
# Цифровая карта безопасности школьника

Интернет стал неотъемлемой частью нашей жизни, мы подключаемся к нему дома, в школе и даже в путешествиях стараемся найти точку доступа для обновления новостной ленты. Но Интернет делает доступным не только общение и поиск информации, он делает доступными личные сведения о нас. И чтобы наши данные не попали в чужие руки, нужно знать основные правила безопасности, о которых не так часто рассказывают. А знаешь ли их ты? Помоги сделать эти сведения доступнее, создай свой сайт о базовых правилах цифровой безопасности.

Group-IB — международная компания, специализирующаяся на предотвращении кибератак и разработке продуктов для информационной безопасности. Поставщик Threat Intelligence (кибербразведка), вошедший в отчеты исследовательских компаний Gartner и Forrester и Официальный партнер Europol и Interpol, член Всемирного экономического форума (WEF), а также Резидент «Сколково».

**Введение:**

Как защитить детей от киберпреступности? Также, как и взрослых, только лучше, умнее и тоньше. Выросло несколько поколений, которые ориентируются в Интернете лучше, чем их родители. Интернет, мессенджеры и закрытые группы для них— такие же экстремальные места для общения и игр, как для поколения 80-х, были стройки, гаражи и лесопарки. Но это не снимает ответственности с родителей и учителей — подготовить ребенка ко встрече с опасностью и уберечь от соблазнов.

В США дети в 6–8 лет изучают основы компьютерной грамотности. В этом возрасте они узнают, что такое фишинг, кардинг и как не стать жертвой киберпреступников. Россия же была полигоном для всех новых типов хакерских атак и инструментов. Два года назад Group-IB выходили с инициативой в Министерство образования, предлагали часть часов информатики или ОБЖ выделять на правила компьютерной гигиены. Недавно в Совете Федераций был представлен курс для начального, общего и полного среднего образования «Основы кибербезопасности».

Противодействие киберпреступности — это совсем не «10 советов, как приготовить шоколадный пирог». Поэтому важно серьезно относится к своей кибербезопасности.

*Илья Сачков, основатель компании Group-IB*

**Проектная задача кейса:**

1. Изучить, что такое цифровая безопасность и какие правила цифровой гигиены существуют.
2. Создать лендинг (одностраничный мультимедийный сайт) о цифровой безопасности школьника. Подбор контента и его оформление ограничено только вашей фантазией.

**Требования и факты, которые необходимо учесть при решении проектной задачи кейса:**

-на лендинге должна быть информация по следующим темам:

1. Как безопасно пользоваться социальными сетями и мессенджерами?
2. Как защитить свою почту?
3. Как безопасно совершать покупки в Интернете?

-контент сайта должен быть ориентирован в первую очередь на школьников;

-лендинг может быть создан на любой из доступных платформ (Tilda, WordPress и т. д.).

**Справочный материал:**

Как не стать жертвой киберпреступников?

Советы для детей и подростков от компании Group-IB:

***Социальные сети и мессенджеры***

1. Возьми за правило публиковать как можно меньше личной информации и фотографий! Помни, все, что попало в интернет, осталось там навсегда и доступно всем!
2. Не сообщай никому в сети свой домашний адрес, свой номер телефона или номера телефона родителей.
3. Не хвались крупными дорогими покупками. Никогда не рассказывай в соцсетях о том, что вся семья уезжает, например, в отпуск.
4. Не доверяй новым виртуальным друзьям. Лицо на аватарке, имя и возраст твоего виртуального друга может быть вымышленным, а за дружелюбным собеседником может скрываться преступник. Не приглашай «виртуальных друзей» к себе домой, не встречайся с незнакомцами из сети, не предупредив своих родителей.
5. Не хами и не оскорбляй никого во время переписки в Интернете.
6. Наткнувшись на “тролля” в Интернете, прекрати диалог, не вступай в ссору или выяснение отношений.
7. Закрывай камеру на компьютере и не отправляй “виртуальным друзьям” свои фотографии и видео.
8. Если заходишь в социальную сеть (или почту) с чужого компьютера, не забудь нажать «выйти».

