



Имеем право!

Приложение к Вестнику
Уполномоченного по правам человека
в Ярославской области



ВАЖНО ЗНАТЬ

Данные статистики подтверждают: в 2020 году в России наблюдался значительный рост активности кибермошенников, ошутимо возросло число кибератак на информационные ресурсы и базы данных физических лиц. Подобное оказалось возможным в условиях перевода большого числа сотрудников на удаленную

Что такое «право на цифровую безопасность»?



Разъясняет Сергей БАБУРКИН

Перевод значительной части социальных контактов в цифровую среду, рост популярности интернет-услуг и онлайн-платежей закономерно ставят вопрос о цифровой безопасности граждан. Проблема защищенности человека и его устройств в цифровом пространстве сохраняет высокую степень актуальности уже не первый год, однако именно в период пандемии уязвимость пользователей сети Интернет возросла в разы.

последствия потери данных медицинских карт в лечебных учреждениях. На все вопросы прозвучали разъяснения в прямом эфире. В завершение эфира были даны рекомендации по безопасному использованию гаджетов, девайсов и цифровых сервисов.



Делимся некоторыми советами с читателями «СК ЯР»:

- Не устанавливайте потенциально вредоносное программное обеспечение: например, нелегальные версии операционной системы, программы из неофициальных магазинов приложений.
- Не вводите пароли к ресурсам организации, если не установлено защищенное соединение по HTTPS. Убедитесь перед вводом пароля, что в начале адреса сайта стоит https://
- Используйте сложные пароли. Рекомендуется включать в пароли цифры, большие и малые буквы алфавита и знаки препинания. По возможности стоит также добавить специальные символы. Для хранения и генерации паролей стоит использовать менеджеры паролей.
- Не используйте один пароль на всех ресурсах. Используйте генератор паролей для создания и хранения уникальных паролей для каждого сайта.
- Не стоит вводить пароли вручную в публичных местах, где их могут подсмотреть или тем более записать на камеру.
- Не сообщайте данные своих банковских карт, пароли, логины и ключи от личных кабинетов третьим лицам. Помните, что сотрудники банков не выясняют подобные данные по телефону или СМС!

работу, ограничений режима функционирования торговых и иных объектов, переориентации торговой деятельности на дистанционное взаимодействие с потребителями.

Сергей БАБУРКИН:

Зачастую мошенники стремятся завладеть денежными средствами граждан через фишинговые сайты и поддельные страницы оплаты на сайтах интернет-магазинов, используя вредоносные программы и вирусы, а также опираясь на методы социальной инженерии. К сожалению, нередко от действий злоумышленников страдают пожилые люди. Не менее острыми являются проблемы утечек персональных данных, онлайн-слежки, неправомерного доступа к личным кабинетам и аккаунтам в социальных сетях, разглашения личной информации в интернете, травли и клеветы в социальных сетях».

Такая ситуация вводит в нашу повседневную жизнь новые понятия – «цифровая безопасность» и «право на цифровую безопасность». Что это такое?

Сергей БАБУРКИН:

Под цифровой безопасностью справедливо понимать комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от внешнего несанкционированного воздействия, вирусных и хакерских атак, иных информационных угроз и рисков. Кроме того, это информационная безопасность гражданина, предполагающая сохранность его данных при их использовании и передаче в цифровую среду. В подобном контексте право на цифровую безопасность – это право на защиту информации в цифровом пространстве, возможность доступа человека к цифровой информации, конфиденциальность данных в цифровой среде. Вопросы цифровой безопасности человека не получили в настоящее время комплексного правового регулирования в рамках единого нормативного правового акта, однако отразно отметить, что с каждым годом российское государство уделяет все большее внимание этим вопросам».

Тема обеспечения права жителей Ярославской области на цифровую безопасность обсуждалась в прямом эфире авторской программы Уполномоченного «Имеем право!» на «Радио России. Ярославль». Гости Сергея Бабуркина стали Снежана Симонова, кандидат юридических наук, руководитель Клуба цифрового права «DigitalFemida», и Александр Фролов, кандидат политических наук, руководитель проекта «Цифровая безопасность».

Омбудсмен и приглашенные эксперты рассказали об основных угрозах цифровой безопасности и рисках, которые важно учитывать

при использовании смартфонов, интернет-ресурсов и социальных сетей. Эксперты осветили правила поведения в цифровой среде, а также меры ответственности за противоправные деяния. Особое внимание Уполномоченный и гости уделили разъяснению правового режима персональных данных в сети Интернет.

Радиослушатели традиционно проявляли активность: их интересовали вопросы ответственности за преступные операции с банковскими картами, проблема избыточного сбора персональных данных для получения банковских и социальных услуг, а также



→ Записаться на личный дистанционный прием к Сергею Бабуркину можно по телефону (4852) 78-60-32

→ Обратиться за защитой прав к Уполномоченному по правам человека в Ярославской области можно круглосуточно через интернет-приемную на сайте www.up76.ru и по электронной почте upch@yarregion.ru

→ Получить консультацию омбудсмена можно на официальных страницах Уполномоченного в социальных сетях в Фейсбук и ВКонтакте

→ Приглашаем присоединиться к числу подписчиков Уполномоченного в социальной сети Instagram. Название страницы – [ombudsman76](https://www.instagram.com/ombudsman76)

СЕВЕРНЫЙ КРАЙ №42 | 267031 | 28 октября 2020 г.