Институт развития интернета

Еженедельный правовой дайджест

Интернет и информационные технологии

Выпуск № 133

24.02.2023

Москва 2023

Оглавление

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Раздел 1. Законы и законопроекты

Об административной ответственности в сфере измерения аудитории и социальной рекламы в сети «Интернет»

Подписан Федеральный закон от 17 февраля 2023 года № 32-ФЗ«О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (законопроект № 228934-8).

За неустановку ПО, предназначенного для исследования аудитории Интернет-ресурсов, а также за непредоставление необходимых для такого исследования данных уполномоченной организации вводится административный штраф в размере до 30 тысяч рублей для граждан, до 100 тысяч – для должностных лиц и до 500 тысяч – для юридических лиц.

Также за неисполнение обязанностей по распространению социальной рекламы в сети «Интернет» вводится административный штраф аналогичного размера.

Закон вступил в силу 17 февраля 2023 года.

Раздел 2. Акты и проекты актов Правительства

Об интеграции классифайдов с ЕСИА

Минцифры России опубликовало проект постановления Правительства Российской Федерации «О случае и правилах интеграции и взаимодействия сервиса размещения объявлений с федеральной государственной информационной системой «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие

информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» и федеральной государственной информационной системой «Единый портал государственных и муниципальных услуг (функций)»».

Интеграция сервиса размещения объявлений (классифайда) с единой системой идентификации и аутентификации (ЕСИА) и единым порталом государственных и муниципальных услуг (ЕПГУ) может быть осуществлена при одновременном соблюдении следующих условий:

- сервис включён в реестр Роскомнадзора;
- отсутствует решение о ликвидации (прекращении деятельности) владельца сервиса;
- отсутствует решение о признании владельца сервиса банкротом;
- отсутствует решение об административном приостановлении деятельности владельца сервиса;
- владелец сервиса не привлекался к уголовной или административной ответственности за нарушение законодательства о персональных данных в течение двух лет;
- на ресурсе сервиса размещены реквизиты и контактные данные его владельца, а также политика обработки персональных данных;
- сервис зарегистрирован в регистре информационных систем ЕСИА.

Классифайд сможет использовать ЕСИА для идентификации и аутентификации пользователей, а также для сведений о пользователе из ЕСИА владельцу классифайда (при согласии пользователя).

ЕПГУ сможет использоваться классифайдом для:

- передачи на ЕПГУ сведений о купле-продаже, мене и (или) передаче в пользование имущества, выполнении работ, оказании услуг, поиске подходящей работы и (или) подборе необходимых работников, которые могут быть

использованы при формировании заявлений на оказание государственных услуг, а также для формирования и отправки посредством ЕПГУ заявлений на предоставление государственных, муниципальных и иных услуг;

- направления в классифайд информации о поступлении в подсистему единого личного кабинета уведомлений, судебных извещений и иных документов.

Раздел 3. Ведомственные акты и проекты ведомственных актов

О взаимодействии с системой ГосСОПКА в случае утечек персональных данных

Минюст России зарегистрировал приказ ФСБ России от 13 февраля 2023 года № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

Взаимодействие операторов персональных данных с системой ГосСОПКА, включая информирование ФСБ России об утечках персональных данных, осуществляется через Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

Информация об инцидентах направляется операторами в НКЦКИ в течение 24 часов с момента их обнаружения:

- с использованием каналов информационного взаимодействия, в том числе посредством электронной почтовой связи и технической инфраструктуры НКЦКИ – для субъектов критической информационной инфраструктуры;
- путем заполнения уведомления на официальном сайте Роскомнадзора –

для иных операторов.

НКЦКИ будет присваивать идентификаторы инцидентам, сведения о которых переданы операторами.

НКЦКИ также сможет запрашивать у операторов проведение проверки сведений о компьютерном инциденте при необходимости.

Раздел 4. Практические кейсы

О детской электронной почте

Минцифры России запустило сервис электронной почты, предназначенной для детей.

Такую почту можно зарегистрировать в процессе создания детской учётной записи на едином портале государственных и муниципальных услуг.

Детская почта обеспечит следующих функционал:

- автоматическая блокировка спама, рекламы и нежелательного контента;
- вход по смс, ребёнку не придётся запоминать пароль;
- проверка входящих. Все письма от новых отправителей, если их ещё не добавили в «белый список», сначала попадают в папку «На проверку», которую видит только родитель. Если родитель их одобрит, письма увидит ребёнок.