**Справочный материал:**

***Электронная почта, аккаунты, пароли***

1. Включи, где это возможно, двухфакторную аутентификацию: для доступа к ящику нужно ввести не только логин и пароль, но и код, который придет на мобильный телефон. Если эта функция подключена, перехвативший пароль взломщик, не имея доступа к телефону, не сможет получить доступ к вашей переписке.
2. Используй надежные безопасные пароли и регулярно их меняй, хотя бы раз в несколько месяцев. Безопасный пароль такой: lndcjhsjdwej;lewk;fkewojfpewjfkewnlfkjw;ojefpowj;lamwdlkhfeofh8993889 — пара строчек известной русской народной песни на английской раскладке.
3. Заведи несколько почтовых ящиков для разных целей: личный ящик, спам-ящик, для регистраций. Придумай сложный пароль, причем отдельный для каждого сервиса (и почтового ящика).
4. Никогда не отвечай на спам, не переходи по указанным в нем ссылкам и не открывай вложенные в письмо файлы, чтобы не заразить свое устройство вирусом. Помни, что зараженный вирусом смартфон превращается в мобильного шпиона!
5. По этой же причине не открывай подозрительные ссылки и письма, даже если они пришли от коллег и друзей!
6. Не храни важные документы и фотографии в облаках. При взломе лишишься не только неудачных селфи, но и чувствительных данных.

**Справочный материал:**

***Онлайн-покупки***

1. Используй для покупок в интернете специальную «виртуальную» карту. Не оставляй данные своей банковской карты или банковской карты родителей на незнакомых сайтах. Прежде, чем совершить оплату, несколько раз перепроверяй адрес отправителя, домен и ссылку. Сомневаешься — обратись за советом к родителям или специалистам.
2. Помни, что фишинговые сайты-клоны как две капли воды похожи на оригинальные ресурсы и не стоит переходить по ссылке и вбивать свои личные данные.
3. Не скачивай музыку, фильмы с торрентов нелегальным путем, не только потому что это незаконно, но и опасно — можешь загрузить зараженный вирусом файл. Пользуйся только официальными магазинами (App Store, Google Play и Windows Market).
4. Не оставляй свой номер телефона и не отправляй сообщения на короткий номер, чтобы бесплатно посмотреть фильм или послушать музыку. Не переводи деньги в ответ на просьбу из смс или любого другого мессенджера.
5. Совершая покупки в интернете, помни, что 40% фишинговых атак в мире против известных брендов приходится на e-Commerce. Оказавшись на странице фальшивого интернет-магазина, ты не только рискуешь остаться без покупок, но и отправить злодеям данные своей карты.

**Справочный материал:**

***Общественный Wi-Fi***

1. Не доверяй Wi-Fi-соединениям в общественных местах, где не спрашивают пароль, поскольку через такие сети чаще всего можно перехватить ваш трафик и ваши личные данные.
2. Если есть возможность – пользуйся мобильным интернетом.
3. Выключай Wi-Fi, если им не пользуешься, и обязательно отключи автоматическое подключение к Wi-Fi на вашем устройстве.

***12 базовых правил цифровой гигиены***

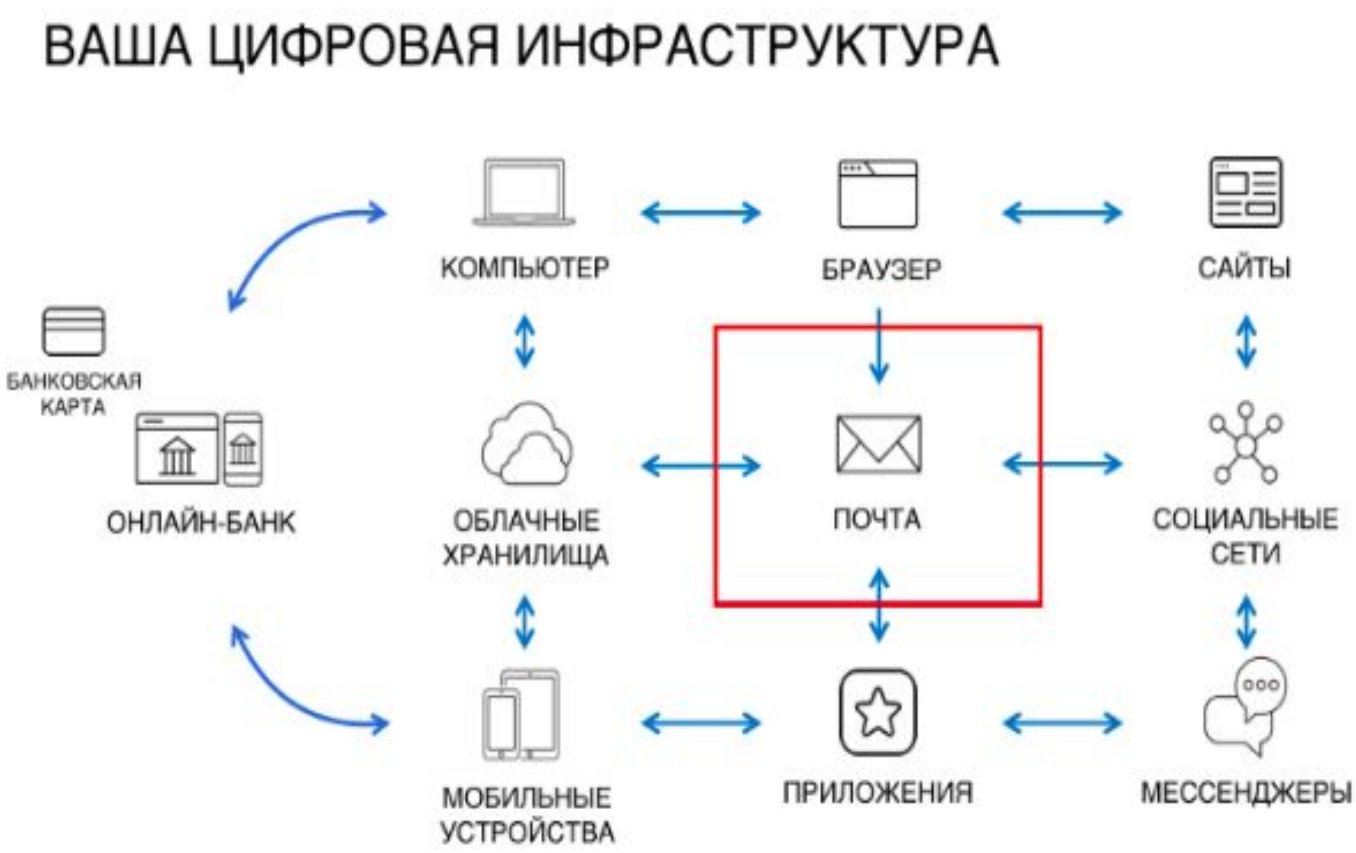
(https://medium.com/@sedakov/12-базовых-правил-цифровой-гигиены-26febe4d9461)

