или иной службе. Например, люди сообщают о минированиях, преследуя цель устроить неразбериху и панику в конкретном месте. **Источник**

Груминг – это установление дружеского и эмоционального контакта с ребенком в Интернете для его дальнейшего совращения.

Нормативные документы

Закон Республики Беларусь от 7 мая 2021 года № 99-З «О защите персональных данных» Ссылка

Закон Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации» Ссылка

Закон Республики Беларусь от 11 мая 2016 года № 362-З «О внесении изменений и дополнений в некоторые законы Республики Беларусь» Ссылка

Указ Президента Республика Беларусь от 1 февраля 2010 года №60 «О мерах по совершенствованию использования национального сегмента сети Интернет» Ссылка

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 26 февраля 2015 года № 16 «О некоторых вопросах регистрации доменных имен» Ссылка

Нормативные документы

Постановление Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 года № 6/8 «Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет» Ссылка

Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1 «О Концепции информационной безопасности Республики Беларусь» Ссылка

Закон Республики Беларусь от 19 ноября 1993 г. О правах ребенка Статья 37-2. «Меры по защите детей от информации, причиняющей вред их здоровью и развитию» Ссылка

Постановление Совета Министров Республики Беларусь 29 января 2021 г. № 57 О Государственной программе «Образование и молодежная политика» на 2021–2025 годы. Ссылка

Законодательство по киберпреступлениям

В **Уголовном кодексе Республики Беларусь** содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

•ст.212 «Хищение путем использования компьютерной техники»;
•ст.349 «Несанкционированный доступ к компьютерной информации»;
•ст.350 «Модификация компьютерной информации»;
•ст.351 «Компьютерный саботаж»;
•ст.352 «Неправомерное завладение компьютерной информацией»;
•ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;
•ст.354 «Разработка, использование либо распространение вредоносных программ»;
•ст.355 «Нарушение правил эксплуатации компьютерной системы или сети»

Актуальная статистика в мире и Беларуси

59,5% глобальное проникновение интернета

53% используют социальные сети (населения мира)

рост за год составил +13%

82,8% проникновение интернета в Беларуси

41% используют социальные сети населения Беларуси

95% из этих пользователей используют соцсети с мобильных устройств

Актуальная статистика в мире

2 часа 25 минут каждый день

среднестатистический пользователь социальных сетей, что соответствует примерно одному дню бодрствования в неделю.

7 часов в день

В среднем человек проводит в интернете.

Год назад этот показатель был равен 6 часов 43 минуты.

