УПРАВЛЕНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОАО «РЖД»

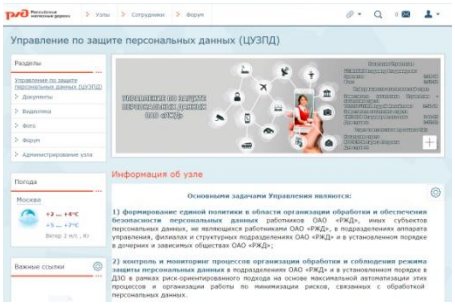
тематический обзор
материалов СМИ и блогосферы

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

№1 (23)

тел.: 8 (499) 262-61-09
danilinna@center.rzd.ru

ОГЛАВЛЕНИЕ



ССЫЛКА

на тематический узел Управления по защите персональных данных

(ресурс доступен исключительно из локальной сети ОАО «РЖД»)

ПРЯМАЯ РЕЧЬ

В.В. Путин, Президент Российской Федерации

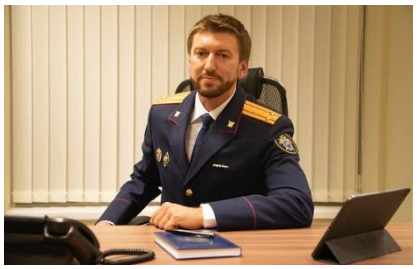
(в ходе видеоконференции с президентским советом по правам человека)

Как особо отметил Президент РФ Владимир Путин, «нельзя принимать такие фундаментальные решения и фундаментальные наши концептуальные документы в сфере искусственного интеллекта, в сфере цифровой экономики без решения проблем и без создания необходимой нормативной базы, связанной с обеспечением интересов и прав граждан в этой сфере». По словам Путина, он обязательно обратит внимание правительства на необходимость привлечения правозащитников к обсуждению вопроса защиты персональных данных россиян.

При этом Путин сослался на результаты недавних соцопросов, согласно которым граждан в наибольшей степени волнуют их права в сфере здравоохранения, в сфере образования, а на третьем месте по актуальности – как раз вопросы защиты личных данных и всего, что связано с личной жизнью, в том числе в цифровой сфере, «то есть это людей реально волнует». **(10/12/20, jpgazeta.ru)** К ОГЛАВЛЕНИЮ

ВЫБОР РЕДАКЦИИ

В СК НАЗВАЛИ ОСНОВНЫЕ ПРИЧИНЫ УТЕЧКИ ДАННЫХ РОССИЯН



15/01/21, banki.ru. Ошибки в работе сотрудников банков, различных ведомств и министерств являются основными причинами утечки баз данных россиян в Интернете. Об этом заявил руководитель отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий Следственного комитета РФ Константин Комарда в интервью ТАСС.

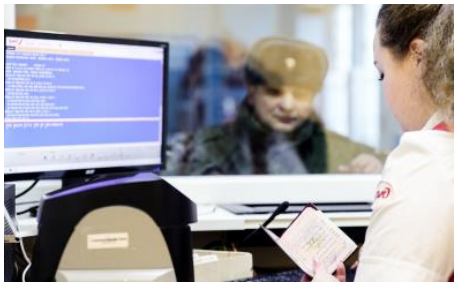
Он отметил, что вопрос утечки в даркнет сведений о паролях от личных кабинетов, данных банковских карт, информации о счетах и остатках денежных средств на них, паспортах, номерах мобильных телефонов стоит сейчас остро. «Низкий уровень компьютерной

грамотности населения является благоприятной средой для деятельности злоумышленников. Добавить к этому недостаточное принятие мер компаниями по защите от внутренних и внешних киберугроз, ошибки в работе сотрудников, производящих утечки информации либо умышленное хищение баз данных, — и сведения о миллионах наших граждан оказываются в глобальной Сети», — сказал Комарда.

Все слитые базы данных в основном продаются на специальных ресурсах в даркнете. «Это уже неоднократно продемонстрировали материалы наших расследований, когда слитые в Сеть персональные данные использовались для подготовки и совершения особо тяжких преступлений. Для решения этой проблемы нужен комплексный подход, в том числе на законодательном уровне», — сказал глава отдела, отметив, что Следственный комитет участвует в этой работе.

К ОГЛАВЛЕНИЮ

РЖД: ВЗЛОМАННЫЕ СИСТЕМЫ НЕ БЫЛИ СВЯЗАНЫ С ОСНОВНОЙ ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРОЙ ХОЛДИНГА



01/02/21, rzd-partner.ru. Защищенная технологическая сеть РЖД не пострадала в результате проникновения в отдельный сектор корпоративной сети, сообщили РЖД-Партнеру в пресс-службе ОАО «РЖД». Напомним, ранее в открытом источнике один из пользователей описал, как ему удалось построить несанкционированное соединение с сетью РЖД. По словам автора блога, в котором и появились детали взлома, обнаруженная уязвимость позволяла получить доступ к системе видеонаблюдения холдинга, IP-телефонии, сетевому оборудованию и другим сетям.

В пресс-службе холдинга подтвердили факт проникновения в систему, но подчеркнули, что это была сеть строящегося объекта одного обособленного подразделения холдинга «РЖД». «Речь идет об отдельной сетевой инфраструктуре филиала, находящейся в стадии формирования, не введенной в постоянную эксплуатацию и не связанной с технологической инфраструктурой РЖД», – пояснили в компании.

«РЖД непрерывно совершенствует собственную IT-инфраструктуру – одну из самых масштабных в России, тестирует и аудирует новые решения. Компания открыта и приветствует предложения по усовершенствованию собственной IT-инфраструктуры, при этом выступает против неправомерного доступа к информационным системам и публикации данных, связанных с информационной безопасностью, в открытых источниках», – добавили в пресс-службе. Представители ОАО «РЖД» также напомнили, что неправомерный доступ к компьютерной информации является уголовным правонарушением.

Отмечается, что компания провела мероприятия по выявлению и устранению уязвимостей строящейся сети с целью недопущения несанкционированного доступа. К ОГЛАВЛЕНИЮ

РЕГУЛИРОВАНИЕ. Российское регулирование

МИНЦИФРЫ ОПРЕДЕЛИЛО УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

03/12/20, comnews.ru. Спустя 14 лет с момента принятия федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных» Минцифры подготовило подзаконный акт об определении угроз безопасности персональных данных. Ведомство отмечает, что цель этого ведомственного приказа - установление единого подхода к определению угроз безопасности персональных данных. Эксперты считают, что это шаг в верном направлении.