***Киберугрозы для школьников***

- взлом аккаунтов и кража информации;
- рекрутинг в хакеры - вирусописатели, взломщики и т.д.;
- шантаж и вымогательство;
- троллинг и оскорбления;
- деструктивные группы («Синие киты»);
- слежка через общественный wi-fi;

**Справочный материал:**

***Цифровая инфраструктура школьника: социальные сети, мессенджеры, электронная почта, компьютерные игры, смартфоны***



**Описание решения:**

Вот мы и добрались до описания решения кейса, этот раздел включает в себя 3 блока.

Тебе необходимо ответить на вопросы, ответы записывай сразу в этой же презентации под вопросом. Что делать, если не хватает места? Смело создавай новое. Главное, не меняй последовательность слайдов, формулировку вопросов и используй шрифт Calibri 18-го размера.

Внимательно изучи информацию о компании, проектную задачу и справочные материалы. Помни, что от того, насколько подробно ты описываешь решение, зависит то, насколько успешным будет решение. Удачи!

**Блок I: «Проверочный вопрос»**

Давайте проверим, как вы поняли тему кейса. Ответьте на поставленный вопрос:

Можно ли переходить на ссылки, присланные в e-mail рассылках от имени компаний или через контекстную рекламу в поисковых сетях, и вводить паспортные данные, если вам обещают подарки и бонусы? Обоснуйте свой ответ.

**Блок II: «Описание решения кейса»**

В этом блоке описывается основное решение кейса. Не забудьте учесть Требования и факты от заказчика кейса.

**1. Предложите не менее трёх основных типов угроз будущего (отличающихся от тематик из Требований и фактов от заказчика). Например, кража воспоминаний и т.д. Обоснуйте, чем именно они будут так опасны для школьника.**

(Минимальное количество символов в ответе - 350 символов, включая пробелы)

**2. Опишите не менее 3-х способов продвижения разрабатываемой Цифровой карты безопасности школьника, способствующих тому, чтобы лендинг был популярен у целевой аудитории.**
(Минимальное количество символов в ответе - 700 символов, включая пробелы)

**3. Какую инфографику, фото и видеоматериалы необходимо добавить на лендинг о цифровой безопасности школьников. Обоснуйте свой ответ. (Минимальное количество символов в ответе - 700 знаков, включая пробелы)**

**4. Подумайте, с какого возраста необходимо обучать детей информационной безопасности. Обоснуйте свой ответ.**

(Минимальное количество символов в ответе - 500 знаков, включая пробелы)

**5. Создайте лендинг (одностраничный мультимедийный сайт) о цифровой безопасности школьника, используя любую из доступных платформ (Tilda, WordPress и т.д.). Приложите ссылку на лендинг в ответе на данный вопрос.**

## III Блок “Оценка эффективности концепции”

Не пугайтесь, в этом блоке необходимо придумать 3 качественных или количественных показателя, по которым можно оценить эффективность разработанной Цифровой карты безопасности школьников. Например, критерий – количество посетителей лендинга в возрасте до 18 лет.

| № | Критерий оценки эффективности концепции |
|---|---|
| 1 | |
| 2 | |
| 3 | |

## IV Блок “О команде”

Опишите здесь роли и информацию обо всех участниках команды. Максимальное число участников в команде – 6 человек. Под каждого участника создайте свой слайд.

