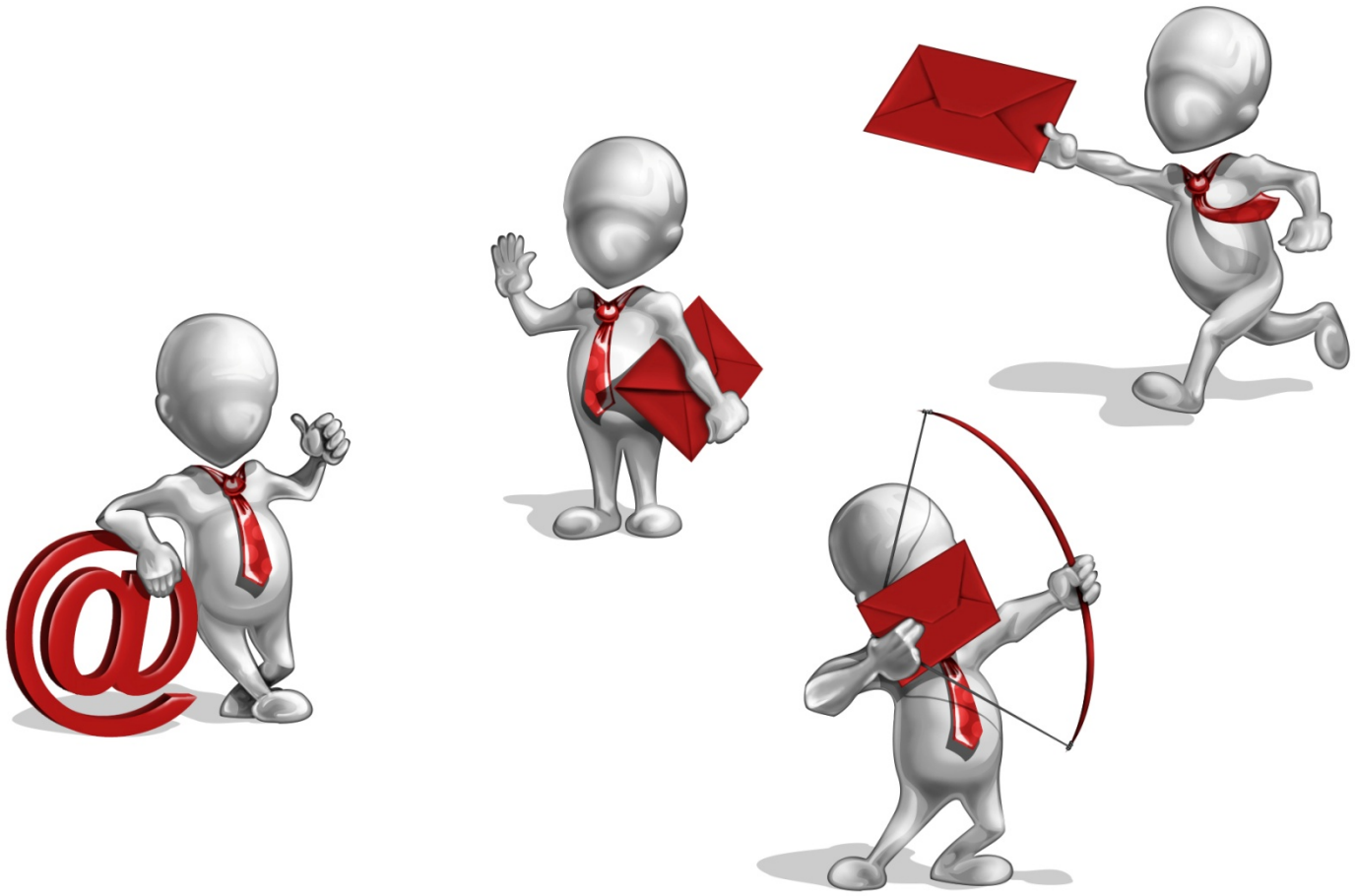
УПРАВЛЕНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОАО «РЖД»

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ



тематический обзор материалов СМИ и блогосферы

№8

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

ОГЛАВЛЕНИЕ *

ВЫБОР РЕДАКЦИИ

РЕГУЛИРОВАНИЕ. Российское регулирование

Опыт и решения компаний

ПО и технические новинки

УТЕЧКИ ИНФОРМАЦИИ. Инциденты

ИНДИКАТОРЫ РАЗВИТИЯ. Российская практика

ИНДИКАТОРЫ РАЗВИТИЯ. Зарубежная практика

Навигация по документу осуществляется путем нажатия на заголовок публикации в самом оглавлении, а также на гиперссылку «К ОГЛАВЛЕНИЮ» в последнем ее абзаце.

Представленные в тематическом обзоре материалы приводятся в оригинальном виде – орфография, пунктуация и стиль автора сохранены. Позиция Управления может не совпадать с отдельным оценочным мнением автора.

ВЫБОР РЕДАКЦИИ

НОВЫЕ ШТРАФЫ В ЗАКОНЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ. УЖЕ С 1 ИЮЛЯ.

09/06/17, knopka.com. В феврале депутаты внесли правки в закон о персональных данных. Он касается всех, кто собирает и обрабатывает личные данные посетителей, клиентов или подписчиков.

Персональные данные — это любые данные, с помощью которых можно определить личность.

Для тех, кто неправильно работает с персональными данными — с 1 июля видов нарушений станет больше, а штрафы вырастут. Раньше предприниматель-нарушитель платил максимум 10 000 ₽, теперь потеряет гораздо больше: штрафы для юрлиц — до 75 000 ₽, для ИП — до 20 000 ₽.

В законе много нюансов, которые сложно описать полностью, мы попытались выделить главное. Рассказываем, за что конкретно могут оштрафовать и как избежать наказания.

Кого касается закон о персональных данных

Многие думают, что операторы по обработке персональных данных — это только сотовые компании и банки. На самом деле, их гораздо больше. В реестре операторов на сайте Роскомнадзора найдёте свыше 380 тысяч компаний. Среди них — страховые компании, банки, сотовые операторы, турагентства, медицинские компании и компании с обучающими курсами.