Министерство цифрового развития, связи и массовых коммуникаций РФ разработало проект приказа «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности».

Проект приказа определяет актуальные угрозы безопасности персональных данных, а также устанавливает единый подход к определению угроз безопасности персональных данных, актуальных при их обработке в конкретных информационных системах (ИС),

и к разработке на их основе частных моделей угроз безопасности персональных данных для этих ИС.

Как отмечено в документе, адаптация актуальных угроз направлена на уточнение (уменьшение) перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в ИС, и осуществляется с учетом их структурно-функциональных характеристик, применяемых информационных технологий и особенностей функционирования (в том числе исключение угроз, которые непосредственно связаны с информационными технологиями, не используемыми в ИС, или структурно-функциональными характеристиками, не свойственными ИС). Принятие проекта приказа дополнительного финансирования из федерального бюджета не потребует.

В пресс-службе Минцифры рассказали, что принятие проекта приказа позволит установить единый подход к определению угроз безопасности персональных данных, актуальных при их обработке в конкретных информационных системах, эксплуатируемых в сферах, регулирование которых осуществляет Минцифры.

«После принятия ведомственного акта содержащийся в нем перечень угроз будет учитываться операторами при разработке частных моделей угроз безопасности персональных данных для конкретных информационных систем путем адаптации в ходе определения актуальных угроз безопасности персональных данных. Принятие соответствующего нормативного правового акта предусмотрено ч.5 ст.19 152-ФЗ от 27.07.2006 «О персональных данных» - в редакции от 25.07.2011 №261-ФЗ», - объяснили в пресс-службе Минцифры.

По словам представителя пресс-службы Минцифры, данный проект приказа разработан для актуализации изданного в 2010 г. Минкомсвязью документа, определяющего угрозы безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных отрасли. Тот приказ был согласован в установленном порядке с уполномоченными федеральными органами власти и одобрен решением Научно-технического совета Минкомсвязи России.

Директор по методологии и стандартизации Positive Technologies Дмитрий Кузнецов отметил, что нормативные документы в области ИБ позволяют операторам персональных данных самостоятельно определять, какие угрозы актуальны для обрабатываемых данных.

«Если защита от какой-то угрозы, например от APT-атаки (сложная целенаправленная атака), на систему со стороны серьезной хакерской группировки требует серьезных затрат, то у оператора есть возможность заявить, что он считает эту угрозу неактуальной. При этом у регуляторов нет правовых оснований по данному решению, что дает оператору возможность легально не выполнять свои обязанности по защите данных от таких угроз. Проект приказа призван такие правовые основания создать: в сферах деятельности, поднадзорных Минцифре, все классы угроз, указанные в приказе, априори считаются актуальными. К сожалению, это изменение затронет лишь отдельные сферы деятельности: связь, средства массовой информации, государственные услуги и т.п., поэтому какого-то серьезного влияния на ситуацию с защитой персональных данных в целом этот приказ оказать не может», - рассказал Дмитрий Кузнецов.

Директор департамента информационной безопасности компании Oberon Евгений Суханов подчеркнул, что документ подготовлен для определения модели угроз в информационных системах, за которые отвечает Минцифры РФ. По его словам, ранее использовалась «базовая модель угроз персональных данных в системах персональных данных», утвержденная ФСТЭК России от 15 февраля 2008 г. «Минцифры РФ продолжило обновление модели - это хорошая практика, поскольку угрозы меняются», - считает Евгений Суханов.

«Для формирования организационно-технических мер защиты персональных данных, да и вообще любой информации, традиционно создаются два документа - модель угроз и модель нарушителя. Актуализированная базовая модель нарушителя будет обновлена следующей. Когда законодательная база меняется вместе с развитием отрасли кибербезопасности - это всегда хорошо. Сложно выстраивать современные системы защиты информации, не имея актуальных регулирующих документов под рукой. На мой взгляд, данная инициатива Минцифры РФ поможет бизнесу выстраивать актуальные ИБ-системы с высоким уровнем защищенности от атак», - объяснил Евгений Суханов.

Руководитель отдела консалтинга департамента аудита и консалтинга Group-IB Андрей Алябьев напоминает, что, по данным ЦБ, в 2019 г. в даркнете обнаружено 13 тыс. объявлений о продаже и покупке персональных данных россиян. По мнению

Андрея Алябьева, организации, которые работают с личными сведениями, зачастую не способны предотвратить утечки: они экономят на средствах защиты и зарплатах сотрудников, что может побудить последних вступить в сговор со злоумышленниками. Чаще всего различные базы оказываются в открытом доступе именно по вине инсайдеров.

«Сфера обработки и хранения персональных данных нуждается в серьезных изменениях. Это комплексная задача, она не сводится исключительно к разработке новых документов с более строгими требованиями. И рассматриваемый проект нормативного акта не способен решить все проблемы. Необходимо создание механизмов и условий для реального соблюдения принципов приватности и безопасности данных со стороны всех игроков рынка. Например, нужно минимизировать объем собираемых данных и ограничить сроки их хранения. Граждане должны иметь возможность контролировать распространение своих персональных данных. Должна быть сформирована единая правоприменительная практика в случае выявления нарушений со стороны операторов. Усиление контроля и надзора за организациями может стать еще одним шагом на пути к цели. В вопросе определения актуальных угроз перспективно выглядит подход ФСТЭК, изложенный в проекте методики моделирования угроз. В соответствии с ним организациям предлагается выстраивать цепочки разных сценариев потенциальных атак, что позволит более эффективно им противодействовать на разных этапах реализации», - сообщает Андрей Алябьев.

Управляющий партнер юридической фирмы Axis Pravo Алексей Сулин подчеркивает, что в условиях, когда сбор персональных данных граждан и их обработка приобретают повсеместный характер, любые разумные меры, направленные на повышение безопасности хранения и обработки персональных данных, являются уместными. «Приказ Минцифры находится в общем векторе законодательного регулирования, основы которого заложены федеральным законом «О персональных данных». П.5 ст.19 данного закона возлагает на федеральные органы исполнительной власти обязанность по принятию нормативных актов в пределах своих полномочий, устанавливающих угрозы безопасности персональных данных. Подобный дифференцированный подход, в зависимости от степени

угрозы и вероятности утечки персональных данных, безусловно, следует считать конструктивным», - отмечает Алексей Сулин.

