ЦИФРОВАЯ ГИГИЕНА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

О необходимости обучать школьников основам кибербезопасности говорят уже как минимум лет двадцать, если не больше. Теперь в школах вводятся уроки цифровой грамотности в рамках курсов информатики и ОБЖ. Но сразу возникают по меньшей мере две проблемы – где найти в достаточном количестве учителей и как будет выглядеть единая методическая база таких уроков.



О БЕСПЛАТНЫХ КУРСАХ

Самое главное – кадры. Нужны квалифицированные педагоги, которые хорошо владеют информационными технологиями, а их не хватает. Значит, надо их готовить, как и методическую базу для обучения детей. Для этого крайне необходим опыт проведения таких занятий. Благо он имеется, и весьма эффективный.

Нет, мы сейчас не о расплодившихся на просторах Сети навязчивых платных предложениях такого рода, а о бесплатных профессиональных курсах, таких как, например, Education от «Лаборатории Касперского», уроки информационной безопасности от «Яндекс.Учебник» и, конечно же, курсы по кибербезопасности для школьников и учителей от компании «Киберпротект». О последних расскажем подробнее.

Идея создания бесплатного, доступного всем обучающего проекта по цифровой гигиене для детей и учителей родилась в голове Елены Бочеровой, исполнительного директора компании «Киберпротект», не случайно. Как мама двух сыновей и опытный в «цифре» профессионал, знающий все угрозы Сети, она изначально желала одного – защитить

детей и дать методическую базу педагогам для занятий по цифровой безопасности.

Конечно, казалось бы, нужно начинать с родителей, но они далеко не всегда компетентны в данных вопросах. И «родительский пример» зачастую не работает именно из-за отсутствия у многих пап и мам глубоких знаний в сфере борьбы с кибербуллингом, интернет-мошенничеством, вирусами, потерей данных и прочими бедами.

Кроме того, согласно исследованиям «Лаборатории Касперского», 58% детей в возрасте от 8 до 16 лет скрывают свои действия в Сети от родителей. При этом 73% участников опроса согласились, что хотели бы знать больше о киберугрозах, поскольку не чувствуют себя защищенными.

Следовательно, нужно давать базовые знания именно педагогам, а уж они научат цифровой безопасности детей. И конечно же, необходим курс для самих школьников для самостоятельного изучения. То есть своего рода ликбез, краткое, но профессиональное, предельно информативное и приближенное к практике обучение для учителей и школьников.

В результате родился Всероссийский образовательный проект по цифровой гигиене и информационной безопасности, который по инициативе Елены Бочеровой был разработан экспертами компании «Киберпротект» при участии образовательной онлайн-платформы CoreApp и информационной поддержке Агентства стратегических инициатив.

Проект включает в себя два бесплатных образовательных курса, дающих методическую базу учителям и представление школьникам о современных киберугрозах и основных способах противодействия им, принципах безопасного общения и поведения в Сети, хранения данных.

Курс повышения квалификации для учителей разработан в формате массового открытого онлайн-курса, состоящего из тринадцати уроков и одного контрольного блока, общей продолжительностью шестнадцать академических часов.

Детский курс состоит из трех уроков, разработанных с учетом требований ФГОС общего образования. Он предназначен для учеников 7–9-х классов.

Подчеркнем, что уроки проводятся в современном формате смешанного обучения по модели «ротация станций» и могут быть интегрированы как в учебные предметы «информатика» или «основы безопасности жизнедеятельности», так и во внеурочную деятельность.

То есть как раз то, о чем мы говорили выше: базовый опыт работы в данном направлении, вполне приемлемый для школ как вариант построения занятий. Конечно, наряду с другими наработками такого рода, которых немало. Главное, что есть из чего выбирать – это ведь не придумывать заново.

К проекту присоединились уже около половины регионов России, а на сайте cyber-care.ru зарегистрировалось порядка 2000 учителей по всей стране.



Все они хотят повысить квалификацию в области информационной безопасности и реализации детского курса «Уроки кибербезопасности» в своих образовательных организациях. Что вполне естественно, ведь в последние годы в интернете резко увеличилось количество агрессивных пользователей, мошенников и киберпреступлений.