Если у вас есть сайт с формой обратной связи, подпиской или с личным кабинетом, где посетители оставляют данные — это явный признак того, что закон к вам тоже относится. Вам тоже нужно зарегистрироваться в реестре, заявление можно подать на сайте Роскомнадзора.

Легче выделить тех, кому можно не регистрироваться. Исключения есть, но их не так много.

Закон вас не касается, если:

- вы частное лицо и собираете данные только для личных и семейных нужд: телефон девушки на сайте знакомств, электронную почту бывшего одноклассника в Вконтакте;
- получаете только данные сотрудников;
- клиент сам разместил данные в открытом доступе;
- получаете только ФИО пользователя, клиента или посетителя;
- получаете персональные данные, чтобы заключить договор без дальнейшей передачи этих данных куда-либо;
- собираете данные для выдачи одноразового пропуска;
- вы общественная или религиозная организация и сами обрабатываете данные участников;
- обрабатываете данные без использования компьютера;
- собираете данные для транспортной безопасности;
- обрабатываете данные со статусом государственных автоматизированных информационных систем;
- работаете с данными, которые включены в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- работаете с документами Архивного фонда Российской Федерации и аналогичных документов;
- работаете с данными, которые являются государственной тайной; данные относятся к публичной информации о деятельности судов в России.

Какие штрафы и как их избежать

Самый высокий штраф грозит за обработку персональных данных без письменного согласия или за нарушение списка сведений в этом документе — для компаний штраф составит 75 000 ₽. Если вы заключили договор на медицинские услуги, занесли ФИО пациента в программу, но не подписали отдельное согласие на обработку данных — будет штраф. Получайте письменное согласие от каждого посетителя, клиента и подписчика.

Когда нет возможности получить письменное согласие, просите согласится с правилами сайта. Под каждой формой, где посетители оставляют данные, укажите галочку с подписью: «Ознакомлен с политикой конфиденциальности» или «Согласен с правилами

обработки персональных данных». На самом деле, это тоже нарушает закон, но можно будет апеллировать к малозначительности такого нарушения, так как вы предприняли максимально возможные действия, чтобы получить согласие. Живой практики пока нет, поэтому мы не уверены, что это сработает. Но наши юристы говорят, что с галочкой лучше, чем без. А мы им доверяем :)

Обработка данных без согласия грозит штрафом от 10 000 ₽ до 20 000 ₽ директору, предприниматель получит такой же штраф, а компания — от 15 000 ₽ до 75 000 ₽. Нельзя просить у клиента телефоны трёх друзей в обмен на скидку. Дать согласие на обработку персональных данных можно только лично.

За обработку и за использование персональных данных не по назначению директор и ИП заплатят от 5 000 ₽ до 10 000 ₽, а компания — от 30 000 ₽ до 50 000 ₽. Запрашивайте только те данные, которые нужны. Не просите фотографию или паспортные данные для подписки на новостную рассылку.

Если не разместить на видном месте доступный всем документ, в котором прописаны все условия использования персональных данных и требования — будет предупреждение или штраф. Для руководителя компании — от 3 000 ₽ до 6 000 ₽, для индивидуальных предпринимателей — от 5 000 ₽ до 10 000 ₽, а для юридических лиц — от 15 000 ₽ до 30 000 ₽. Обязательно разместите на сайте документ «Политика конфиденциальности» или «Политика обработки персональных данных», а в нём расскажите, как вы заботитесь о личной информации клиентов.

Если информации на сайте ещё нет, а клиент прислал письмо: «Вы нормально храните мои персональные данные? Мне тут звонят и предлагают кредиты из всех банков, а анкету я только у вас заполнял» — у вас есть 30 дней, чтобы привести всё в соответствие с законом и ответить клиенту. Если не успеете, штрафа не избежать.

За отказ предоставить информацию об обработке персональных данных — предупреждение или штраф от 4 000 ₽ до 6 000 ₽ для руководителей, от 10 000 до 15 000 ₽ — для ИП и от 20 000 ₽ до 40 000 ₽ для компаний.

За отказ клиенту в уточнении, блокировке или в уничтожении его персональных данных тоже полагается наказание. Успевайте выполнить требование клиента за 30 дней, иначе штраф: для

руководителей — от 4 000 ₽ до 10 000 ₽, для ИП — от 10 000 ₽ до 20 000 ₽, а для организаций — от 25 000 ₽ до 45 000 ₽.

Если собирали данные на физических носителях, а потом не смогли защитить информацию, и она попала к третьим лицам, исчезла, была изменена или распространена — штрафа не миновать. Директору придётся заплатить от 4 000 ₽ до 10 000 ₽, ИП — от 10 000 ₽ до 20 000 ₽ и компании — от 20 000 ₽ до 50 000 ₽.

Государственные и муниципальные органы тоже будут штрафовать, если персональные данные не были обезличены или были обезличены с нарушениями. Пишете сводку происшествий по району и лично знаете участников, всё равно скажите: «Вчера вечером Н. зашёл к Ж. и попросил в долг пятьдесят рублей». Если напишете Николай и Жора — штраф.

Все наказания распространяются не только на предпринимателей. Для обычных людей тоже предусмотрены штрафы, если вы используете их не для личных целей. Суммы меньше, но всё же есть — от 500 ₽ до 2500 ₽.

	Директор	**Предприниматель**	**Компания**
Штраф за обработку персональных данных без письменного согласия	От 500 ₽ до 1 000 ₽	От 500 ₽ до 1 000 ₽	До 75 000 ₽
Штраф за обработку данных без согласия	От 10 000 ₽ до 20 000 ₽	От 10 000 ₽ до 20 000 ₽	От 15 000 ₽ до 75 000 ₽
Штраф за использование персональных данных не по назначению	От 5 000 ₽ до 10 000 ₽	От 5 000 ₽ до 10 000 ₽	От 30 000 ₽ до 50 000 ₽
Штраф, если не разместить на сайте доступный всем документ	Предупреждение или штраф от 3 000 ₽ до 6 000 ₽	Предупреждение или штраф от от 5 000 ₽ до 10 000 ₽	Предупреждение или штраф от 15 000 ₽ до 30 000 ₽
Штраф за отказ предоставить информацию	Предупреждение или штраф от 4 000 ₽ до 6 000 ₽	Предупреждение или штраф от 10 000 ₽ до 15 000 ₽	Предупреждение или штраф от от 20 000 ₽ до 40 000 ₽
Штраф за отказ клиенту в уточнении, блокировке или в уничтожении данных	От 4 000 ₽ до 10 000 ₽	От 10 000 ₽ до 20 000 ₽	От 25 000 ₽ до 45 000 ₽
Штраф за утерю данных с физических носителей	От 4 000 ₽ до 10 000 ₽	От 10 000 ₽ до 20 000 ₽	от 20 000 ₽ до 50 000 ₽

Что дальше?

