НЕДЕЛЯ БЕЗОПАСНОГО ИНТЕРНЕТА

НОВОЕ ПОКОЛЕНИЕ КОНТЕНТНЫХ УГРОЗ

Тема цифровой безопасности будет оставаться актуальной, пока существуют цифровые технологии – потому что любое устройство и любая технология, от топора до атомной энергии, может приносить как пользу, так и вред. По мере технологического прогресса в «цифровом мире» открываются новые возможности – и, как следствие, новые угрозы, подчас серьезно влияющие на наше восприятие действительности и на общественные максимы поведения.

В настоящее время технологии создания цифрового контента переживают очередную микрореволюцию, выводящую привычную нам цифровую реальность на новый уровень. «Локомотивами», или драйверами, этой микрореволюции являются биометрические технологии и искусственный интеллект. Биометрия рассматривается как более надежный способ идентификации, чем пароли или проверка через «привязанные» устройства, в связи с чем от нее ждут упрощения нашей жизни при доступе к информации, деньгам, пространству (например, на пограничном контроле). Искусственный интеллект, по замыслу разработчиков, должен научиться самостоятельно принимать решения – и этим дополнить труд специалиста. Всё это на практике переводится в программные приложения и комплексные технические решения, которые, по мере их развития, становятся доступными не только в неких специальных сферах, но и в том, что под силу каждому обычному пользователю.

Например, некоторые банки всерьез полагают, что биометрия успешно заменит банковские карты. Дескать, подошел человек к банкомату, тот сфотографировал лицо, сравнил его со своей базой данных (ну, может, еще отпечатки пальцев сверил) – и выдал деньги. То же самое в «умном» доме – вместо того чтобы искать ключ или пропуск, достаточно просто подойти к двери, и замок сверит отпечатки пальцев и лицо. В более глобальном масштабе некоторые убеждены, что системы распознавания лиц не оставят без внимания ни одного преступника. И так далее…

Однако всё это порождает и новый блок угроз, причем чем сложнее технология, тем труднее жертвам преодолевать ее последствия. Биометрические параметры – это очень специфичная форма идентификации и персональных данных, поскольку они, как правило, неизменны. Если взломанный пароль легко поменять на новый, можно изменить номер телефона, номер документа, даже место жительства, то отпечатки пальцев изменить практически невозможно, да и с лицом сложновато, пластическая операция – дело дорогое и небыстрое. Именно поэтому утечка или компрометация таких данных, можно сказать, фатальна для жертвы. А гарантировать стопроцентную безопасность их оборота или хранения, разумеется, нельзя. Как нельзя гарантировать и то, что эти технологии не будут использоваться во вред гражданам: предсказанный Оруэллом ужас тотальной слежки уже перестал быть фантастикой и успешно реализован в Китае.

Добавление к этому еще и возможностей искусственного интеллекта с его функцией машинного обучения привело, по сути, к новому лозунгу цифровой безопасности – «Не верь глазам своим». В мире цифрового контента безусловную веру в фотографии и сканы впервые поколебал «Фотошоп», и несмотря на обилие фальшивого статичного визуального контента, святая вера в незыблемость картинки еще сохраняется у некоторых пользователей. Затем компьютер научился имитировать голос. И только видео до недавнего

В статье использованы иллюстрации с сайта https://runet-id.com/event/csf19

У.У. ПАРФЕНТЬЕВ, координатор Центра безопасного Интернета, директор фонда «НеДопусти»

времени считалось несомненным «мерилом истинности» – если, конечно, нет явных следов монтажа. Теперь же стало возможным создавать и целиком фальшивые видео с внешностью и голосом реального человека, где он будет делать или говорить то, что захочет автор. Если на начальном этапе такая технология (ее называют deepfake – от понятий «глубокое машинное обучение» и «фальшивка») применялась из-за ее сложности разве что в богатом Голливуде, то сейчас она предсказуемо шагнула вниз – и некоторые соцсети предложили ее своим юзерам в качестве «забавного прикола». В итоге отвергнутому подростку теперь ничего не стоит сделать фальшивое интимное видео с внешностью своего объекта мечтаний – особенно если этот объект навыкладывал в соцсети кучу своих фото и видео. И доказать, что на видео на самом деле не она, а ее цифровая копия, жертва не сможет – ей просто не поверят. Ибо будет совпадать даже дикция – не говоря уже о внешности.