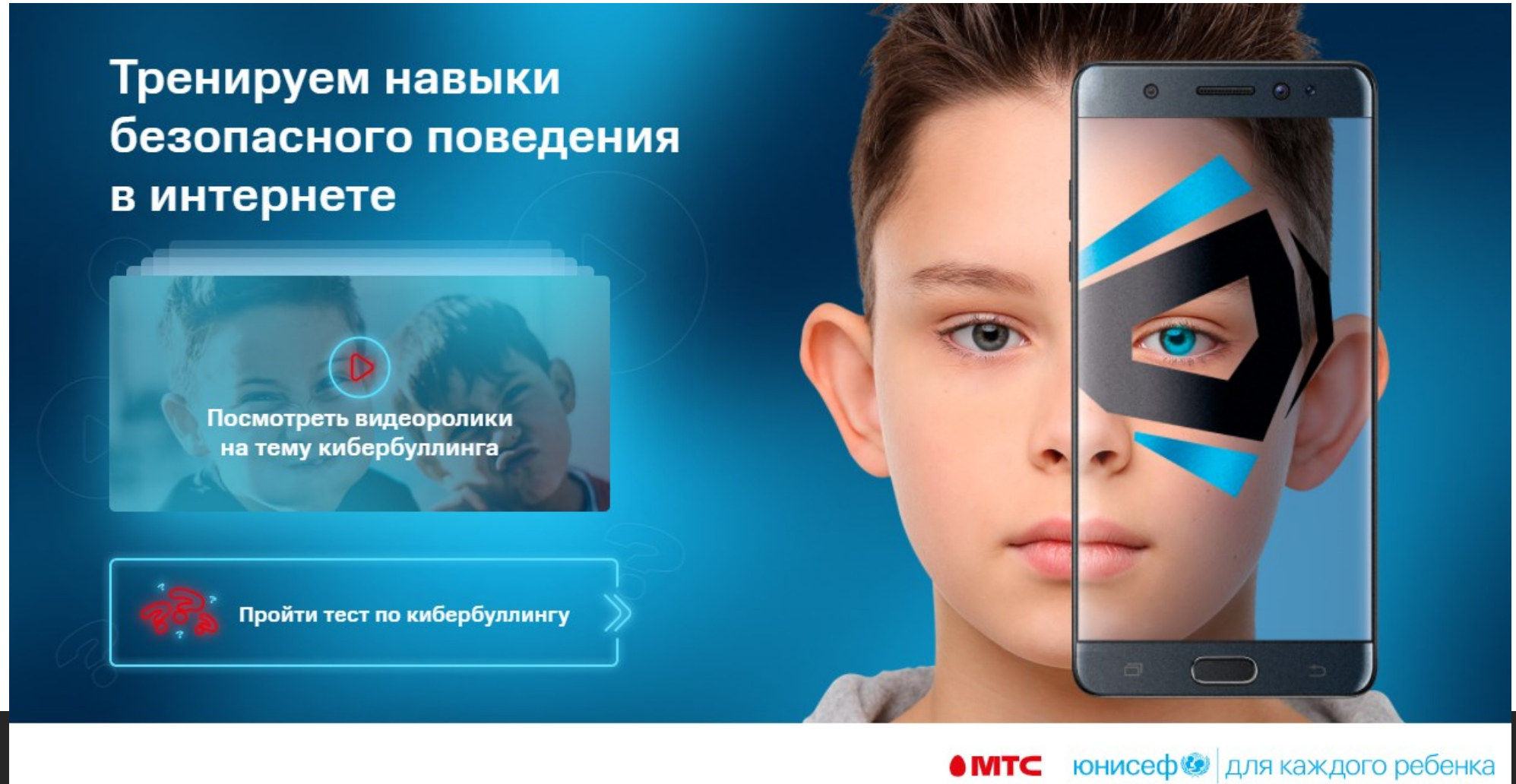
По информации Белстата в Беларуси

84% детей в возрасте 6-10 лет

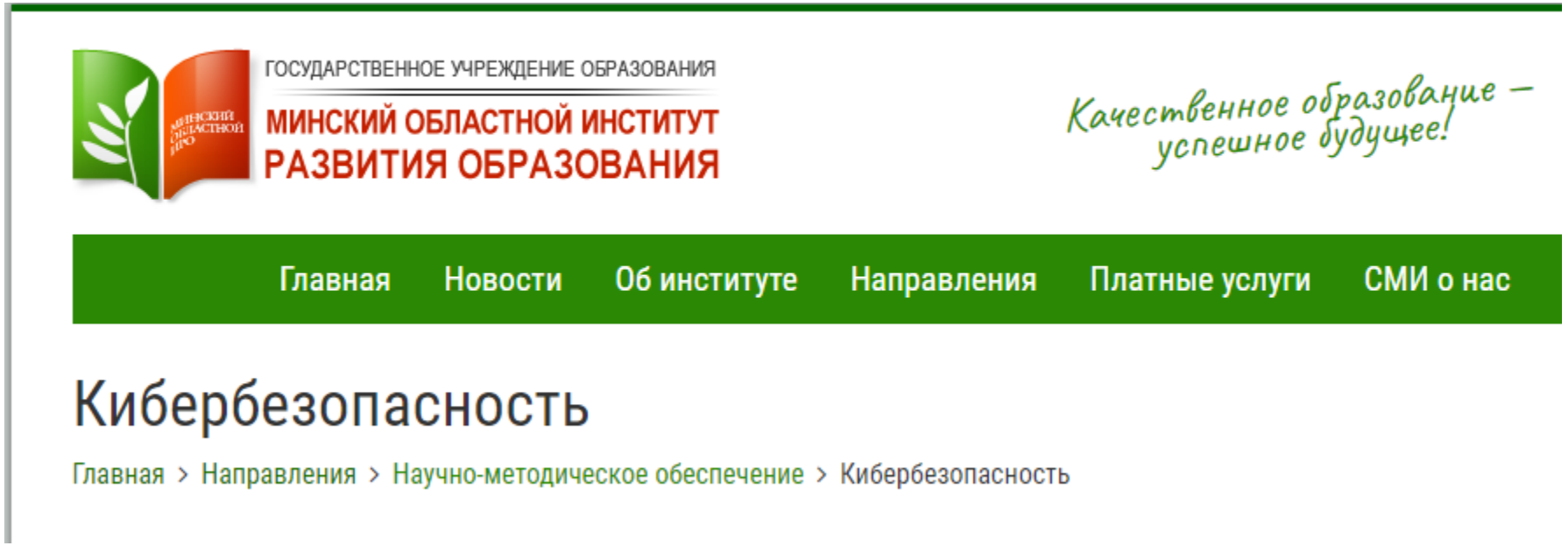
98,1% детей в возрасте 11-15 лет

Совместный проект МТС и Детского фонда ООН (ЮНИСЕФ) по профилактике кибербуллинга среди детей и подростков

[Ссылка]