К сожалению, штрафы не касаются проблемы утечки персональных данных и не восполняют нанесённый вред тому, чьи персональные данные были распространены. У операторов данных до сих пор нет мотивации защищать базу от утечки.

Зато за нарушение правил сбора и хранения персональных данных суммы штрафов выросли значительно. Если совершить сразу несколько нарушений, то и штрафов будет несколько. Получится немыслимый вклад в бюджет государства. На самом деле, нет. В сравнение со штрафами в других странах, штраф 75 000 ₽ ничтожен.

Например, во Франции и в Германии оператор персональных данных может получить штраф до 300 000 евро. При этом в Германии, если финансовая выгода нарушителя превышает сумму штрафа — может быть начислен и больший штраф. В Италии нарушитель может быть подвергнут штрафу до 720 000 евро.

Скорее всего, обновлённые штрафы затронут в первую очередь средний и малый бизнес, а не владельцев крупнейших баз персональных данных. Однако, новые наказания дают хоть какие-то рычаги давления на многочисленных злостных нарушителей, которые распоряжаются персональными данными граждан, как им захочется.

Если ваши личные данные попадут в список неизвестных вам компаний, и вам будут звонить или писать и предлагать сомнительные услуги — рекомендуем жаловаться в территориальное подразделение Роскомнадзора, обязательно в письменном виде. На сайте можно найти контакты вашего отделения.

Помните, перечень нарушений обновили в соответствии с рейтингом Роскомнадзора. Это значит, что процесс взимания штрафов и поиска нарушителей уже хорошо отлажен и избежать возмездия будет непросто. К ОГЛАВЛЕНИЮ

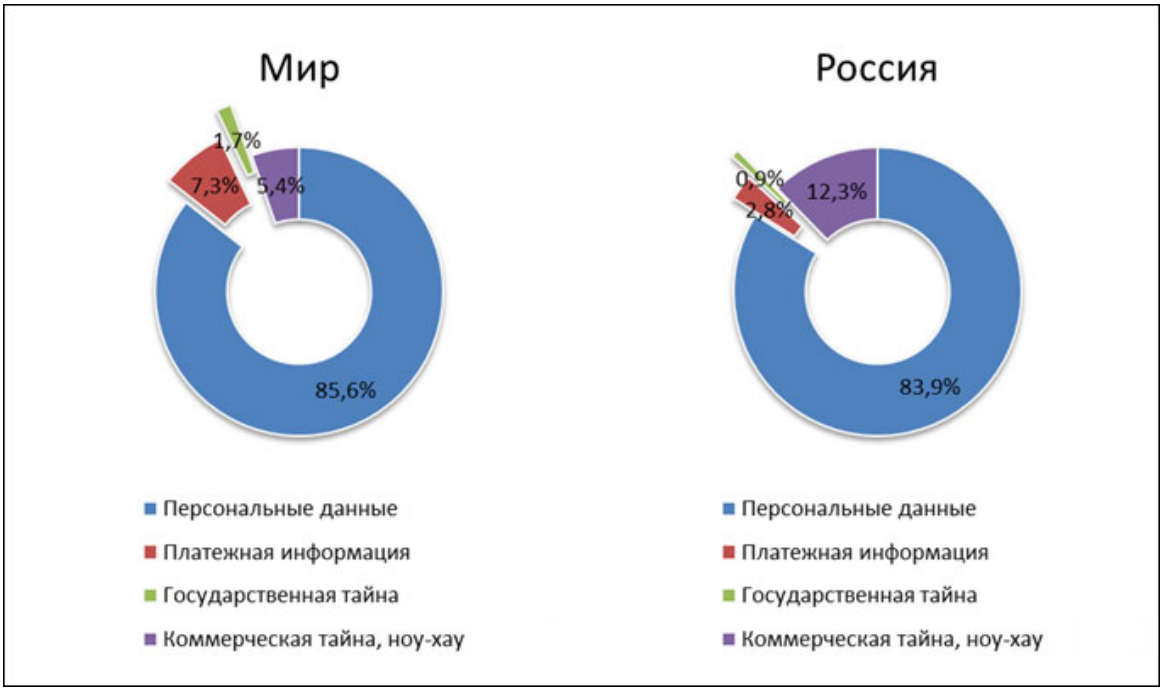
ПЕРСОНАЛЬНЫЕ И ФИНАНСОВЫЕ ДАННЫЕ СОСТАВИЛИ 90% ОТ ВСЕХ УТЕЧЕК В РОССИИ ЗА ГОД – INFOWATCH

08/06/17, d-russia.ru. По результатам исследования утечек конфиденциальной информации из организаций в России в 2016 году было зафиксировано 213 случаев утечек информации из российских компаний и государственных органов, что на 80% больше чем в 2015

году. В девяти из десяти случаев в России утекали персональные данные (ПДн) и платежная информация, сообщает InfoWatch.