Владелец IT-legal компании «Катков и партнеры» Павел Катков считает, что проект данного приказа - шаг в верном направлении. «Чем более осознанным будет подход к угрозам безопасности в отношении персональных данных, чем более проработанным будет противодействие этим угрозам, тем, соответственно, выше шансы на успех. Думаю, можно ожидать, что этот приказ станет частью большой системы управления этими угрозами - во всяком случае, исходя из нашего опыта, это было бы правильно», - рассказал Павел Катков. К ОГЛАВЛЕНИЮ

РОССИЯ ВОШЛА В БЮРО КОМИТЕТА СОВЕТА ЕВРОПЫ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ

16/12/20, crn.ru. Минцифры России будет представлять интересы Российской Федерации в Бюро Комитета Конвенции Совета Европы № 108 о защите физических лиц при автоматизированной обработке персональных данных. Комитет является основным рабочим органом Конвенции — глобального международного договора в сфере защиты персональных данных, имеющим обязательный характер.

Комитет, среди прочего, разрабатывает и принимает стандарты использования данных, осуществляет мониторинг в части соблюдения Конвенции государствами-участниками и рекомендует меры, которые необходимо принять в случае, если государство-участник не соблюдает положения Конвенции. Рабочий орган также готовит заключения относительно уровня защиты персональных данных кандидатов на присоединение к Конвенции, выдвигает предложения и выражает мнение о поправках к Конвенции, формирует предложения для облегчения или улучшения применения Конвенции.

«Доверие при использовании информационно-коммуникационных технологий возможно обеспечить лишь в случае уверенности пользователя в том, что его информация и обрабатываемые данные защищены. Международное сотрудничество является единственным механизмом по обеспечению глобальной

защиты персональных данных и созданию безопасных условий для трансграничного потока таких данных. В рамках работы по совершенствованию соответствующего национального законодательства Россия опирается на международный опыт и учитывает существующие общепризнанные глобальные стандарты», — сообщил врио директора департамента информационной безопасности Минцифры России Дмитрий Реуцкий.

С учетом представительства Российской Федерации в Бюро Комитета планируется дальнейшая активизация деятельности по представлению интересов страны в Совете Европы с учетом основ государственной политики Российской Федерации в сфере информационной безопасности и развития информационно-коммуникационных технологий в целях надлежащего правоприменения положений Конвенции, а также при разработке нормативно-методического инструментария организации в обозначенной сфере.

К ОГЛАВЛЕНИЮ

ГОСДУМА УВЕЛИЧИВАЕТ ШТРАФЫ ЗА НАРУШЕНИЕ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

09/02/21, tass.ru. Госдума во вторник приняла во втором - основном - чтении законопроект, который в том числе ужесточает санкции в сфере защиты персональных данных. Изменения предлагается внести в статью 13.11 Кодекса об административных правонарушениях (КоАП). Согласно поправкам, обработка персональных данных в случае, если это не предусмотрено законодательством, повлечет штрафы для граждан в размере от 2 тыс. до 6 тыс. рублей, для должностных лиц - от 10 тыс. до 20 тыс. рублей, для юридических лиц - от 60 тыс. до 100 тыс. рублей. Сейчас штрафы за это правонарушение установлены в два раза меньше.

Кроме того, в КоАП предлагается прописать, что повторное нарушение повлечет штраф для граждан в размере от 4 тыс. до 12 тыс. рублей, для должностных лиц - от 20 тыс. до 50 тыс. рублей,

для индивидуальных предпринимателей - от 50 тыс. до 100 тыс. рублей, для юридических лиц - от 100 тыс. до 300 тыс. рублей.

Обработка персональных данных без согласия, данного в письменной форме, повлечет штраф для граждан в размере от 6 тыс. до 10 тыс. рублей (сейчас от 3 тыс. до 5 тыс. рублей), для должностных лиц - от 20 тыс. до 40 тыс. рублей (сейчас от 10 тыс. до 20 тыс. рублей), для юридических лиц - от 30 тыс. до 150 тыс. рублей (сейчас от 15 до 75 тыс. рублей).

Данные положения были включены в законопроект, который изначально предусматривал только штрафы за нарушения положений закона об устойчивом интернете в РФ. К ОГЛАВЛЕНИЮ

ГОСДУМА ПОДДЕРЖАЛА ПОПРАВКИ В ЗАКОН О ПЕРСОНАЛЬНЫХ ДАННЫХ

17/02/21, rspectr.com. Государственная дума приняла в первом чтении поправки в законопроект о порядке обезличивания персональных данных. Изменения позволяют, в частности, оформлять одно согласие на их обработку сразу для нескольких целей. Ко второму чтению законопроект предложили доработать, чтобы он позволял защитить персональные данные граждан и предусматривал безусловную возможность отзыва согласия на их обработку, отмечает в своем блоге глава комитета Госдумы по информационной политике информационным технологиям и связи Александр Хинштейн.

Согласно документу в законопроект будут внесены следующие изменения:

- вместо ФИО и адреса разрешить использование «уникального идентификатора»;
- оформлять одно согласие на обработку данных для нескольких целей, для каждой из них должны быть указаны сроки действия и лица, которым дается разрешение;
- использовать для уничтожения информации только те средства, которые прошли процедуру соответствия в ФСБ России или в Федеральной службе по техническому и экспортному контролю (ФСТЭК) России;

❖ утвердить процедуру обезличивания данных. Требования и методы их обезличивания утвердит Роскомнадзор.

«Регламентация требований и методов по обезличиванию персональных данных на уровне нормативного акта Роскомнадзора с учетом развития информационных технологий позволит оперативно вносить необходимые изменения и дополнения в существующую методологию обезличивания персональных данных», – говорится в документе.