О постановлении Государственной Думы

Государственная Дума приняла постановление № 297029-8 «Об информации Министра цифрового развития, связи и массовых коммуникаций Российской Федерации М.И. Шадаева о ходе цифровой трансформации и обеспечения информационной безопасности Российской Федерации».

Правительству Российской Федерации в числе прочего рекомендовано:

- предоставить Роскомнадзору возможность оперативных проверок утечек

персональных данных;

- разработать и внести в Государственную Думу поправки, предусматривающие административную и уголовную ответственность за нарушения в сфере персональных данных;
- обеспечить развитие отечественного программного и аппаратного обеспечения.

Минцифры России рекомендовано в том числе:

- совместно с Государственной Думой проработать вопрос о запрете удаленной работы для граждан – ИТ-специалистов, выехавших за пределы Российской Федерации после начала специальной военной операции, связанной с разработкой, внедрением и администрированием государственных информационных систем, информационных систем объектов критической информационной инфраструктуры, а также с оборотом персональных данных;
- рассмотреть вопрос о подготовке проекта федерального закона, предусматривающего компенсацию вреда физическим лицам со стороны операторов персональных данных, допустивших утечку персональных данных, в том числе в досудебном (добровольном) порядке;
- принять меры по гармонизации государственных информационных систем, устранению их технологической разобщенности и взаимного дублирования;
- осуществлять комплексную подготовку кадров в ИТ-сфере в среднесрочной и долгосрочной перспективах в масштабах страны;
- проработать вопрос о включении школьных учителей информатики и ИТ-специалистов высших учебных заведений в перечень получателей мер государственной поддержки и иных преференций, предусмотренных для сотрудников аккредитованных ИТ-компаний;
- активизировать работу по сохранению и защите ценностей традиционной семьи в распространяемом в цифровой среде контенте;

- активизировать усилия по поддержке и развитию игровой ИТ-индустрии, уделив особое внимание патриотическому и просветительскому контенту;
- проработать возможность разработки и введения в эксплуатацию национальной сети доставки контента (CDN) при участии ИТ-компаний и координации данной сферы со стороны Министерства
- рассмотреть вопрос о разработке и запуске национального VPN-сервиса для доступа соотечественников и иных лиц к российским ресурсам сети «Интернет», заблокированным за пределами Российской Федерации.

ЗАРУБЕЖНЫЕ СТРАНЫ

Раздел 1. Зарубежное нормотворчество

О противодействии алгоритмической дискриминации в США

Президент США подписал исполнительный указ, который среди прочего предусматривает противодействие и устранение алгоритмической дискриминации, которые должны будут обеспечить исполнительные департаменты и агентства.

Под алгоритмической дискриминацией в указе понимаются случаи, когда автоматизированные системы способствуют неоправданному различному обращению или оказывают неблагоприятное воздействие на людей на основе их фактической или предполагаемой расы, цвета кожи, этнической принадлежности, пола, религии, возраста, национального происхождения, ограниченного владения английским языком, инвалидности, статуса ветерана, генетической информации или любой другой классификации, защищенной законом.

Для реализации противодействия дискриминации в государственных ведомствах будут организованы специальные подразделения – команды равенства (Equity Teams).

О датском руководстве по файлам cookie

Датский орган по защите данных (Datatilsynet) опубликовал руководство по стене файлов cookie (cookie wall).

Datatilsynet установил четыре критерия, предъявляемые к стене cookie:

1) Разумная альтернатива. Компании должны предлагать посетителям, которые не хотят давать согласие на обработку своих персональных данных, разумную альтернативу. Разумная альтернатива подразумевает, что контент или услуга, предлагаемая компанией, должны быть в значительной степени схожими, независимо от того, дает ли посетитель согласие на обработку своих персональных данных или, например, платит за доступ к контенту или услуге. Если альтернативная услуга значительно отличается от услуги, которую компания предлагает с согласия посетителя, согласие не будет считаться добровольным, по мнению Управления по защите данных Дании. Это может быть, например, случай, когда посетители получают доступ к значительно большему количеству контента, оплатив его, чем посетители, которые дают свое согласие на сбор файлов cookie.

2) Разумная цена. Компании не должны устанавливать неоправданно высокую цену за альтернативу оплаты. Таким образом, компаниям не запрещено предлагать доступ за плату в качестве альтернативы согласию посетителей. Однако цена этой альтернативы не должна быть настолько высока, чтобы на практике свобода выбора посетителей оказывалась иллюзорной.