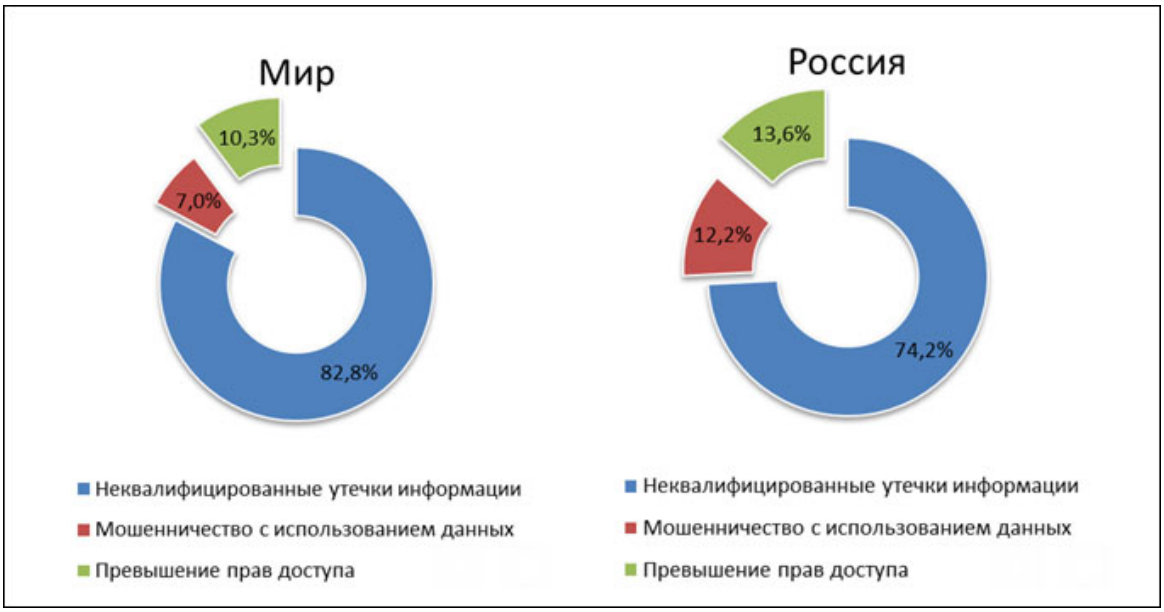
Общий объем скомпрометированных за год данных увеличился более чем в 100 раз — до 128 миллионов записей, но не превысил 4% от мирового объема утечек информации.

Как говорится в отчете, утечка информации из организации превратилась в рядовое явление. Очевидно, что защищать все и от всего одинаково хорошо уже не получится. Необходимо сосредоточиться на наиболее ценных активах, «проблемных» каналах передачи и сотрудниках, которые подвержены риску компрометации данных.

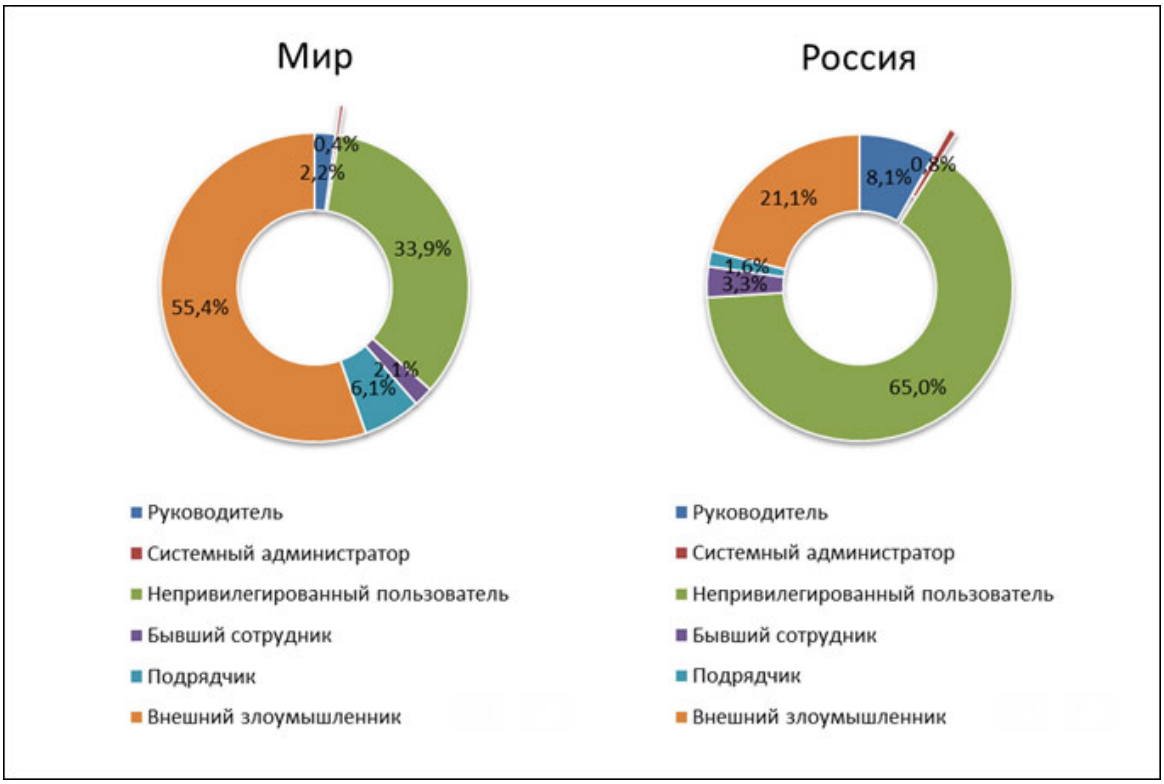


Для России характерна более высокая по сравнению с остальным миром доля так называемых квалифицированных утечек данных —

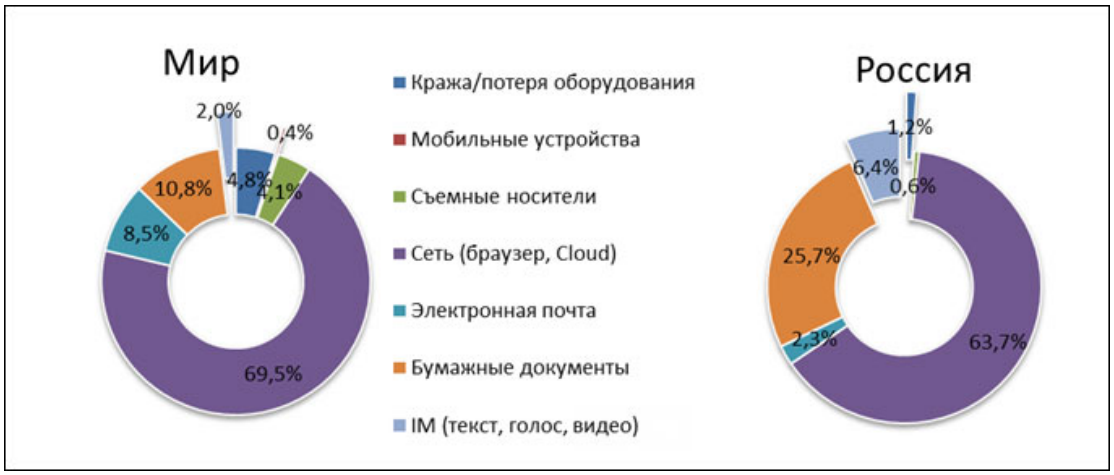
случаев, когда злоумышленник осознанно использует украденную им информацию для достижения личной выгоды (мошенничество с данными, банковский фрод), или получает доступ к информации, заведомо не нужной ему для выполнения трудовой функции (превышение прав доступа).