В правительстве считают, что принятие законопроекта позволит существенно повысить эффективность системы защиты прав субъектов персональных данных, а также предоставит им право на использование методологической базы по обезличиванию персональных данных.
К ОГЛАВЛЕНИЮ

ВСТУПИЛ В СИЛУ ЗАКОН О ПРАВЕ ТРЕБОВАТЬ УДАЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

01/03/21, tass.ru. Закон о запрете распространения персональных данных граждан России без их специального согласия вступил в силу с 1 марта. Операторы теперь обязаны удалять персональные данные по первому запросу их владельца. Автор закона - депутат, член комитета Госдумы по информполитике Антон Горелкин пояснил ТАСС, что с 1 марта каждый гражданин России впервые станет полноправным хозяином своих персональных данных в интернете.

Теперь граждане могут потребовать от любого ресурса в сети (сайт, соцсеть, мессенджер и так далее) прекратить распространять персональные данные. У администрации ресурса будет три дня на рассмотрение заявки и принятие решения по ней. Если через три дня ресурс продолжает распространять данные, гражданин вправе подать в суд.

«Отказать в удовлетворении требования могут, только если распространение ваших персональных данных представляет общественную значимость. Например, ваше имя упоминается в журналистской публикации на важную тему или связано

с обнародованием материалов резонансного уголовного дела. Но даже в этих случаях у вас все равно остается право на суд, и владельцы ресурса должны будут доказать законность публикации ваших персональных данных в каждом конкретном случае», - пояснил Горелкин.

Он также сказал, что все это касается даже той информации, которую гражданин сам о себе выложил в публичный доступ. «Увидели опубликованный скрин вашей открытой страницы в соцсети - уже можете требовать его удалить. Аналогично с номером телефона, домашним адресом и даже просто вашим лицом. И тот факт, что информация взята из открытого источника, не будет оправданием для ее распространителя», - указал депутат.

Отдельное согласие

Также с 1 марта у граждан РФ должны будут спрашивать отдельное согласие на распространение личной информации. При регистрации на любых интернет-ресурсах, сказал Горелкин, уже недостаточно будет «галочки» под пользовательским соглашением: «Должен быть отдельный вопрос с возможностью прямого ответа на него. Никаких «подразумевается по умолчанию» и прочего юридического камуфляжа».

Перерегистрироваться на тех платформах, где уже есть аккаунты, не понадобится. Дополнительных запросов со стороны соцсетей или мессенджеров по поводу персональных данных пользователя сейчас тоже не будет. Но при перезаключении пользовательского соглашения, например, после очередного обновления ресурса, у пользователя уже должны будут спросить согласие в соответствии с новой нормой. Горелкин отметил, что на практике взаимодействие пользователя с интернет-ресурсами принципиально не изменится. Свои запросы по поводу персональных данных можно писать в той же форме обратной связи, которая использовалась на сайте до этого. Или же направлять их на официальный почтовый ящик организации, которая владеет ресурсом.

В пресс-службе Роскомнадзора ТАСС пояснили, что новый закон определяет согласие гражданина как единственное условие для распространения персональных данных. Он дает возможность определить перечень тех сведений, которые он готов сделать общедоступными. Кроме того, подчеркнули в ведомстве, операторы

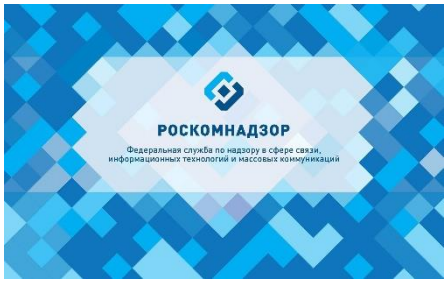
теперь обязаны удалять персональные данные по первому запросу их владельца.

До вступления закона в силу персональными данными, размещенными в общем доступе, например, открытыми профилями в социальных сетях, анкетами поиска работы на рекрутинговых сайтах и так далее мог воспользоваться неограниченный круг лиц. В частности, скопировать и далее распространить их на иных интернет-ресурсах без соответствующего согласия гражданина. Теперь в ситуации, когда персональные данные оказалась доступны неограниченному кругу лиц в результате правонарушения, преступления или форс-мажора, любой оператор, допустивший их дальнейшее распространение и тиражирование, обязан будет подтвердить законность своих действий или принять меры по прекращению такого распространения.

Например, пояснили в ведомстве, если произошла утечка базы данных какой-либо организации, ресурс или пользователь, разместивший у себя на веб-сайте или на странице в социальных сетях эту базу или ее часть, будет обязан доказать законность ее копирования, распространения и обработки. Если доказать законность обработки не удастся, то сайт должен удалить персональные данные либо его владелец будет оштрафован.

К ОГЛАВЛЕНИЮ

РОСКОМНАДЗОР РАЗРАБОТАЛ ЕДИНУЮ ФОРМУ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ



01/03/21, tass.ru. Роскомнадзор разработал специальную форму согласия на обработку персональных данных в развитие вступившего в силу закона, запрещающего распространять личную информацию без согласия ее владельца. Об этом в понедельник сообщил первый замглавы комитета Госдумы по информационной политике, информационным технологиям и связи Сергей Боярский («Единая Россия»).

По словам парламентария, которого цитирует пресс-служба фракции, Роскомнадзор в качестве уполномоченного органа

уже подготовил специальную форму согласия, соответствующий приказ находится на утверждении в Минюсте. «Коллеги были намерены сделать ее в наиболее простой и доступной форме для комфорта граждан. Я также надеюсь, что в целом форма согласия на обработку персональных данных в обозримом будущем сможет обрести унифицированный вид, люди фактически заранее будут знать ее содержание», - отметил он.

Депутат также напомнил, что по новому закону граждане смогут свободно отзывать согласие на обработку персональных данных - как письменно, так и в электронном виде через специальную систему. "Новый закон закрепляет правило, что молчание или бездействие гражданина ни при каких обстоятельствах не может считаться согласием на обработку его персональных данных, разрешенных им для распространения", - пояснил единоросс.

«Актуальная редакция закона «О персональных данных» - это очередной шаг по совершенствованию всего механизма защиты персональных данных от их недобросовестного и незаконного распространения. Теперь у граждан появится возможность указывать, какие именно персональные данные можно обрабатывать и собирать, а какие можно распространять и передавать дальше», - заключил Боярский.