3) Сбор данных ограничен только тем, что необходимо. Когда компании предлагают выбор между оплатой или согласием на сбор персональных данных в отношении доступа к контенту или услугам компании, компании должны быть в состоянии продемонстрировать, что все цели, для которых компания запрашивает согласие, являются необходимой частью этой альтернативы.

4) Обработка персональных данных при оплате посетителями. В случаях,

когда посетители платят за доступ к контенту или услуге, компания может обрабатывать информацию, необходимую для предоставления контента или услуги. При этом запрещается обработка персональных данных для большего числа целей, чем это необходимо для предоставления соответствующей услуги. Это может быть, например, персонализация или маркетинг.

Раздел 2. Зарубежные практические кейсы

Об аудите рабочих смартфонов сотрудников Минобороны США

Управление Генерального инспектора Минобороны США провело аудит использования приложений на смартфонах сотрудников Пентагона и Министерства обороны США.

Регулятор обнаружил на рабочих защищённых и проверенных перед выдачей в эксплуатацию смартфонах большое количество запрещённых к установке мобильных приложений сторонних разработчиков.

Эксперты в ходе аудита выяснили, что многие из установленных несанкционированных приложений требовали доступ к камере, микрофону, данным GPS, файлам, контактам, а также отсылали техническую информацию об устройстве пользователя разработчикам.

На служебных смартфонах были обнаружены развлекательные приложения (включая видеостриминг), приложения для онлайн-знакомств, бронирования недвижимости и ресторанов, игры, в том числе детские и многопользовательские, криптокошельки, приложения для покупок, включая онлайн-аукционы, потребительские бонусные программы и приложения для аренды роскошных яхт и другие.

По мнению главного инспектора использование сторонних мобильных приложений на мобильных устройствах для ведения служебной деятельности

создаёт большие операционные риски и проблемы кибербезопасности, а также может привести к тому, что пользователи непреднамеренно раскроют конфиденциальную информацию Минобороны разработчикам других стран или совершат внедрение вредоносных программ в информационные системы госведомства.

Об иске к Facebook в Великобритании

Апелляционный суд по вопросам конкуренции Великобритании вынес решение по коллективному иску к компании Meta Platforms, Inc. (*запрещена в России*).

Истцы обвиняли компанию в нечестном сборе данных пользователей соцсети Facebook, поскольку компания не платила пользователям за сбор и использование данных, при этом получая значительную прибыль в результате таргетинга рекламы.

Кроме того, по мнению истцов условия сбора данных Facebook сложные, непрозрачные, вводящие в заблуждение и не предполагают изменения, что можно квалифицировать как недобросовестные торговые условия.

Суд не нашёл оснований для удовлетворения иска, указав, что убытки пользователей должным образом не доказаны. При этом суд дал 6 месяцев на предоставление дополнительного экономического анализа.

О запрете TikTok на устройствах сотрудников Европейской комиссии

Европейская комиссия запретила TikTok на корпоративных устройствах, ссылаясь на проблемы с защитой данных.

В электронном письме, направленном чиновникам ЕС, сотрудников также попросили удалить TikTok с личных устройств, использующих корпоративные приложения, чтобы защитить данные Комиссии.

У сотрудников есть время до 15 марта, чтобы выполнить это требование.

О встроенных камерах в Tesla

Нидерландский орган по защите данных (Autoriteit Persoonsgegevens) заявил, что не будет штрафовать компанию Tesla за возможные нарушения, связанные со встроенными камерами безопасности ее автомобилей.

По результатам проведенного регулятором расследования, Tesla изменила функцию Sentry Mode, чтобы запись велась только при разрешении пользователя, и сократила время хранения изображений.

Регулятор также отметил, что в ходе расследования было установлено, что ответственность за изображения, записанные автомобилями, несут владельцы автомобилей, а не Tesla.

О необоснованно обработке данных о путешествиях пассажиров в Нидерландах

Нидерландский орган по защите данных (Autoriteit Persoonsgegevens, AP) приказал Министерству юстиции и безопасности немедленно прекратить крупномасштабную обработку данных о путешествиях пассажиров авиакомпаний (PNR, Passenger Name Records).

Регулятор установил, что необходимость и пропорциональность такой обработки является необоснованной.

Хотя данные о поездках всех авиапассажиров предназначались для получения информации о передвижении террористов и серьезных преступников, теперь они собираются и хранятся в базе данных в течение многих лет.