Внутренние нарушители в организации стали причиной примерно восьми случаев потери данных из десяти, почти каждая десятая утечка происходила при участии руководства организации. Для России характерна более высокая, чем в мире доля утечек по вине руководства (8% против 2%), и более низкая доля утечек по вине внешнего злоумышленника (21% против 55%).

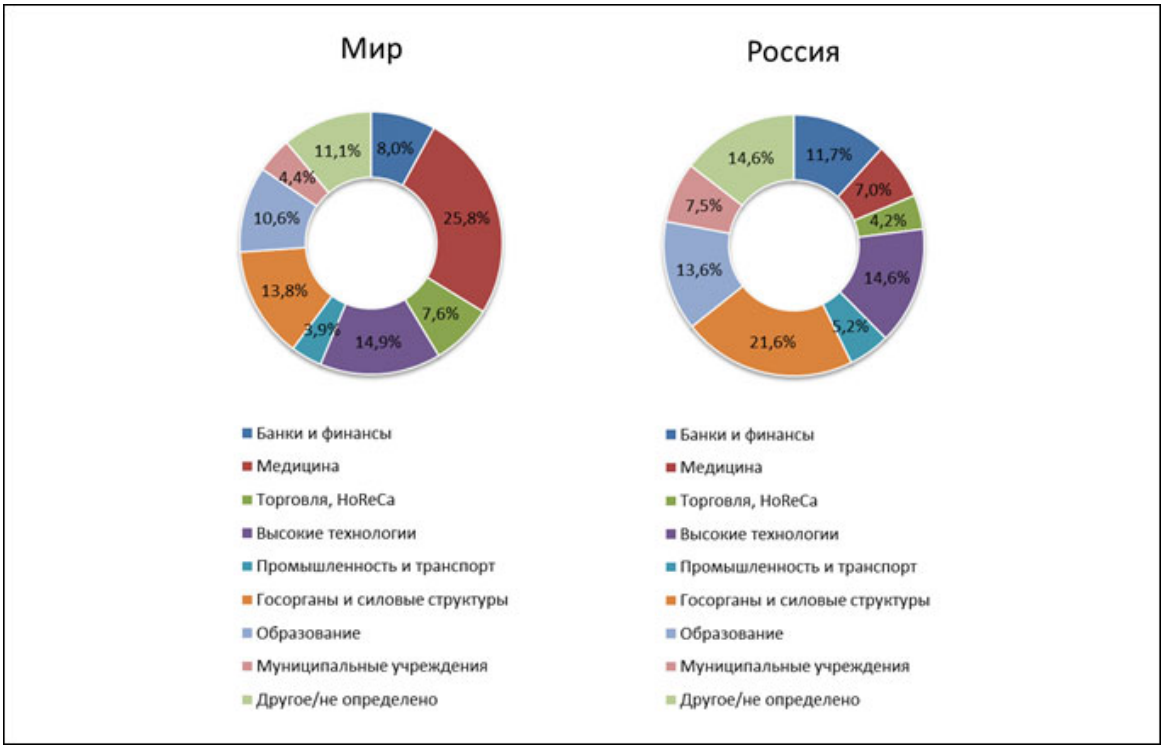


Чаще всего (в 64% случаев) для кражи данных использовался сетевой канал (браузер с подключением к Интернету), каждый четвертый инцидент произошел с использованием бумажных носителей.

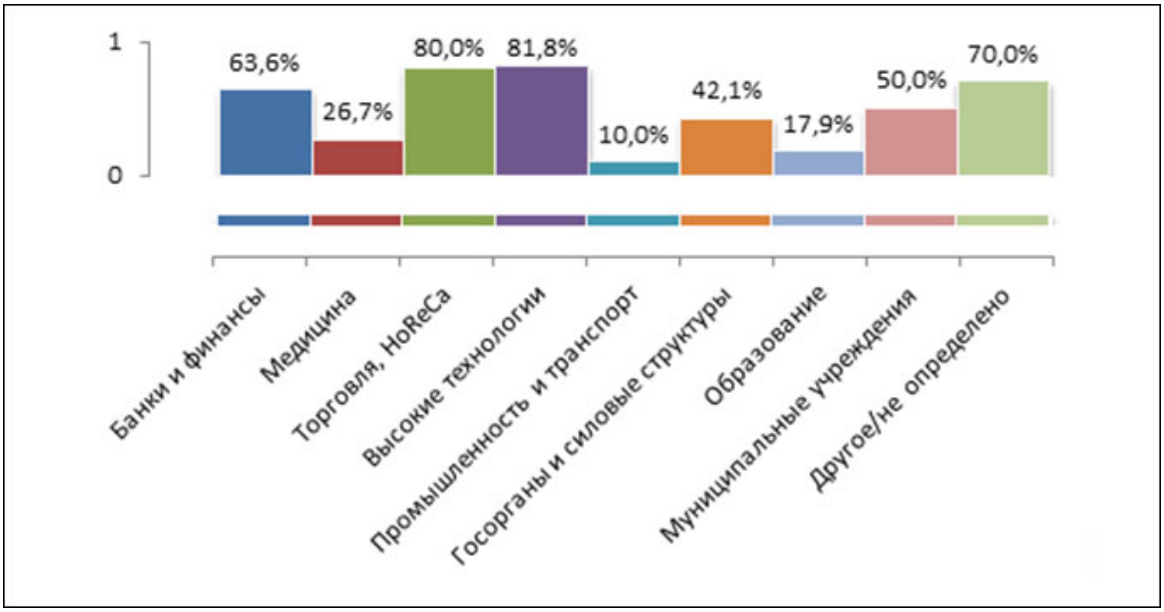


Российское отраслевое распределение утечек серьезно отличается от мирового. В мире более 25% утечек информации происходит из медицинских учреждений, в России доля таких утечек составляет 7%. Обращает на себя внимание высокая (в сравнении с общемировой) доля утечек, которые пришлись на банки и финансовые организации (12%).