Ресурсы


ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
МИНСКИЙ ОБЛАСТНОЙ ИНСТИТУТ
РАЗВИТИЯ ОБРАЗОВАНИЯ
Качественное образование –
успешное будущее!
Главная
Новости
Об институте
Направления
Платные услуги
СМИ о нас
Кибербезопасность
Главная > Направления > Научно-методическое обеспечение > Кибербезопасность

Классификация областей сети Интернет, наиболее подверженных рискам

Направления	Характеристика	Риск для пользователя
Техносфера	техническая безопасность и базовая техническая грамотность пользователей	заражение ПК либо мобильного устройства вирусом, потеря информации
Сфера потребления	заказы, услуги, покупки, совершаемые онлайн	безопасность личных данных (пароли доступа к банковской карте, аккаунту), мошенничество, финансовые потери
Информационная среда	создание, поиск, отбор, критическая оценка контента	потребление незаконного и непредназначенного для детей контента
Сфера коммуникации	создание, развитие, поддержание отношений, самопрезентация, идентичность, репутация	разглашение личной и/или конфиденциальной информации, троллинг, кибербуллинг

Рекомендации при работе в сети

- Внимательно следить за тем, какие веб-сайты открываются и что загружается. Адрес сайта начинается с комбинации https:// – это значит, что соединение с веб-сайтом зашифровано.
- При подключении через общедоступную сеть Wi-Fi нельзя пользоваться платежными системами и другими важными сервисами.
- Необходимо использовать надежные пароли. Не использовать один и тот же пароль для доступа в различные аккаунты. Регулярно изменять свои пароли
- Регулярно обновлять браузер и операционную систему. Устанавливать ПО только из надежных источников.
- В случае обнаружения подозрительных признаков работы ПК после загрузки из сети интернет, нужно немедленно удалить ПО и проверить систему с помощью антивирусной программы.

Контентные риски в сети Интернет и способы защиты от негативной информации

Информация оказывает

благоприятное влияние

негативное влияние

Основные виды негативного контента:

1) информация, пропагандирующая либо оправдывающая войну и иные международные преступления;

2) информация, пропагандирующая либо оправдывающая терроризм, иные преступления и правонарушения;

3) информация, разжигающая расовую, национальную, религиозную ненависть и вражду, пропагандирующая либо оправдывающая экстремистскую деятельность;

4) информация, оскверняющая историческую память, символы воинской славы или государственные символы;

5) информация, оскорбляющая религиозные чувства верующих;

6) информация, отрицающая или дискредитирующая традиционные ценности, пропагандирующая деструктивные ценности и установки;

7) информация, пропагандирующая либо оправдывающая насилие и жестокость, девиантное поведение, а также действия, опасные для жизни и здоровья человека;

Основные виды негативного контента:

8) информация о способах и средствах совершения преступлений, иных правонарушений или антиобщественных действий, а также действий, опасных для жизни и здоровья человека;

9) сексуально откровенный контент и иная непристойная информация;

10) нецензурная брань;

11) контент устрашающего характера, включая изображение или описание насилия, жестокости, катастроф или несчастных случаев;

12) заведомо ложная информация;

13) дискредитирующая информация;

14) скрытая информация, воздействующая на подсознание человека;

15) реклама товаров и услуг, которые могут причинить вред жизни и здоровью человека.

Средства защиты от нежелательного контента

безопасный поиск

специальное ПО

формирование и развитие у них информационной культуры

Поведение педагога в социальных сетях

- Отказа от общения в социальной сети с учениками
- Включения учеников в «друзья», общение с ними в социальных сетях

Противодействие и профилактика киберпреступности

Фишинг

Вишинг

Фальшивый сайт

Противодействие и профилактика киберпреступности

ЗВОНОК ИЗ БАНКА

ЗАНЯТОЙ ПОКУПАТЕЛЬ

ДЕШЕВЫЕ ВЕЩИ

АРЕНДА КВАРТИР

ПИСЬМО ОТ ДРУГА

РОЗЫГРЫШИ И ЛОТЕРЕИ (ОТДАМ ДАРОМ)

СБОР ДЕНЕГ НА ЛЕЧЕНИЕ

МНЕ ТОЛЬКО ПОЗВОНИТЬ

Общие правила при работе в Интернете

1. Поступайте и пишите в Сети так, как поступили бы в реальной жизни и как хотели бы, чтобы поступали с вами.
2. Уважайте своих собеседников и чужую собственность в Интернете, за ними скрываются настоящие люди и реальный труд.
3. Не сохраняйте на своем компьютере неизвестные файлы, не переходите по ссылкам от незнакомцев, какими бы заманчивыми они не были.
4. Обязательно установите антивирус и фаерволи регулярно обновляйте их базы.
5. Не запускайте неизвестные файлы, особенно с расширением *.exe
6. Старайтесь давать как можно меньше информации о себе в Интернете.
7. Будьте осторожны при общении с незнакомыми людьми.