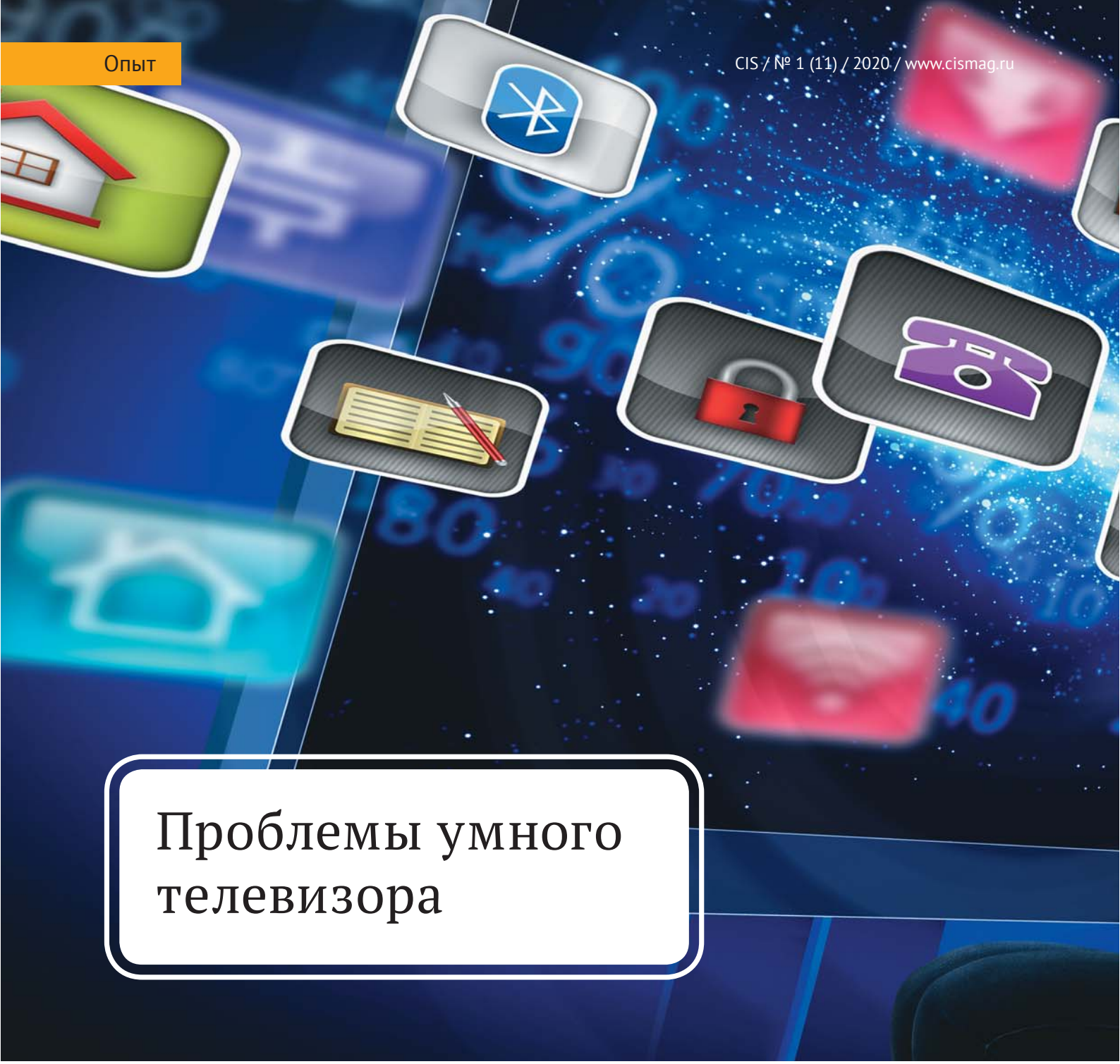
CIS / № 1 (11) / 2020 / www.cismag.ru



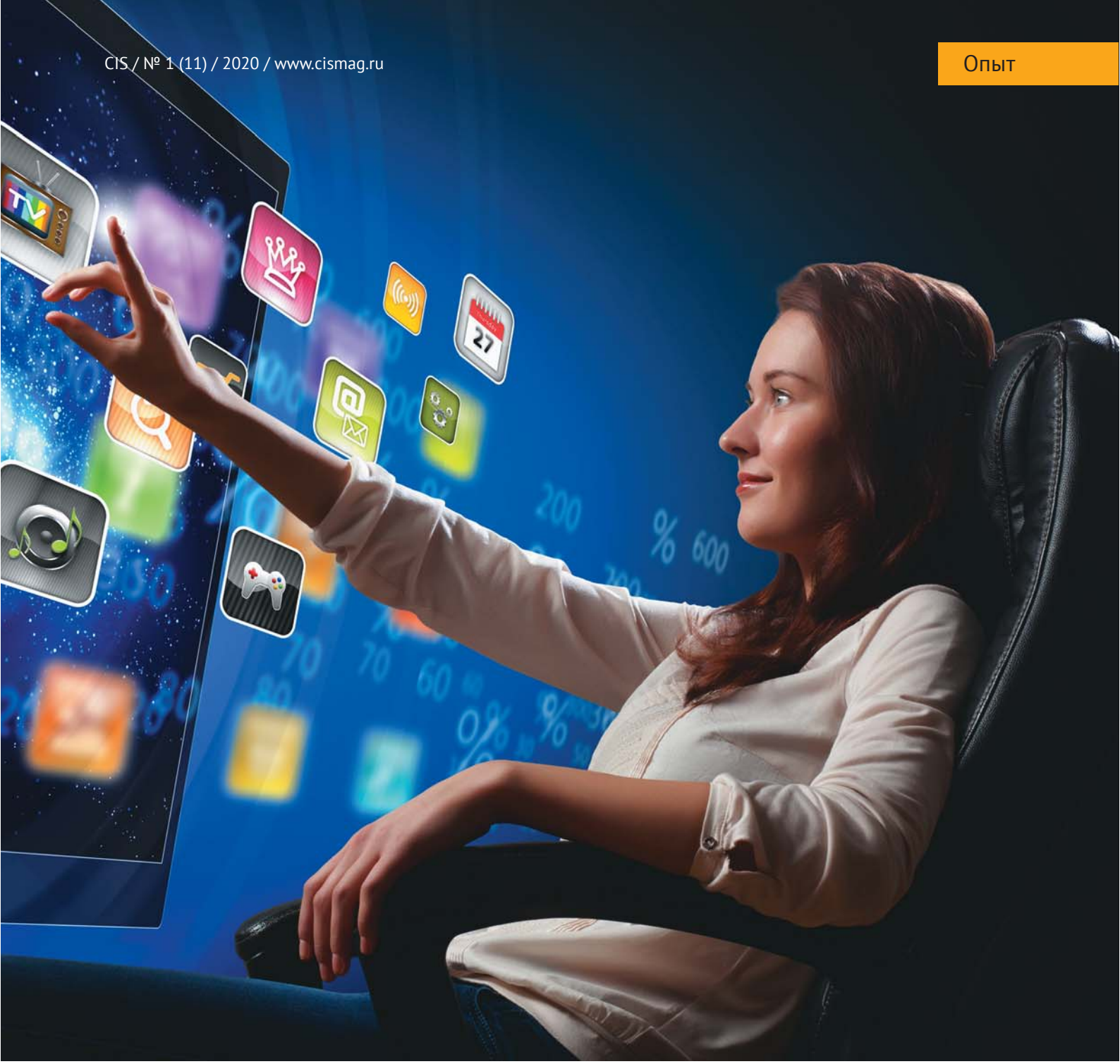
Проблемы умного телевизора

Весьма возможно, что вы используете умный телевизор. Тем более, что таких сегодня большинство. Однако проблема в том, что умный телевизор записывает ваши привычки: что вы смотрите, когда, а затем компания-разработчик монетизирует эти знания. Увы, проблема в том, что технологии производства сегодняшних телевизоров уже практически не развиваются, а, следовательно, ждать прорыва уже неоткуда.

Снижать бесконечно цены, чтобы победить конкурентов, уже тоже практически невозможно. А ведь прибыль получать хочется всем. И потому на помощь компаниям, выпускающим телевизоры, приходит идея очень тихо зарабатывать на своих покупателях, вернее, на их данных.