Фамилия

Имя

Отчество

Роль в команде

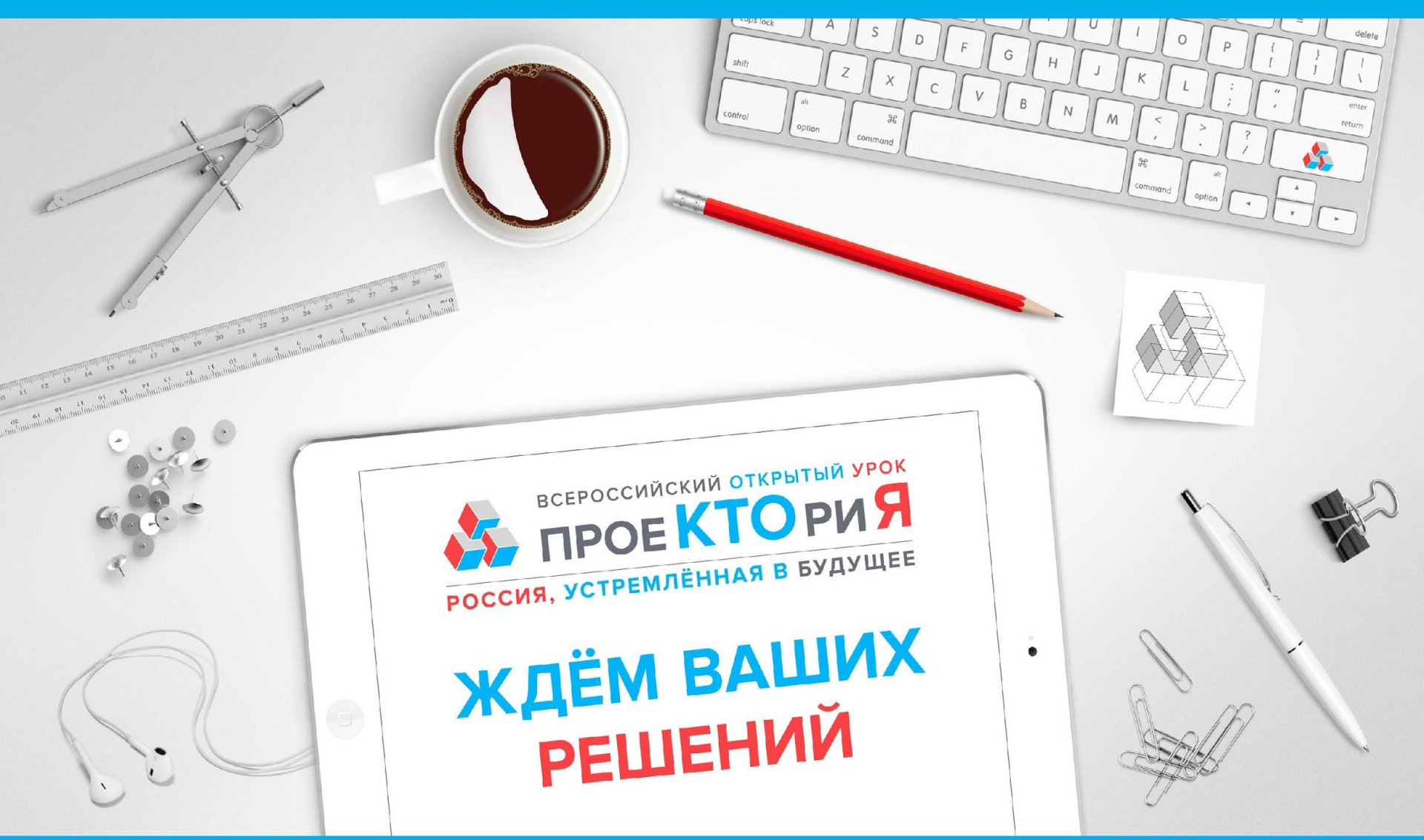
Город

Образовательное учреждение

Класс

E-mail

Предпочтительный способ связи
(email, телефон, vk, skype и т.д.)




http://proektoria.online

info@proektoria.online