Закон о запрете распространения персональных данных граждан России без их специального согласия вступил в силу с 1 марта. Операторы теперь обязаны удалять персональные данные по первому запросу их владельца. Граждане могут потребовать от любого ресурса в сети (сайт, соцсеть, мессенджер и т. д.) прекратить распространять их персональные данные. У администрации ресурса будет три дня на рассмотрение заявки и принятие решения по ней. Если через три дня ресурс продолжает распространять данные, гражданин вправе подать в суд. К ОГЛАВЛЕНИЮ

ОПЫТ И РЕШЕНИЯ КОМПАНИЙ

РЖД СООБЩИЛИ О НАЧАЛЕ ОФОРМЛЕНИЯ БИЛЕТОВ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

22/01/21, interfax.ru. ОАО «РЖД» внедряет систему автоматического ввода данных паспорта в бланки билетов в кассах дальнего следования,

сообщили РЖД. «Для этого АО «Федеральная пассажирская компания» оборудует кассы программно-аппаратными комплексами на основе средств искусственного интеллекта», - говорится в сообщении.

При оформлении билетов кассиру достаточно приложить документ к сканеру и данные пассажира автоматически появятся на бланке проездного документа. Отмечается, что подобные комплексы позволят значительно сократить время оформления билетов, минимизировать возможность ошибки при оформлении и повысить производительность работы кассиров.

Отмечается, что устройство способно за несколько секунд распознать данные не только российского внутреннего паспорта, но и заграничного паспорта, свидетельства о рождении, а также паспортов почти 200 стран мира.

В сообщении говорится, что это особенно эффективно при оформлении билетов гражданам других стран, «так как в зависимости от страны выдачи паспорта и особенностей самого документа поля с указанием имени и фамилии могут меняться местами и содержать несколько слов».

Ранее, при ручном вводе, кассиру требовалось дополнительное время на определение правильной последовательности реквизитов в иностранном паспорте и корректности их ввода. Сейчас, вне зависимости от типа паспорта, весь процесс ввода данных занимает не более 5 секунд.

ФПК получила 835 таких аппаратных комплексов, они установлены на крупнейших вокзалах России.

Как уточняется в сообщении, программно-аппаратный комплекс для ввода данных пассажиров – это отечественная разработка на основе средств искусственного интеллекта. Устройство представляет собой видеосканер, который подключается к компьютеру через разъем клавиатуры без установки дополнительного программного обеспечения. Он полностью автономен, оснащается видеокамерой и встроенным вычислительным модулем для обработки документов без подключения к внешним устройствам. Персональные данных пассажиров, как уточняется, не сохраняются в компьютере или облачном хранилище. К ОГЛАВЛЕНИЮ

КОМПАНИЯ «РЖД» КОРРЕКТИРУЕТ ПОЛИТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10/02/21, gudok.ru. ОАО «РЖД» непрерывно совершенствует собственную IT-инфраструктуру – одну из самых масштабных в России, тестирует и аудирует новые решения. Но компании с высокими показателями цифровой зрелости также приходится принимать всё больше вызовов в области кибербезопасности. Вопросы информационной безопасности в РЖД находятся в зоне ответственности двух подразделений – службы безопасности и IT-блока. О том, как обеспечивается защита систем цифровых сервисов, мы поговорили с Евгением Чаркиным, заместителем генерального директора ОАО «РЖД».

– Евгений Игоревич, как организован аудит информационной безопасности в компании?

– Системы информационной безопасности ОАО «РЖД» обрабатывают более 46 000 событий ежесекундно. Каждый узел сети сканируется ежемесячно, а серверный сегмент – не реже одного раза в неделю. Для этого используется система контроля защищённости с применением программных и аппаратных решений, основанных на отечественных продуктах.

Глобальный аудит критических уязвимостей IT-инфраструктуры РЖД также осуществляется на постоянной основе. А в 2020 году был проведён ряд дополнительных аудитов в связи с переводом на удалённую работу более 100 тыс. сотрудников компании. Хочу отметить, что в ходе беспрецедентного перевода на удалённую работу такого количества пользователей, реализованного за прошедший год дважды, проблем с информационной безопасностью не возникало.

– Какие серьёзные попытки взлома инфосистем ОАО «РЖД» были в последние годы? Какие системы подвергались атакам, как были ликвидированы нападения?

– За 2020 год зафиксировано 28 094 попытки заражения вредоносным программным обеспечением (компьютерными вирусами и «червями»). Более 1000 таргетированных компьютерных атак на конкретные объекты информационной инфраструктуры и даже конкретных людей были успешно отражены. Особенно опасны атаки на финансовый блок и системы управления производственной деятельностью. Ежемесячно на веб-ресурсы компании осуществляются DDoS-атаки.

Например, в последние месяцы прошлого года средствами системы управления информационной безопасности регистрировалась целевая компьютерная атака так называемого критического уровня влияния. Данный вид атак хорошо спланирован, и при положительном результате злоумышленник может закрепиться в инфраструктуре, а в последующем иметь доступ к ресурсам компании и оставаться незамеченным месяцами, иногда годами. Целью конкретной атаки был финансовый сектор ОАО «РЖД»: хакеры пытались получить логины и пароли для доступа к системам перечисления денежных средств, а также критическим системам для сдачи бухгалтерской отчётности. Данная атака не дошла до продуктивных систем и работников компании, которые даже не узнали о происходящем. Негативных вмешательств в бизнес-процессы РЖД допущено не было.

– Расскажите о случаях, которые получили широкую огласку.

– В январе этого года пользователь под псевдонимом @LMonoceros на одном из популярных сайтов опубликовал пост о взломе сети передачи данных компании и получении доступа к ресурсам двух дирекций, в том числе к камерам видеонаблюдения на вокзальных комплексах. В ходе расследования факт неправомерного доступа был подтверждён. Автор нашумевшей статьи воспользовался уязвимостью в настройке маршрутизатора, обеспечивающего сопряжение сети Интернет и не введённого в эксплуатацию сегмента обособленной информационной системы. Описав подробный сценарий действий и предположительные угрозы, он привлёк к сети РЖД внимание широкой аудитории хакеров как в России, так и из других стран. Таким образом, он спровоцировал массовые атаки на информационную систему огромной компании, от деятельности которой зависит безопасность миллионов пассажиров.

С сожалением должен отметить, что массовое распространение непроверенной информации через СМИ только ухудшило ситуацию.