ACR: всё связано

Наверное, у нас с вами не было бы такой угрожающей ситуации, если бы не автоматическое распознавание контента (Automatic Content Recognition – ACR). Эта функция Smart TV использует всего несколько пикселей того изображения, которое вы просматриваете в данный момент. Затем эти сведения используются для показа рекламы как внутри вашего телевизора, так и на других ваших интернет-устройствах. Так как ваш смарт-телевизор, вероятно, связан с вашим домашним маршрутизатором, он использует тот же IP-адрес, который идентифицирует ваши конкретные домашние устройства. Этот общий адрес означает, что вы можете использовать рекламу, полученную с помощью вашего телевизионного устройства на все устройства, подключённые к домашней сети. Другими словами, та же реклама, которую вы видели на своём телевизоре Smart TV, может легко появиться на вашем смартфоне.



Возможно, это звучит особенно страшно, потому что телевидение предшествовало Интернету, и люди помнят время, когда просмотр телевизора казался скорее однонаправленным распространением информации. Но времена изменились, и сегодня телевизор уже не только даёт информацию, но и фильтрует её, чтобы вы получали направленную рекламу.

Почему данные ACR могут стать будущим телевизионных измерений

Данные ACR (автоматического распознавания контента) со смарт-телевизоров могут быть одним из самых революционных способов для сетей и рекламодателей измерить привычки просмотра. Это также одна из наименее изученных технологий в телевизионной экосистеме.

Настройка

Весь процесс ACR запускается, когда зритель впервые распаковывает свой телевизор. Когда вы его устанавливаете, появляется экран с вопросом, хотите ли вы поделиться тем, что смотрите. Очень часто этот вопрос формулируется в терминах: «Чтобы получить более точные рекомендации, вы позволите нам отслеживать то, что вы смотрите?» При этом вас не уведомляют о своих намерениях (например, о продаже данных маркетологам и фирмам, которые проводят измерения), но реальность такова, что независимо от того, насколько они искренни, большинство людей просто спешат настроить телевизор и потому на все вопросы просто отвечают «Да», не читая их (безусловно, хорошая новость заключается в том, что вы можете вернуться и изменить свои ответы, если у вас появятся подобные мысли). Но большинство людей, считает абсолютно нормальным, когда маркетологи знают, какие телевизионные шоу они смотрят.

После того как владелец телевизора дал разрешение и подключил

телевизор к Интернету, у него всё впереди: производитель смарт-телевизора может собирать эти данные и использовать их по своему усмотрению.

Сбор данных

На технологическом уровне данные ACR работают, потому что умные телевизоры (с вашего разрешения) захватывают несколько пикселей из того, что зритель в данный момент смотрит, и обмениваются ими с программным обеспечением отслеживания ACR производителя телевизора. Программное обеспечение берёт эти пиксели и сопоставляет их с базой данных, которая отслеживает локальные трансляции в любом регионе, в котором находится зритель. Посмотрев время, продолжительность рекламных пауз и какие рекламные ролики просматриваются, провайдер данных ACR может узнать несколько вещей:

1. Зритель смотрит линейный канал, OTT, DVR или VOD?
2. Какие шоу и рекламные ролики он смотрит каждую секунду.
3. Каков IP-адрес зрителя, что позволит ему узнать свой физический адрес и какие веб-сайты и приложения он посещает (все эти данные анонимны, например: фактические имена не прилагаются). Но прилагается IP-адрес.

Рынок

Зайдите в любой магазин: почти каждый телевизор, который вы увидите, будет умным или подключённым к Интернету. По оценкам, к 2020 году около 75% всех телевизоров, используемых в США, будут умными телевизорами.

Одно существенное изменение с момента запуска умных телевизоров заключается в том, что две компании – Samsung и VIZIO – стали доминировать на рынке. Несмотря на то, что нет конкретной статистики, по большинству оценок Samsung занимает около 40% рынка, а VIZIO – 30%. Такие игроки, как LG, Sony, Panasonic, Magnavox, Philips и тому подобное теперь занимают гораздо меньшую долю рынка, чем пятнадцать или двадцать лет назад. Новые игроки из Китая, такие как Huawei, являются восходящими, но, за исключением Samsung и VIZIO, никто не владеет более чем 10% рынка.

Samsung и VIZIO собирают данные со смарт-телевизоров, но в то время как Samsung использует эти данные только в своих целях (рекомендации и реклама на домашнем экране), VIZIO владеет компанией Inscape, которая продаёт необработанные данные для маркетологов, сетей и измерительных компаний. Другая компания – Samba TV объединяет несколько небольших OEM-производителей и предлагает агентствам возможность переориентировать потребителей.