Наибольшее количество утечек данных в Росси было зафиксировано в компаниях высокотехнологичного сектора, образовательных учреждениях, государственных органах и банках.



В 2016 году наиболее «привлекательными» для похитителей данных в России оказались торговые и высокотехнологичные компании, к которым добавились финансовые учреждения. В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер.



Жертвами внешних атак, направленных на хищение данных чаще всего становились организации сферы высоких технологий и торговли. От злонамеренных действий внутреннего нарушителя чаще страдали банки, торговые компании и муниципальные учреждения, где чрезвычайно высока ликвидность данных, с которыми работает персонал, говорится в исследовании. К ОГЛАВЛЕНИЮ

ДОРОГА В ЦИФРЕ

14/06/17, rzd-partner.ru. Диджитализация процессов становиться настоящим трендом по всему миру, не обходит эта тенденция и транспортную отрасль. В ОАО «РЖД» пришли к выводу, что реализация проекта «Цифровая железная дорога» являет одним из основных факторов повышения конкурентоспособности.

Комплексная информатизация

По результатам проведенного анализа основных трендов перспективного технологического развития железнодорожного транспорта удалось выявить, что, наряду с инновационными энерго- и

ресурсоэффективными системами, ключевым является создание умной железной дороги. Ее основу составляют сквозные интеллектуальные системы управления работой, обеспечивающие не только повышение уровня безопасности, но и эффективности перевозочного процесса.

«Для нас цифровая железная дорога, это комплексная программа развития, включающая такие направления, как внедрение интеллектуальных систем, работа с большими данными, внедрение интернета вещей, систем связи, создание мобильных приложений и ряда других инициатив. Все они положены в основу принятой в этом году Стратегии развития информационных технологий ОАО «РЖД» до 2020 года. Цель проекта заключается в обеспечении устойчивой конкурентоспособности компании на основе повышения привлекательности услуг», - считает старший вице-президент - главный инженер компании Сергей Кобзев.

По его словам, в основу работы заложены такие принципы, как: полная согласованность, бизнес в режиме онлайн и сервисное управление. Первым шагом в реализации проекта стал анализ всех действующих в холдинге IT решений, который выявил определенные проблемные места в автоматизации внутренних и внешних сервисов. «При формировании структуры цифровой железной дороги поставлена задача по максимальному использованию потенциала средств автоматизации и современных цифровых технологий. Это позволит выйти на новый уровень конкурентоспособности», - добавил он.

Особого внимания, в рамках реализации проекта, уделяется клиентским сервисам. Так, в этом году была запущена электронная торговая площадка «Грузовые перевозки». «Мы начали с базовой услуги по перевозке, но в течение этого года функционал сервиса будет пополнен интермодальными перевозками и сопутствующими сервисами, в частности, складской комплекс, финансовые и цифровые услуги», - отметил директор по информационным технологиям ОАО «РЖД» Евгений Чаркин.

Пассажир не заскучает

На базе цифровых технологий формируются стандарты качества услуг и в сфере пассажирских перевозок, они основаны на передовом опыте создания без барьерной транспортной среды. «Комплекс услуг, проставляемых пассажирам, на всех этапах перевозки, реализуется за

счет максимального применения мобильных приложений», - завил С. Кобзев.

Причем это касается не только приобретения билетов, но и досуга пассажира непосредственно в пути. Сейчас в компании прорабатывают возможности обеспечения доступа пассажиров в интернет, к мультимедиа контенту, социальным сетям и Интернет-торговле. С этой целью реализуется программа «Инновационная мобильность».

В частности, уже запущен поездной портал «Попутчик. Еще одним направлением работы стали вокзалы. «Идея сделать из вокзалов своеобразные торгово-развлекательные хабы, чтобы люди приходили туда не только в ожидании поезда, но и активно пользовались услугами, для этого мы развиваем собственную сеть Wi-Fi и скоро покроем все крупные вокзалы. Помимо этого, в I квартале этого года было запущено мобильное приложение, где последовательно реализуется навигация на вокзале, с отражением всех услуг, которые там предоставляются», - пояснил Е. Чаркин.

Третьим направлением стала реализация приложения, позволяющего пассажиру выстроить свой маршрут по принципу «от двери до двери», с учетом всех видов транспорта.

Локомотивы с интеллектом

«Мы ведем свою работу в соответствии со Стратегией, которая предусматривает такие направления, как обновление парка локомотивов, внедрение интеллектуальных систем управления и развитие информационных систем», - пояснил вице-президент - начальник Дирекции тяги ОАО «РЖД» Олег Валинский.

Значительную роль в повышении эффективности перевозочного процесса, по его словам, играют внедряемые в локомотивном комплексе автоматизированные системы управления и диагностики. Предпосылками к этому стало увеличение веса и скорости движения поездов, при существующих инфраструктурных ограничениях, переход к системе ремонта локомотивов по фактическому состоянию, развитие инфраструктуры сортировочных станций и другие факторы. О сортировочных станциях речь ведется в контексте станции Лужская Октябрьской железной дороги, где совместно с компанией Сименс реализуется проект по внедрению системы управления маневровым локомотивом без участия человека.

«В рамках развития информационных и управляющих систем, мы тоже работаем по целому ряду направлений. В частности, «Электронный маршрут машиниста», проект направлен на решение задач по сокращению непроизводственных потерь за счет повышения качества планирования работы локомотивных бригад, контроля выполнения обязательных производственных операций, соблюдение режима труда и отдыха и многое другое», - заключил О. Валинский.