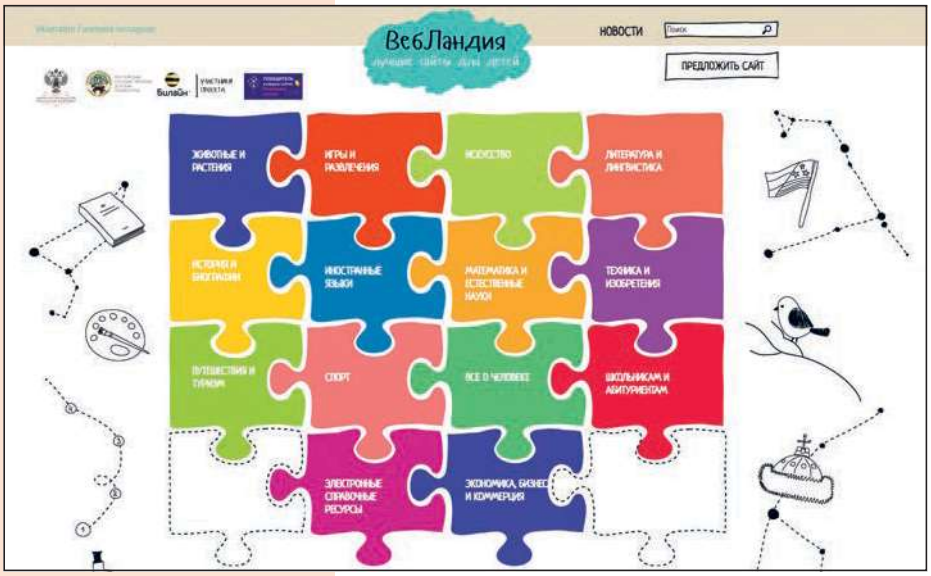
Если опасности неумеренного употребления биометрических идентификаторов предсказал Оруэлл, то проблемы с фальшивыми видео обрисовал Роберт Хайнлайн. В его повести 1940 года «Если это будет продолжаться» схожая технология «синтезированного персонажа» применяется ни много ни мало для совершения государственного переворота. Современные силовики считают, что такой сценарий из фантастической книжки уже перестал быть полностью фантастичным и может быть применен в пропаганде терроризма, организации массовых беспорядков, а уж «вечно живые» вожди террористических групп – это чуть ли не минимум из того вреда, что могут причинить злоумышленники.

Как давно известно, минимизация угроз начинается с профилактики и обучения потенциальных жертв – повышения их осведомленности об опасностях. Очевидно, что ведущаяся сейчас информационно-просветительская работа в сфере цифровой безопасности должна вслед за цифровым прогрессом выйти на новый уровень. Проще говоря, пользователи должны получать качественную информацию о возможности таких угроз, их формах и местах применения, а также о том, что им делать и как себя вести, чтобы избежать опасных для себя последствий.

Основные меры профилактики и защиты от нового поколения угроз эксперты озвучили на CyberSecurityForum – 2019, который завершил 12-ю Неделю безопасного Рунета. В первую очередь, пользователь должен помнить, что любой контент может быть недостоверным. В том числе и видео – хоть «новостной сюжет», хоть «бытовая съемка». Поэтому верить всему, что предстает на экране, явно опрометчиво. В связи с этим возрастает важность старого тезиса «Думай, что публикуешь»: обилие собственных фотографий и видео в соцсети теперь может легко сыграть против ищущего таким образом популярности персонажа. Так что лучше обойтись небольшим набором фотографий. Что же касается биометрии, то на данном этапе говорить об «автоматизированном принятии решений» пока рано, иначе в том же Китае «электронный мозг» не признал бы многократным нарушителем ПДД лицо из рекламы с бортов автобусов. Поэтому по возможности пользователям лучше обходиться старыми проверенными методами аутентификации и воздерживаться от «инновационных» предложений.

ИНТЕРНЕТ ДЛЯ ДЕТЕЙ: БЕЗОПАСНЫЙ, ПОЗНАВАТЕЛЬНЫЙ И РАЗВЛЕКАТЕЛЬНЫЙ

Вселенная Интернета продолжает расширяться. Количество цифрового контента многократно возрастает, и всё больше детей и подростков пользуется ресурсами Сети. При этом о многих позитивных и интересных ресурсах Интернета, как правило, не знают ни они, ни родители, ни специалисты. Чтобы ориентироваться в этом огромном информационном пространстве, где существует обилие негативной, некачественной информации, нужны информационные гиды – навигаторы. Но только грамотные специалисты могут отвести ребенка к лучшим сайтам, порекомендовать их, показать и рассказать о наиболее качественных, лучших ресурсах для детей и их наставников. Этими специалистами становятся библиотекари, работающие с детьми. Для решения этой задачи и возник, например, такой проект Российской государственной детской библиотеки, как «Вебландия. Лучшие сайты для детей».



Новая рубрика посвящена позитивному и безопасному детскому контенту. Она поможет всем нам объединить свои силы для того, чтобы развивать и продвигать именно разнообразный и позитивный цифровой контент для детей. Каждый специалист, который знает что-либо значимое и интересное о таком контенте, может прислать в журнал свои материалы, рассказать о своей практике создания и продвижения позитивного контента.

Адрес: socic@rbdb.ru

Но всё же, открывая эту рубрику, мы бы хотели, чтобы библиотекари и педагоги ориентировались на ресурсы для детей, а не на чисто педагогические ресурсы, подготовленные для сферы образования. Сегодня для этого контента уже созданы и создаются специальные платформы и сайты. Но очень важно решить другую задачу: развивать интересы детей, их стремление познавать мир, расширять горизонты. Сайты, которыми могут пользоваться дети (а также их родители и наставники), прежде всего, должны быть им интересны и понятны. Поскольку хороших, наиболее качественных сайтов для детей не так уж и много и часто они теряются в пространстве Интернета, важно не пропустить такой ресурс – например, сохранить его в «Вебландии».

Приглашаем всех желающих участвовать в отборе и продвижении лучшего контента для детей. Вы можете писать здесь о том, какие сайты нравятся лично вам, как вы их используете в работе с детьми и подростками, а также с родителями и другими воспитателями. Если у вас есть замечательные сайты, интернет-проекты развивающего характера, пишите об этом в новой рубрике, участвуйте в проекте «Вебландия». Вместе мы сможем сделать Интернет более светлым и гуманным для детей и взрослых!

Команда «Вебландии» ФГБУК «Российская государственная детская библиотека»:

Наталья Александровна Аракчеева – советник директора,

Евгения Анатольевна Армадерова – редактор сайта «Вебландия»,

Вера Петровна Чудинова – научный консультант проекта, кандидат педагогических наук