Значение данных ACR

Данные ACR от умных телевизоров – единственный способ измерить уровень того, что смотрят люди. Это означает, что засчитано будет всё независимо от источника сигнала. Что, учитывая нынешнюю суету вокруг того, как именно измерить зрительскую аудиторию, кажется крайне необходимым для отрасли.

Представьте себе: идёт политическая реклама. Как посчитать хотя бы приблизительно, как будут голосовать? Довольно просто: зная, какую рекламу смотрят, а какую нет, верно?

Рекламодателям нравятся данные ACR, потому что они обеспечивают каждую секунду обратную связь, как работают их объявления. Nielsen предоставляет свои данные в 15-минутных блоках, поэтому, если зрители отключились после первого объявления в пакете, рекламодатель не сможет узнать об этом. А поскольку IP-адреса включены, такие компании, как iSpot.tv и Data + Math, могут использовать эту информацию для создания атрибутивных рейтингов, которые помогают рекламодателям понять, как определённые объявления и места размещения помогли зрителям пройти через воронку продаж от просмотра рекламы, чтобы погуглить продукт, чтобы фактически купить его. Это длительный процесс, который требует большого количества данных и строгости, но это отличный способ доказать маркетологам, что телевизионная реклама действительно работает.

Будущее измерения ACR

Ценность данных ACR будет продолжать расти: к 2021 году она должна превратиться в бизнес стоимостью 5 миллиардов долларов, поскольку сети и рекламодатели используют её, чтобы помочь определить, кто просматривает широкий спектр форматов и вариантов. Данные ACR не вытеснят данные Nielsen, а, скорее, дополнят их вместе с данными телевизионных приставок (от тех, кто всё ещё использует таковые). Взятые вместе, они должны дать нам гораздо лучшее понимание шаблонов просмотра, что, в свою очередь, позволит рекламодателям лучше ориентировать рекламу на определённую аудиторию в зависимости от того, когда, где и на каком устройстве они смотрят. Всё это должно помочь отрасли получить доступ к святому Граалю меньшего количества более целенаправленной рекламы, за которую бренды будут платить больше денег.

На подключённом к Интернету Smart TV этот собранный контент не ограничивается цифровой информацией из передач, которые вы транслируете через интернет-сервисы, такие как Netflix, но также может включать пиксельные подписи с обычного кабельного телевидения и DVD-дисков. И эта информация может передаваться с вашего телевизора компаниям каждые несколько секунд [1].

Опасения по поводу наблюдения

Сегодня даже ФБР озабочено данной проблемой и предостерегает пользователей о необходимости защищать свои умные телевизоры [2]. Однако, как выясняется, текущая бизнес-модель добычи данных, которую используют многие технологические компании, также порадует государственные силовые структуры.

Вместе с тем необходимо учесть, что сегодня, как в ноутбуках и смартфонах, в некоторых смарт-телевизорах есть микрофоны и камеры, хотя, как сообщается, в новых моделях камеры стали меньше [3]. Фактически эти камеры и микрофоны – всё та же проблема «подслушки-подглядки». Это превращает телевизоры в универсальные подслушивающие-подглядывающие устройства. И хотя правоохранительные органы будут предостерегать вас от атак злоумышленников, кто мешает самим правоохранителям вторгаться в вашу личную жизнь? Ведь наблюдение возможно даже тогда, ког-

да вам кажется, что ваш телевизор выключен [4].

Угрозы Smart TV

Вместе со сбором рекламных данных смарт-телевизоры представляют и другие проблемы безопасности, такие как возможность атак злоумышленников для проникновения в домашние настройки Wi-Fi и проникновения на другие устройства в вашей сети. Ведь вполне вероятно, что даже если ваш компьютер хорошо защищён, то незащищённый телевизор может дать возможность проникновения в маршрутизатор или сеть [2].

Несмотря на то, что ФБР напрямую не предупреждает о ботнет, следует отметить, что Internet of Things (IoT), такие как смарт-телевизоры, являются популярными объектами для атак. Тем более, что телевизор служит своему хозяину не год и не два. А обновления к его прошивке практически не выпускаются.

«Многие кибератаки, такие как вредоносное ПО Mirai и атаки Dyn, заражают сеть компьютеров, включая интеллектуальные устройства, такие как бытовые приборы, камеры видеонаблюдения, радионяни, системы кондиционирования / обогрева, телевизоры и т. д., и превращают их все в скомпрометированные серверы, – пишет Алан Грау, вице-президент IoT по встраиваемым решениям в Sectigo [6]. – Эти скомпрометированные серверы затем действуют как узлы в атаке и вместе создают ботнет. Они могут участвовать в различных скоординированных атаках, заражать другие устройства и расширять сеть ботов или участвовать в атаках типа «отказ в обслуживании».