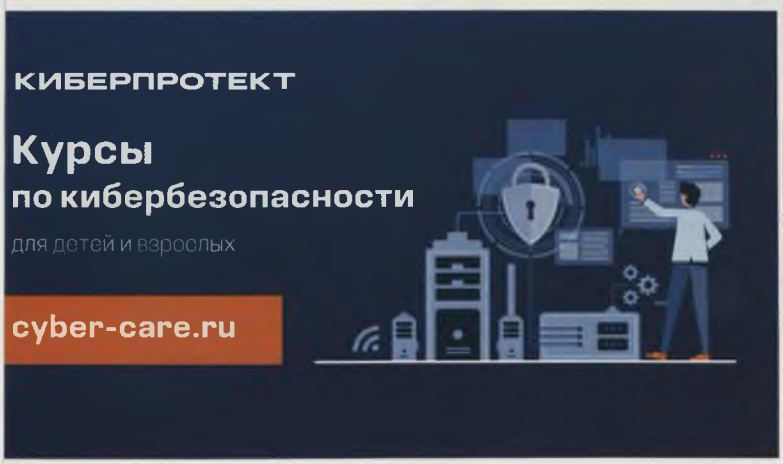
ОТЗЫВЫ ПЕДАГОГОВ

– Курсы повышения квалификации для учителей по кибербезопасности я прошел прошлой осенью, – *рассказывает Иван Рузин, преподаватель информатики столичной школы № 1560.* – Там очень много полезной информации, касающейся не только ИКТ, но и обществознания. Нас ознакомили с законодательством в области персональных данных, цифровых продуктов, нарушениями в сфере кибербезопасности, эффективными способами противодействия и многими другими важными вопросами. Я проводил уроки и параллельно проходил курс повышения квалификации. Они легко встраиваются в программу по предмету и полностью соответствуют ФГОС. Детям все это очень понравилось, особенно когда мы изучали тему, связанную с защитой банковских карт. Думаю, что они могли бы и самостоятельно это освоить, дистанционно на сайте. Но все-таки вместе с педагогом лучше, он всегда поможет. А чтобы изучать материал одному, нужна очень сильная мотивация.

– Уроки по информационной безопасности я провожу уже давно, – *делится впечатлениями Алексей Четверов, учитель информатики школы № 1409 Москвы.* – Когда я узнал о существовании курсов от «Киберпротекта», очень заинтересовался ими. В результате нашел для себя эффективный вариант проведения занятий, как и ответы на самые актуальные вопросы в ходе такого обучения.



На сегодняшний день востребованы квалифицированные педагоги, которые хорошо владеют информационными технологиями



И другие опрошенные мною педагоги пришли к общему мнению, что уроки, проводимые со школьниками в рамках курса, эффективны. Это действительно своего рода ликбез, дети обучаются основополагающим вопросам безопасности в Сети, с чем сталкиваются ежедневно.

На уроках по информационной безопасности подробно говорится о серьезных последствиях пренебрежения вопросами безопасности, и школьник начинает понимать, насколько это важно. А понять, осознать – это главное, так как человек сам начинает жестко контролировать свои действия в интернете. И «просто так», например, уже не станет выкладывать свои личные данные на всеобщее обозрение, понимая, какой опасности себя этим подвергает.

УМК «ПОД КЛЮЧ»

Большой плюс курса в том, что учителю предоставлен полный учебно-методический комплект для проведения этих уроков: рабочие тетради для учеников, необходимый тестовый материал, который проверяется автоматически, а также презентация, все в электронном виде.

В интересной интерактивной форме можно очень доходчиво рассказать детям о тех или иных аспектах информационной безопасности – избирательном, крайне осторожном использовании Wi-Fi-сетей, признаках фейковых страниц, кибербуллинге и т.п.

Заметим, что практическая часть создана на базе учебной платформы CoreApp – это полностью российская разработка. Ее достоинство в том, что, создав некий объем тестового материала для интерактивного урока, учитель может сохранить его в личном кабинете, а потом поделиться им с коллегами, которые также могут воспользоваться его разработками. Причем можно отследить результативность использования урока: сколько времени ученик потратил на тест, как на него отвечал, какие вопросы вызвали наибольшее затруднение и т.д.

– В процессе общения с детьми я выяснила, что многие из них сталкивались с такими проблемами, как хищение личных данных со страниц в социальных сетях, кибербуллинг, заражение компьютера вирусами, и прочими угрозами, – *рассказывает Надежда Грунина, педагог-психолог многопрофильного лицея села Малая Сердоба Малосердобинского района Пензенской области.* – Поэтому ребята весьма позитивно отнеслись к таким урокам. Материалы с сайта я использовала при проведении внеурочных занятий в рамках курса «Школа выживания: информационная безопасность». Там прекрасные методические разработки, много наглядного материала. Это важно, учитывая, что у современных детей развита в основном зрительная память. Хочу отметить, что «работа по станциям» – уникальная находка для педагогов, поскольку в процессе активной познавательной деятельности подросток не устает и не теряет интереса к уроку. Информация изложена доступным для понимания языком, тексты сопровождаются видеофрагментами, для закрепления нового материала предусмотрен короткий тест-опрос.