Отмечается, что большое количество персональных данных систематически собирается, автоматически обрабатывается и хранится у очень многих людей, которые не принадлежат к группе, для которой, собственно, и предназначена база данных.

АР потребовало от министра юстиции и безопасности сообщить в течение 14 дней, какие действия были или будут предприняты министерством.

ИССЛЕДОВАНИЯ, ЭКСПЕРТНЫЕ МНЕНИЯ, ПОЗИЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНИЗАЦИЙ

О российском ИТ-секторе

«СПАРК-Интерфакс» опубликовал исследование динамики российского сектора информационных технологий.

По оценкам экспертов в 2022 году ИТ-сектор заметно превосходил национальную экономику по динамике оборота (на 14 процентных пунктов) и регистрации новых МСП (на 17 процентных пунктов).

Однако ряд итоговых данных за 2022 год обнаруживает, что сектор ИТ все же уступал по таким показателям, как финансовый результат (прибыли минус убытки), конкурсные производства, инвестиции в основной капитал.

Так, за три квартала 2022 года инвестиции ИТ-компаний упали на 12% на фоне их увеличения в России почти на 8%. Финансовый результат сократился соответственно на 16% и 8% в январе-октябре 2022 года. Количество конкурсных производств выросло на 4% в 2022 году при общем падении их числа на 6%.

Одним из последствий беспрецедентного санкционного давления стало снижение рентабельности бизнеса по сравнению с 2021 годом при сохранении общей прибыльности российской экономики.

Как показывают оценки, сделанные на основе данных Росстата, в 3 квартал 2022 года средняя рентабельность активов упала на 7 процентных пунктов по сравнению с 3 кварталом 2021 года. Тем не менее даже в этих условиях ИТ-сектор сумел выйти на позитивную динамику.

Об атаках на российские компании и онлайн-ресурсы

Компания «Ростелеком-Солар» опубликовала Отчет об атаках на онлайн-ресурсы российских компаний за 2022 год и Отчет о кибератаках на российские компании в 2022 году.

По оценкам экспертов:

- самая мощная DDoS-атака в 2022 году составила 760 Гбит/с, что почти в 2 раза превышает аналогичный показатель 2021 года;
- самый продолжительный DDoS длился 2 000 часов, то есть почти 3 месяца;
- выявлено 21,5 миллиона веб-атак с высокой степенью критичности.

Эксперты пришли к следующим выводам:

- После начала СВО был зафиксирован очевидный всплеск атак на онлайн-ресурсы. Злоумышленники атаковали каналы связи и инфраструктуру как на сетевом и транспортном уровне;
- Была зафиксирована рекордная по мощности и продолжительности DDoS-атака. Однако в целом хакеры вели «ковровые бомбардировки» несложными и массовыми атаками. При атаках на веб злоумышленники продолжали эксплуатировать известные уязвимости и дыры в безопасности, многие из которых имеют высокую степень критичности и могут привести к полному контролю хакеров над приложением и краже данных пользователей.
- Конец года компенсировал резкий всплеск первых двух кварталов – злоумышленники сконцентрировались на целевых более сложных атаках на конкретные компании и отрасли. При этом уровень сетевых атак остается высоким и превышает средние показатели предыдущих лет, поэтому угроза остается актуальной.

Эксперты также отметили следующие тенденции:

- Вредоносное ПО остается бессменным лидером в инструментарии

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф
ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

киберпреступников. Однако волна фишинга с рассылкой вредоносов пришлась на III квартал года и в IV квартале уже пошла на спад;

- К концу года в топ вернулись веб-атаки, которые лидировали в I и II кварталах, но в III резко сократили свою долю почти до нуля. Также в отчетном периоде было обнаружено увеличение числа сетевых атак и инцидентов, связанных с компрометацией учетных записей;
- Сокращение доли инцидентов с высокой степенью критичности (с 7% в I полугодии до 2% во II) указывает на то, что компании за год значительно повысили уровень своей киберзащиты и смогли закрыть уязвимости, обнаруженные в начале года. Также многие организации успешно решили вопросы импортозамещения и проблемы с обновлением ПО после ухода зарубежных вендоров;
- В ближайшее время можно увидеть спад массовых атак хактивистов, связанных с СВО.
- Хаотичных ударов, которые наблюдались в начале 2022 года, скорее всего больше не будет. Но атаки продолжат усложняться и становиться более целевыми и продуманными.

Институт развития интернета

ири.рф