К ОГЛАВЛЕНИЮ

РЕГУЛИРОВАНИЕ. Российское регулирование

ЗА 2 ГОДА ПО РЕШЕНИЮ СУДА ЗАБЛОКИРОВАНО БОЛЕЕ 300 САЙТОВ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РОССИЯН

05/06/17, rkn.gov.ru. С момента действия Федерального закона № 152-ФЗ «О персональных данных» Уполномоченным органом по защите прав субъектов персональных данных в Реестр нарушителей прав субъектов персональных данных внесено 313 записей на основании судебных решений.

Основанием для ограничения доступа к сайтам-нарушителям послужило размещение персональных данных граждан на ресурсах, предоставляющих доступ к такой информации неограниченному кругу лиц в отсутствие правовых оснований. Большую часть сайтов можно классифицировать как телефонные справочники, сайты с копией личной информации интернет-пользователей из социальных сетей, сайты с доступом к персональной информации российских автовладельцев, используя номер автомобиля.

В 2016 году впервые был апробирован механизм судебного пресечения деятельности иностранного интернет-ресурса за нарушение требований ч. 5 ст. 18 Федерального закона № 152-ФЗ в части локализации баз персональных данных на территории Российской Федерации. Решением суда г. Москвы ограничен доступ к иностранному сайту Linkedin.com в связи с нарушением требований ч.5 ст. 18 Федерального закона «О персональных данных».

Меры в виде блокировки интернет-страниц направлены на профилактику правонарушений в сфере персональных данных. Они представляют собой стимул к соблюдению операторами законодательства в области персональных данных. Применение данного инструмента в деятельности Уполномоченного органа является уникальным в международной правовой системе регулирования сферы защиты персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных в России введен Федеральным законом № 152-ФЗ «О

персональных данных». Он обеспечивает контроль и надзор за соответствием обработки персональных данных. В настоящий момент этим органом является Роскомнадзор.

Реестр нарушителей прав субъектов персональных данных создан Уполномоченным органом в 2015 году в качестве инструмента, направленного на пресечение нарушений в сфере персональных данных. К ОГЛАВЛЕНИЮ

ДУМА РАЗРЕШИЛА ФСО ЗАЩИЩАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ НАХОДЯЩИХСЯ ПОД ГОСОХРАНОЙ ЛИЦ

21/06/17, interfax.ru. Госдума приняла в третьем окончательном чтении закон, предоставляющий Федеральной службе охраны (ФСО) право принимать меры для защиты персональных данных охраняемых службой лиц, а также ограничивать движение на тех трассах, где проезжают охраняемые лица.

Согласно принятым поправкам, обработка персональных данных таких охраняемых лиц и членов их семей осуществляется с их согласия и с согласия органов госохраны. Исключение будут составлять те персональные данные, которые подлежат опубликованию или раскрытию в соответствии с федеральными законами, определяется в принятой поправке.

Также, согласно принятому закону, ФСО имеет право "принимать меры по защите персональных данных объектов государственной охраны и членов их семей".

Кроме того органы государственной охраны наделяются правом использовать на безвозмездной основе аэропорты, аэродромы, вертодромы, посадочные площадки, морские и речные порты, а также получать на безвозмездной основе обеспечение полетов и судовождения. ФСО также получает возможность временно ограничивать или запрещать движение транспортных средств и пешеходов на трассах, по которым проезжают охраняемые лица.

Согласно принятому закону, на службу в ФСО не могут быть приняты граждане при наличии судимости, в том числе снятой или погашенной, при освобождении от уголовной ответственности по нереабилитирующим основаниям, при занятии бизнесом, а также при употреблении наркотиков и любых новых психотропных веществ.

Уточняются также правила применения сотрудниками органов госохраны физической силы, специальных средств и оружия, а также порядок отчуждения зарегистрированного на них за пределами РФ имущества. К ОГЛАВЛЕНИЮ

ЗАКОН О ТЕЛЕМЕДИЦИНЕ СТАВИТ ПОД УГРОЗУ ВРАЧЕБНУЮ ТАЙНУ

22/06/17, mk.ru. В конце прошлой недели Госдума приняла в первом чтении законопроект о телемедицине. С одной стороны, это крайне важный документ, который создаст правовые основы для применения самых передовых технологий в медицине — врачебных консультаций онлайн, транслирования операций сложных пациентов или просто в обучающих целях, во время которых решения многими известными врачами принимаются коллегиально...

И все же далеко не со всеми пунктами нового документа можно согласиться на все сто. Так, жаркие споры вызвало положение законопроекта, по которому вся информация о диагнозе и тактике лечения пациентов теперь должна быть сконцентрирована в единой базе данных. Эксперты считают, что это может привести к самым непредсказуемым последствиям.

Конечно, развитие телемедицины крайне важно. Это понимают на самом верху — например, в ходе последнего Послания Федеральному собранию Владимир Путин особо подчеркнул, что телемедицина должна предоставить населению возможность получать консультации специалистов ведущих федеральных и региональных медицинских организаций. И вот проект закона, регулирующего применение информационно-телекоммуникационных технологий в здравоохранении и предусматривающий в том числе возможность дистанционного оказания медицинских услуг и мониторинга состояния здоровья, принят Госдумой в первом чтении.

«Суть телемедицины — в оперативном взаимодействии между врачом и пациентом. Ее внедрение должно позволить пациентам получить оперативную и квалифицированную медицинскую помощь, где бы они ни находились», — отмечает руководитель Центра мониторинга НТР Анна Заборенко, подчеркивая, что в первую очередь речь идет о сельских жителях, больных хроническими заболеваниями и маломобильных гражданах. Кстати, по официальным данным, в нашей

стране не хватает более 30 тысяч врачей, а в некоторых регионах медучреждения укомплектованы кадрами лишь на 60%. При этом текущий уровень развития информационных технологий в области охраны здоровья уже сегодня позволяет в ряде случаев удаленно провести диагностику заболевания, скорректировать лечение и контролировать состояние здоровья пациента.

— Законопроект открывает двери применению новейших информационных и телекоммуникационных технологий в здравоохранении и направлен в первую очередь на повышение качества, доступности и комфортности медицинских услуг для граждан. В том числе за счет выписки электронных рецептов, онлайн-записи к врачу, доступа к электронным базам данных. Что, в свою очередь, делает само обращение к врачу более простым и удобным и для жителей отдаленных регионов. Вся история болезни пациента будет доступна в любом медицинском учреждении, даже в случае переезда в другой город. Законопроект предусматривает создание единой государственной информационной системы в сфере здравоохранения. Справки, рецепты, направления на процедуры и прочие документы будут формироваться в электронном виде, что будет удобно и пациенту, и врачу, и работнику аптеки. Благодаря этим нововведениям станет проще планировать распределение лекарств и загрузку процедурных кабинетов, — рассказывает министр РФ по вопросам Открытого правительства Михаил Абызов.