– Тема цифровой безопасности и гигиены важна не только в школе или вузе, но и в детском саду, – *убеждена Екатерина Ваколюк, дошкольный методист из Калининграда.* – Правда, это касается не столько самих детей, сколько администрации, бухгалтерии, педагогов и воспитателей, которые имеют доступ к интернету. И конечно же, это напрямую касается родителей наших ребят. Все мы периодически сталкиваемся с киберугрозами, защищаясь от них скорее инстинктивно. А надо действовать вполне обдуманно и осознанно, чему на курсах как раз и учат. Я адаптировала материал для коллег и родителей, провела с ними просветительскую работу, рассказав о том, как нужно оградить детей от возможных киберугроз, а также подготовила для них памятки и оформила информационный стенд в нашем дошкольном учреждении.

РЕКОМЕНДАЦИИ ЭКСПЕРТА

– Очень важно, чтобы цифровая грамотность стала естественной составляющей взаимодействия детей с цифровым миром, – *отмечает Яна Коваленко, директор проектов Центра цифрового развития АСИ.* – Это так же важно, как и обучать детей правилам дорожного движения: родители должны быть спокойны, когда их дети переходят дорогу самостоятельно. То же самое и в цифровой безопасности: ребенок должен самостоятельно обеспечивать свою безопасность. Рекомендую данный курс не только детям и педагогам, но и родителям, ведь цифровая среда в семье, как правило, единая, и всем в ней необходимо знать, как грамотно реагировать на действия киберхулиганов и, самое главное, как защитить и сохранить очень чувствительный актив – данные.

Вот практические советы Яны Коваленко как опытного специалиста, которые она дает родителям, педагогам и детям.

Надежные пароли. Используйте надежные и уникальные пароли (10–12 символов длиной, с заглавными, прописными буквами, цифрами и спецсимволами). Организуйте их безопасное хранение при помощи менеджера паролей. По возможности используйте двухфакторную или многофакторную аутентификацию.

Безопасные сайты. Посещайте безопасные сайты с расширением https или значком замка. Буква s и закрытый замок означают, что соединение защищено: когда вы вводите на сайте данные, они автоматически шифруются, соответственно, их не могут перехватить злоумышленники. Всегда проверяйте правильность написания адреса сайта: в нем не должно быть ошибок и лишних слов.

Иногда злоумышленники подделывают доменные имена, добавляя лишние слова к названию реально существующего сайта. Избегайте посещения сайтов с большим количеством всплывающих окон, орфографических ошибок или отличающихся по дизайну от оригинальных.

Публичный Wi-Fi – опасно! Не используйте публичный Wi-Fi для доступа к важным сервисам, особенно с целью осуществления финансовых операций. Всегда проверяйте правильность написания названия сети.

Антивирусные программы. Используйте их обязательно, регулярно обновляйте приложения и ОС.

Резервное копирование. Создавайте резервные копии важных файлов как в облаке, так и на внешнем жестком диске. Руководствуйтесь правилом 3–2–1: создавайте не менее трех копий, храните их в двух разных форматах, всегда храните минимум одну копию на физически удаленном носителе (например, в облаке).

Онлайн-покупки. Заведите отдельную карту для онлайн-покупок. Не храните на ней деньги. Пополняйте ее ровно на ту сумму, которая необходима для совершения покупки.



КУРСЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ ПОМОГУТ ПЕДАГОГАМ ПРОВОДИТЬ УРОКИ ПО ЭТОЙ ВАЖНОЙ ТЕМЕ, А ДЕТЯМ ДАДУТ ЗНАНИЯ.

Цифровой след. Сокращайте ваш цифровой след. Предоставляйте приложениям доступ только к тем данным, которые нужны для их работы. Удаляйте аккаунты, которыми не пользуетесь. Откажитесь от персонализированной рекламы.

Молчание – золото! А болтун – находка для мошенника. Не публикуйте свои персональные данные в интернете: адрес, паспортные данные, телефон и т.д. Никогда не сообщайте незнакомцам данные своей банковской карты, CVC-коды и коды подтверждения из СМС. Будьте бдительны: мошенники часто используют страх, эйфорию от легкого выигрыша и сострадание как эмоциональные крючки, чтобы получить доступ к личной информации или ресурсам.

Нулевая толерантность. Не терпите кибербуллинг! Если вас травят и оскорбляют в социальных сетях и мессенджерах, разглашают ваши личные секреты или персональные данные, присылают угрозы или преследуют вас навязчивым вниманием, то сразу заблокируйте обидчика.

Знания – сила! Помните, что главная угроза – отсутствие знаний. Узнайте больше о цифровой безопасности на сайте cyber-care.ru.

Вадим Мелешко