Факт наличия выхода этой сети в Интернет – тема внутреннего расследования, которое сейчас ведётся в компании. Не исключена намеренно оставленная уязвимость. С этим будет разбираться служба безопасности РЖД. А органы правопорядка, в свою очередь, дадут правовую оценку действиям автора этой публикации.

Как уже говорилось в официальных заявлениях компании, произошедший инцидент не был связан с организацией перевозочного процесса, угрозы безопасности движения поездов не было, а личные данные клиентов холдинга не пострадали.

Другой случай произошёл в прошлом году в ноябре. Тогда украинский телеграмм-канал DC8044 сообщил о размещении в открытом доступе на сайте «РЖД Бонус» файла резервной копии базы данных этого сайта (так называемый дамп) размером около 2,4 Гб. В нём содержалась информация об адресах электронной почты пользователей сайта, их идентификаторах в программе лояльности (это набор цифр) и хеш пароля для доступа в личный кабинет. Инцидент произошёл из-за ошибки администратора подрядной организации, выполняющей работы над сайтом.

В обоих случаях для нейтрализации актуальных угроз безопасности были оперативно предприняты первоочередные действия по защите информации в сети передачи данных ОАО «РЖД» и личных данных клиентов, а также по обеспечению безопасности перевозочного процесса. Для этого у нас разработаны и применяются соответствующие нормативные документы: положение и регламенты выявления, регистрации, реагирования на инциденты информационной безопасности.

– Были ли сделаны в компании какие-то выводы после инцидента со взломом сети видеокамер?

– Да, конечно. Сейчас мы разрабатываем механизм привлечения внешних пользователей к аудиту уязвимостей сети на взаимовыгодной основе: будем внедрять специальную линию call-центра, которая поможет маршрутизировать звонки о разных «находках» на внешнем периметре корпоративной сети профильным специалистам в РЖД. Варианты взаимовыгодного сотрудничества тоже обсуждаем.

Верхнеуровневая задача для менеджмента компании сейчас – проанализировать эти кейсы и скорректировать политику информационной безопасности в масштабе всего холдинга, чтобы исключить возможность повторения такой ситуации.

Цифровизация процессов становится основным драйвером развития РЖД. Но перевод в «цифру» всё большего числа данных повышает опасность их утечки в результате намеренного взлома системы или сбоя в работе её защиты.

– Из каких уровней состоит система защиты информации в компании, на ликвидацию каких угроз она рассчитана?

– Мы постоянно проводим комплексные как организационные, так и технические мероприятия по удовлетворению требований федерального законодательства в области информационной безопасности. И особое внимание уделяем защите объектов критической информационной инфраструктуры, прежде всего связанных с производственными бизнес-процессами.

Управление информационной безопасностью базируется на принципах риск-ориентированного подхода и встроено в систему управления рисками внутреннего контроля ОАО «РЖД». Ядром является централизованная Система управления информационной безопасностью, развёрнутая на сети ОАО «РЖД» и представляющая собой комплекс систем обеспечения, контроля и реагирования на инциденты информационной безопасности.

– Расскажите подробнее, как организована защита от внешнего и несанкционированного внутреннего проникновения?

– В РЖД мы, как вы правильно заметили, уделяем особое внимание защите информационной инфраструктуры не только от внешнего, но и от внутреннего проникновения, действий инсайдеров. Информационная безопасность компании строится исходя из парадигмы комплексной защиты от внешнего и несанкционированного внутреннего проникновения. В компании организованы мониторинг и контроль за потенциальными точками проникновения в инфраструктуру, которые позволяют быстро обнаружить действия злоумышленников. Для этого развёрнуты и активно применяются различные технические решения, в том числе

так называемые DLP-системы (от англ. Data Loss Prevention). Система предотвращения утечек информации собирает данные с различных сенсоров, расположенных на стыке с сетью Интернет, и отображает обнаруженные в них признаки аномалий поведения пользователей, попыток утечки информации, детектирует сложные целевые атаки на инфраструктуру компании, когда внутренний и внешний злоумышленники действуют сообща.

К технологиям детектирования таких атак относятся, например, выполнение проверок всех исполняемых файлов в облачной инфраструктуре на основе технологии машинного обучения. Также мы выявляем подозрительные и вредоносные активности информационных объектов на основе анализа их поведения в изолированной среде: это почтовые сообщения, различные документы, файлы. Ведём анализ файлов с использованием ранее созданных пользовательских сигнатур. Также мы ведём так называемые репутационные списки вредоносных и фишинговых ресурсов, адресов узлов управления вредоносным ПО, адресов хакерских группировок.

Для минимизации рисков, связанных с внутренними угрозами, в компании осуществляется постоянный контроль каналов передачи информации. Это позволяет выявлять неправомерные действия сотрудников компании, находить закрытые к публикации данные в открытом доступе на локальных и сетевых ресурсах компании, а также проводить анализ поведения сотрудников и выявлять признаки противоправных действий. Комплексное использование различных технических решений в области обеспечения информационной безопасности позволяет практически мгновенно реагировать на угрозы безопасности информации в автоматизированном режиме.

– Что происходит после обнаружения IP-адресов, с которых проведена атака? Добивается ли компания уголовного преследования злоумышленников?

– При обнаружении внешних атак на инфраструктуру компании система защиты информации в автоматизированном режиме блокирует IP-адреса атакующего. Как правило, это адреса так называемого теневого сегмента сети Интернет, но, если при отработке инцидента удаётся деанонимизировать источник атаки, направляются заявления в правоохранительные органы, возбуждаются уголовные дела. Например, в 2019 году житель Краснодарского края незаконным

способом получил доступ к охраняемой законом компьютерной информации, находящейся на серверах Сервисного портала работника, руководителя и неработающего пенсионера ОАО «РЖД». Полученную информацию он скопировал себе на компьютер, а позже разместил в общем доступе на одном из интернет-ресурсов. По данному факту было направлено заявление в МВД и позже возбуждено уголовное дело. В мае 2020 года хакер был признан виновным в совершении нескольких преступлений: неправомерном доступе к компьютерной информации и незаконном получении и разглашении сведений, составляющих коммерческую тайну. Наказанием послужил штраф в размере 100 тыс. руб.

– Сейчас в компании идёт строительство собственной фабрики программных роботов, предполагающее замену человеческого труда при осуществлении рутинных операций в работе с инфосистемами. Для роботов будет разработан собственный механизм безопасности?