ФБР предупредило о потенциальном риске того, что Smart TV может слушать вас и наблюдать за вами, отметив, что новые телевизоры со встроенными камерами позволяют вести видеочаты. Кроме того, некоторые модели имеют функцию распознавания лиц, «поэтому телевизор знает, кто смотрит, и может предложить соответствующие программы», – говорится в уведомлении, что также может привести к проблемам с конфиденциальностью.

Увы, это не теория. Недавно исследователи обнаружили, что умные телевизоры от Samsung, LG и других компаний отправляют конфиденциальные пользовательские данные в технологические фирмы-партнёры, даже когда устройства не работают [7].

На сегодняшний день уже обнаружены несколько уязвимостей в смарт-телевизорах. А производители Smart TV, как и многих других устройств IoT, не следуют принципам обеспечения безопасности.

По словам ФБР, чтобы защитить себя от всех этих угроз, потребители должны изменить стандартные настройки и пароли безопасности интеллектуальных телевизоров и знать, как отключить микрофоны, камеры и сбор личной информации, если это возможно. Кроме того, необходимо регулярно проверять наличие обновлений программного обеспечения от производителей.

Наши устройства стали умными (возможно, слишком умными), но это не значит, что вы должны быть «тупыми» в том, как их использовать. В следующий раз, когда вы настроите новое интеллектуальное устройство, обязательно подумайте о его возможностях и о том, что можете сделать, чтобы защитить свою конфиденциальность.

Как вы можете защитить свой умный телевизор?

В 2018 году по всему миру было продано 114 миллионов умных телевизоров [5]. В Соединённых Штатах около 45% домов имели хотя бы один умный телевизор. И одна из причин, по которой умные телевизоры стали такими доступными, заключается в том, что возможности отслеживания помогают удерживать цены. Поскольку умные телевизоры и другие интеллектуальные устройства становятся всё более привлекательными для покупки, важно, чтобы рядовой пользователь знал, как ограничить сбор данных на своих машинах.

4. Будьте осторожны при настройке телевизора. Не соглашайтесь автоматически на все условия, чтобы не упустить возможность отказаться от сбора данных. Если вы читаете это до того, как начнёте работать с новым умным телевизором, то подумайте, что вам по вкусу, потому что производители усложняют поиск и отказ от своих функций сбора контента после того, как вы уже согласились с ними. Способ изменения настроек варьируется для каждого телевизора, поэтому вам нужно будет найти спецификации для вашей собственной модели.
5. Вы можете просто выбрать «тупой» вариант и не подключать свой умный телевизор онлайн. Затем вы можете, например, запустить любимый потоковый сервис со своего ноутбука и подключить его к порту HDMI телевизора. Конечно, вы всё равно будете подвергаться врождённому отслеживанию, которое происходит в потоковом сервисе, который используете, но несколько ограничите его распространение.

Если хотите, чтобы телевизор работал в режиме реального времени, вам может помочь VPN. Защита вашего домашнего маршрутизатора с помощью VPN – это отличный способ зашифровать соединение, которое защитит вас от хакеров и повысит анонимность в сети. Вместе с тем нужно помнить, что от «подслушки-подглядки» это не защитит! Безусловно, это усложнит анализ, но не сильно. Да и практически все крупные компании с сервисами ведут у себя логи. Кроме того, стоит помнить, что в ряде стран есть только «доверенные» VPN, которые сдали ключи соответствующим ведомствам.

Поскольку телевизоры относятся к устройствам IoT, они обновляются редко или вообще не получают обновлений. А значит, на сетевом уровне их нужно выделять в отдельную подсеть и отделять от компьютеров. В условиях организации – обязательно, в домашних условиях – желательно. Между подсетями должен быть разрешён только одобренный трафик. Либо подключать телевизор и компьютеры к разным роутерам. Это вполне реально, например: у меня дома есть подключения к двум интернет-провайдерам и установлены два роутера. Далее на телевизорах под управлением Ос Android можно рекомендовать установку специализированных антивирусов, например Eset Smart TV Security.

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам информационной безопасности