



КООРДИНАЦИОННЫЙ ЦЕНТР
НАЦИОНАЛЬНОГО ДОМЕНА
СЕТИ ИНТЕРНЕТ

Качество и безопасность информации: национальные интересы

Михаил Анисимов

1. Рассказ о рисках, с которыми пользователи могут столкнуться в интернете
2. Рассказ о том, как можно дать обратную связь, если пользователь столкнулся с угрозой
3. Удаление противоправного контента и создание безопасной доверенной среды

Опасность: Вся информация, которую вы отдаете интернету, остается там навсегда

© nokia.ru



Совет: Ни в коем случае не оставлять свои данные (адрес, телефон, личные фотографии, информацию из документов) на непроверенных сайтах

Опасность: Мошенники часто обманом похищают деньги при покупках в интернете



Совет: Все покупки в интернете должны делаться только на проверенных сайтах. Нельзя оставлять на неизвестных сайтах номера кредитных карт и банковского счета

Как проверить надежность сайта:

1. Сайт широко известен и знаменит

Яндекс



2. У сайта есть специальный сертификат, и в адресной строке перед доменом виден замочек



Опасность: На ваш компьютер, ноутбук, телефон или планшет могут быть установлены вредные программы

Виды вирусов:

1. Шифровальщики. Они превращают всю информацию на компьютере или телефоне (фотографии, контакты, документы) в набор нечитаемых букв и цифр. Чтобы расшифровать их нужен код, за который мошенники просят деньги
2. Троянские программы. Они устанавливаются скрытно и похищают данные пользователя
3. «Зомби». Они используются для того чтобы управлять компьютером извне и рассылать с него спам, рекламу или атаковать другие компьютеры

Как вирусы попадают на компьютеры и телефоны

Опасность: Вирусы могут приходить в письмах, по ссылкам в чатах, мессенджерах, социальных сетях



Совет: Не открывать вложения в письма, которые пришли от неизвестных людей, не открывать неизвестные ссылки

Как вирусы попадают на компьютеры и телефоны

Опасность: Вирусы могут распространяться с флешками и дисками, которые раздают на выставках, концертах, фестивалях



Совет: Не вставлять в компьютер или телефон флешки и диски, приобретенные у неизвестных людей

Как вирусы попадают на компьютеры и телефоны

Опасность: Вирусы могут попадать на компьютеры и телефоны через неизвестные приложения в магазинах



Совет: Проверять, насколько приложение новое (а значит возможно еще не проверенное) и обязательно читать о нем отзывы.

Опасность: Интернет-хулиганы («Тролли») могут специально провоцировать людей ругательствами, спорами и нападками

**НЕ КОРМИТЕ
ТРОЛЛЕЙ!**

не отвечайте на их темы
пускай они будут
забыты или закрыты!



Совет: «Не кормить троллей» - не давать повода вывести себя из равновесия, игнорировать чужую ругань и нападки

Опасность: Взрослые злоумышленники часто притворяются детьми и подростками чтобы узнать что-то у вас или выманить на встречу

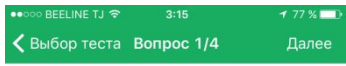


Совет: Не рассказывать ничего лишнего людям, которых вы никогда не видели в реальности, и не ходить с ними на встречи. Если попытки продолжаются, сообщить родителям или учителям

Образовательные и просветительские программы позволяют обучать дистанционно и в игровой форме



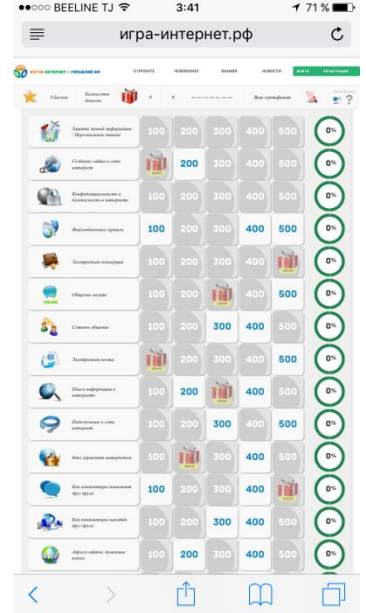
Изучи интернет!	
История Интернета – 1	1050 / 1...
Устройство Интернета – 1	1050 / 1...
Браузеры и интернет-сервисы – 1	800 / 1050
Интернет в России – 1	0 / 1050
Интернет-сайты – 1	0 / 1050
Интернет-культура – 1	0 / 1050
Безопасность и конфиденциальность в Интернете – 1	0 / 1050
Браузеры и интернет-сервисы – 2	0 / 1100
Интернет в России – 2	0 / 1100
Интернет-культура – 2	0 / 1100
Браузеры и интернет-сервисы – 3	0 / 1150
Интернет-сайты – 2	0 / 1100
История Интернета – 2	0 / 1100
Браузеры и интернет-сервисы – 4	0 / 1100



Как называется рассылка рекламы или иных видов сообщений лицам, не выразившим желания их получать.



- мусор
- СПАМ
- анонимная реклама



Необходимо, чтобы пользователи знали не только как распознать угрозу, но и что делать при столкновении с ней



Подать сообщение о ресурсе, содержащем запрещенную информацию

** - поля, обязательные для заполнения*

Указатель страницы сайта в сети "Интернет" *
(с обязательным указанием протокола)

Источник информации

Тип информации *

Скриншот
(pdf, jpeg, png; не более 1Мб)

Вид информации *

Доступ к информации

Дополнительная информация
в том числе логин/пароль и/или иные сведения
для доступа к информации

веб-сайт

Выберите файл | Файл не выбран

рисованные изображения
 видео изображения
 фото изображения
 текст
 online-трансляция
 другая информация

свободный

Досудебная блокировка сайтов. Как все происходит?

1. Жалоба поступает в Роскомнадзор (или он попадает в мониторинге).
2. Роскомнадзор -> хостинг-провайдер
3. Хостинг-провайдер -> клиент
4. Клиент устранил добровольно – «Всем спасибо! 😊»
5. Связи нет / не успел / не пожелал - сайт блокируется на уровне провайдера
6. Одумался, устранил, сообщил – доступ возобновляется.

3 дня

Компетентные организации

С 2012 года Координационный центр внедрил практику взаимодействия с организациями, компетентными в определении нарушений в интернете



Спасибо!

E-mail: m.anisimov@cctld.ru