– Безусловно, работы по обеспечению безопасности информации в информационной системе роботизации рутинных операций (одной из многих информационных систем компании) строятся в полном соответствии с требованиями регулятора – ФСТЭК России.

Мы разработали требования к защите информации, содержащейся в данной системе, создали свою подсистему защиты, провели оценку соответствия программного обеспечения и оценку эффективности реализованных мер. А также провели аттестационные испытания системы по требованиям безопасности информации.

– Какова роль искусственного интеллекта в дальнейшем совершенствовании системы киберзащиты ОАО «РЖД»?

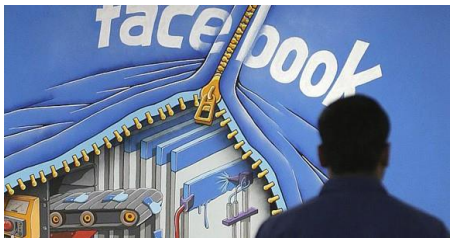
– В компании в настоящее время рассматриваются решения по построению перспективной системы управления информационной безопасностью, в которой традиционные средства, комплексы и системы защиты информации будут дополнены сервисами с использованием искусственного интеллекта. Тем самым система управления информационной безопасностью приобретёт качественно новые функциональные возможности в области сбора, пред-обработки, хранения и анализа информации об инцидентах информационной безопасности.

Первый этап анализа известных решений в области создания отдельных интеллектуальных сервисов и систем управления информационной безопасностью уже практически завершён. Мы также изучаем международные и национальные стандарты в области управления информационной безопасностью и опыт их внедрения.

Следующим этапом для компании станет формирование принципов построения и разработка архитектуры многоуровневой интеллектуальной системы управления информационной безопасностью ОАО «РЖД». К ОГЛАВЛЕНИЮ

ИНДИКАТОРЫ РАЗВИТИЯ. Российская практика

FACEBOOK ВЫПЛАТИЛ 4 МЛН РУБЛЕЙ ЗА НАРУШЕНИЕ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

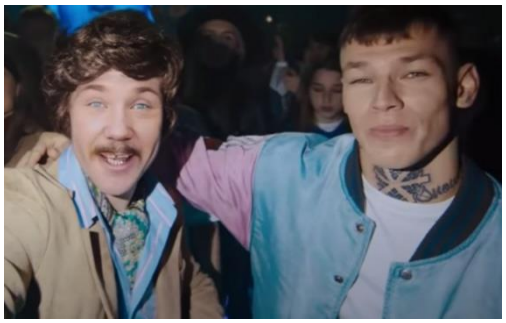


26/11/20, rspectr.com. Компания выплатила штраф в размере 4 млн рублей за непредставление сведений о локализации баз данных российских пользователей. Судебное производство о принудительном взыскании штрафа с Facebook прекратили, сообщает «Интерфакс» со ссылкой на пресс-службу суда.

В феврале суд оштрафовал компании Facebook и Twitter на четыре миллиона рублей каждую за нарушение закона о хранении персональных данных российских пользователях на территории России. Twitter пока штраф не оплатил.

Закон, который обязывает интернет-компании, работающие с персональными данными россиян, регистрироваться как организатор распространения информации (ОРИ), вступил в силу 1 августа 2015 года. Согласно документу, компании должны в течение шести месяцев хранить на территории России всю переданную и полученную жителями страны информацию. К ОГЛАВЛЕНИЮ

О БИОМЕТРИИ ОБРАЗА ЖОРЖА МИЛОСЛАВСКОГО



10/12/20, kommersant.ru. Многим, наверное, запомнился недавно появившийся динамичный ролик Сбербанка, в котором вор Жорж Милославский из фильма «Иван Васильевич меняет профессию» попадает в наши дни. Сама по себе идея рекламы банка с жуликом в главной роли выглядит неоднозначно. Даже учитывая, что он рекламировал «Сбер» еще в 1973 году: «Граждане! Храните деньги в Сберегательной кассе, если, конечно, они у вас есть». Но в Сбербанке гордятся примененными передовыми технологиями, которые позволили, как отметил директор департамента маркетинга и коммуникаций банка Владислав Крейнин, «зарядить предпраздничным настроением» «несколько поколений нашей страны».

Между тем мастерская имитация внешности и голоса Леонида Куравлева — актера, сыгравшего Жоржа Милославского почти 50 лет назад, — вызвала пристальный интерес специалистов по информационной безопасности, обсуждавших ролик в профильном Telegram-канале. И возможности «самых передовых технологий» Сбербанка привели их вовсе не в праздничное настроение. Российский эксперт в области информационной безопасности и защиты данных Михаил Емельянников назвал ролик реквиемом «по ЕБС и биометрии по лицу и голосу в целом».

ЕБС — единая биометрическая система, которую под надзором ЦБ внедряют в свою практику российские банки. Сдав образы лица и голоса, клиент кредитной организации впоследствии сможет получать различные услуги — открывать вклады, платить по счетам, брать кредиты и т. п., — идентифицируя себя дистанционно, например через смартфон.

Однако после такого ролика идентифицироваться в ЕБС, по мнению эксперта, «как-то странно».

Ведь теперь мошенник при удаленной идентификации сможет с помощью технологии deepfake накладывать на свое изображение лицо

жертвы и изменять свой голос. И обновленный Жорж Милославский это прекрасно всем продемонстрировал.

Мощности компьютеров и сами технологии развиваются такими темпами, что скоро для подделки профиля любого гражданина не нужно будет ресурсов экосистемы «Сбера». И красть биометрические данные клиентов из хранилища банков тоже не потребуется: образцы голоса и фотографии или видео клиента легко можно найти в Facebook, Instagram и других соцсетях.

Да, способы защиты от deepfake уже прорабатываются. Однако затраты на них пока высоки, а самой системе необходимо время для проведения анализа. И будет ли ее эффективность близка к 100% гадать, скажем так, преждевременно.

В этой истории немного утешает только тот факт, что ЕБС еще толком не запущена, хотя банки продолжают собирать образы своих клиентов. Так что не исключено, что в новой версии закона о биометрической идентификации вспомнят о сберкнижках, которые также рекламировал Жорж Милославский. К ОГЛАВЛЕНИЮ

МИНТРАНС ПРЕДЛОЖИЛ МАССОВО ВНЕДРЯТЬ БИОМЕТРИЮ В АЭРОПОРТАХ

17/01/21, rbc.ru. К концу 2023 года биометрическая идентификация при прохождении предполетных процедур должна появиться в 6% российских аэропортов, рассчитывает Минтранс. Но внедрение может быть и масштабнее, если ведомство найдет финансирование. О том, что к концу 2023 года 6% российских аэропортов должны будут использовать биометрию для идентификации пассажиров и искусственный интеллект при обработке данных «для упрощения транспортных процедур», говорится в опубликованной программе цифровой трансформации Минтранса. Если у министерства получится найти дополнительное финансирование (реализовать так называемый сценарий развития), показатель должен достичь 15%.

На конец 2019 года в России было 202 аэропорта: 78 международных, 89 федерального значения,

четыре с пассажиропотоком до 10 млн человек в год и 31 — до 1 млн человек в год, приводятся в документе данные Росавиации. То есть если к концу отчетного периода число аэропортов не изменится (сам Минтранс публично данных по развитию аэропортовой инфраструктуры на этот временной диапазон не давал), то к началу 2024 года система должна быть внедрена не менее чем в 12 аэропортах в базовом сценарии и в 30, если появятся дополнительные средства.

Для использования технологий оператор аэропорта должен будет заключать соглашение об информационном взаимодействии с оператором Единой государственной информационной системы обеспечения транспортной безопасности (ЕГИС ОТБ). Будет ли как-то влиять размер аэропорта по объему пассажиропотока для внедрения систем, в документах Минтранса не указано.

Расходы конкретно на оснащение биометрией аэропортов в программе не указаны, но на развитие ЕГИС ОТБ предусмотрены 585,2 млн руб. из бюджета, а при реализации «сценария развития» потребуется еще 3,8 млрд руб. Всего на реализацию программы цифровой трансформации министерство намерено потратить 8,7 млрд руб., размер необходимого дополнительного финансирования оценен еще в 12,7 млрд руб.

С 2018 года в России работает Единая биометрическая система (ЕБС), куда можно загрузить фото своего лица и запись голоса, чтобы с их помощью вместо паспорта подтверждать личность для получения цифровых услуг. Оператором системы является «Ростелеком». Изначально с помощью ЕБС можно было открывать счета, вклады и получать кредиты, в прошлом году в тестовом режиме ее начали применять при проведении экзаменов в Уральском федеральном университете им. Б.Н. Ельцина, для оплаты в сети кофеен Coffee Bean и др. В декабре 2020 года президент России Владимир Путин подписал закон о расширении использования ЕБС, с ее помощью можно будет дистанционно заключать договоры на оказание услуг связи, участвовать в судебных заседаниях и др. К ОГЛАВЛЕНИЮ

ОБЛАСТЬ ПОДОЗРЕНИЯ: ЧИСЛО СУДЕБНЫХ ДЕЛ ИЗ-ЗА УТЕЧЕК ДАННЫХ УДВОИЛОСЬ

29/01/21, iz.ru. Количество судебных дел, связанных с хищением персональной информации, за последний год выросло в два раза, говорится в исследовании сервиса разведки утечек данных DLBI (есть у «Известий»). Чаще других под следствие попадали сотрудники операторов сотовой связи. Но представители этих компаний, а также банков заявили, что не фиксируют утечек, а комплекс мер защиты позволяет эффективно противодействовать хищению информации. По данным опрошенных «Известиями» экспертов, в 2020 году с переходом на удаленную работу выросло число «теневых» утечек, которые не фиксируются службами безопасности.

В ходе исследования эксперты рассматривали данные, публикуемые правоохранительными органами, в момент, когда дела передавались в суд или по ним выносился приговор. «Средний срок следствия составляет около года, в редких случаях шесть-девять месяцев, поэтому нужно понимать, что значительная часть указанных хищений была совершена в 2019 году», — уточнили в DLBI.

Из всех направленных в суд дел, связанных с утечками данных, лидирующую позицию заняли обвинения против сотрудников операторов и салонов сотовой связи: их доля выросла с 44% от общего числа таких инцидентов в 2019 году до 67% в 2020-м, говорится в исследовании. А доля дел в отношении банковских работников упала с 27 до 18%.

При этом общее число переданных в суд дел по продаже данных из госведомств осталось на прежнем уровне, из банков — выросло на 30%, из коммерческих организаций — увеличилось в два раза, а из операторов связи — втрое. Общее число таких дел за прошедший год выросло в два раза — как минимум до 100 инцидентов, сообщили в DLBI.

— Даже с учетом задержки, необходимой для розыска и следствия, количество дел не соответствует числу предложений

о продаже данных на черном рынке. Только по сайтам и форумам даркнета можно говорить более чем о 50 постоянно действующих российских магазинах пробива, на каждый из которых работают десятки инсайдеров в различных структурах. При этом ни один такой магазин не прекратил в прошлом году работу, — рассказал основатель сервиса разведки утечек данных DLBI Ашот Оганесян.

Рост хищений из баз сотовых операторов объясняется, во-первых, низким уровнем заработной платы сотрудников фронт-офисов и салонов связи, отмечается в исследовании. Другая причина в том, что работавшие в салонах злоумышленники продавали украденные данные, не конспирируясь, и часто передавали их своим знакомым, что позволяло правоохранителям без труда выявлять таких торговцев, а потом документировать их действия контрольными закупками.

По данным исследования, сотрудники сотовых компаний и салонов связи продают как услуги «пробива», передавая заинтересованным лицам детализацию звонков и SMS-сообщений, так и клонируют SIM-карты по заказу мошенников, взламывающих системы двухфакторной авторизации. Из-за этого в 2020 году выросла доля хищений цифровых активов, помимо денег со счетов в банках — от криптовалютных кошельков до «красивых» доменов и имеющих большую аудиторию групп в социальных сетях, отмечают эксперты DLBI.

В 2020 году на основании 70 судебных решений ограничен доступ к 777 интернет-ресурсам, на которых были размещены персональные данные с нарушением закона, сообщили в Роскомнадзоре. «Известия» направили запрос в Следственный комитет. К ОГЛАВЛЕНИЮ