И все же есть в новом документе положения, которые вызывают у экспертов серьезные опасения. В первую очередь речь идет, конечно, о статье, предполагающей, что информация обо всех пациентах нашей страны, независимо от того, лечатся они в государственных клиниках или частных, теперь должна будет отправляться в единую государственную базу данных. То есть все медицинские учреждения, включая государственные, а с 2019 года и частные, обязаны будут интегрировать с помощью электронных средств связи все данные о проводимых услугах, включая поставленный диагноз, протокол врача и СНИЛС пациента, в Единую государственную информационную медицинскую систему. Иными словами, в ней будут храниться и диагнозы россиян, и то, какое им проводится лечение, и особенности течения их заболеваний — в общем, все-все-все, что представляет собой врачебную тайну.

По идее, тайна должна оставаться тайной, однако мы знаем немало примеров, когда даже самые засекреченные базы данных вскрывались хакерами. Буквально недавно хакерская атака накрыла больницы Лондона — и врачи, и пациенты оказались в полной растерянности. Вскрывались даже базы данных ЦРУ, даже базы данных о клиентах банков. В России же с защитой информации дела обстоят, увы, плачевно. До сих пор не представляет никакого труда купить милицейские базы данных — и «пробить» адреса и телефоны любых людей. И очень сомнительно, что наше государство потратит какие-то миллиарды рублей на то, чтобы сделать базу данных о наших пациентах какой-то суперзащищенной. Разумеется, этого не будет, а значит, нет никакой гарантии, что информация о вашем диагнозе или о диагнозе ваших близких не попадет в открытый доступ.

В первую очередь это, конечно, грозит известным и публичным персонам. Представьте, что будет, если вдруг станет известно, что какой-то важный государственный деятель неизлечимо болен. Кстати, в свое время беда приключилась с бывшим президентом Франции Франсуа Миттераном. Он многие годы страдал онкологией, однако держал свой диагноз в тайне. Лишь после его смерти стало известно, что он болел раком простаты все четырнадцать лет своего президентства и в последние месяцы был практически недееспособен. Но представьте, что было бы, если бы кто-то предал его диагноз огласке? И что будет, если о диагнозах наших политиков и селебрити узнает широкая общественность?

Впрочем, закон коснется, разумеется, не только известных персон, но и рядовых граждан. Заинтересованность в том, чтобы знать состояние вашего здоровья изнутри, может быть у кого угодно. Да хотя бы у вашего начальника. Положим, он раскопает, что у вас в анамнезе есть растяжение связок, вследствие чего вам рекомендовано каждые пару месяцев проходить курс лечебной гимнастики. «А оно мне надо, отпускать работника так часто?» — подумает шеф и найдет повод потихоньку от вас избавиться. А если ваше здоровье или здоровье ваших детей требует еще более пристального внимания? В общем, у очень многих людей могут начаться проблемы на работе. И не только. Ведь путей использовать данные о вашем здоровье в недобросовестных целях, согласитесь, масса. К примеру, получив данные о болячках пенсионеров и инвалидов на участке, активизируются мошенники, которые будут звонить им и предлагать лечение их ревматизма или

ишемической болезни с помощью новейших чудо-таблеток. Это происходит, конечно, и сейчас — но с единой базой данных наверняка приобретет еще более серьезные масштабы.

— Конечно, в такой редакции законопроект несет в себе риски для врачебной тайны, которая гарантирована всем пациентам нашей страны, — говорит глава Лиги защиты прав пациентов Александр Саверский. — Я считаю, что власти должны хорошенько подумать над механизмами, которые бы обеспечили ее сохранность и гарантировали бы, что информация о диагнозах и способах лечения пациентов не окажется в широком доступе. Конечно, я понимаю, что утечки будут в любом случае, да и уже сейчас базу данных поликлиники обо всех инвалидах и пенсионерах купить довольно просто, что журналисты проделывали не раз. Однако в существующем виде новый законопроект может значительно ухудшить ситуацию в этой области.

Член правления Ассоциации частных клиник Москвы Филипп Миронович подчеркивает, что в статье есть пункт, согласно которому любой уполномоченный представитель пациента, включая его самого, может затребовать все хранящиеся в Единой государственной информационной медицинской системе данные. «Представителем пациента, между прочим, может называться любой оператор. Наши люди не очень-то задумываются, когда соглашаются с условиями пользовательских соглашений в том или ином мобильном приложении, многие эти соглашения просто не читают. Между тем, соглашаясь с политикой конфиденциальности или правилами обслуживания, вы нередко наделяете оператора (то или иное юридическое лицо, например, оператора сотовой связи или телемедицинской услуги) правом пользоваться вашей личной информацией в своих целях. А дальше это юрлицо может обратиться к Единой информсистеме и запросить о вас все данные, даже не ставя вас, пациента, в курс дела. Это дает возможность различным сервисам с клиентскими базами собрать пациентские данные, минуя физические и юридические лица, которые их создавали и несут за них ответственность. Допустим, врач собрал анамнез, подписал протокол лечения, о котором, по сути, должен знать только он и пациент. С другой стороны, врач обязан направить эту документацию в третью систему, ему не подконтрольную, но при этом нести ответственность за сохранность врачебной тайны. Иными словами, с 1 января 2019 года врачебная тайна перестанет в России существовать как понятие.

Как сообщили в Минздраве России, в Российской Федерации действуют нормативные документы, обеспечивающие безопасность персональных данных граждан. «Данные требования в полной мере учитываются при работе по данному законопроекту. Вопрос защиты медицинских данных является одним из ключевых и внимательно прорабатывается экспертами в рамках обсуждения законопроекта. Необходимо отметить, что персональные медицинские данные в электронном виде обрабатываются и хранятся в информационных системах медицинской организации, где пациенту оказывалась помощь (аналогично тому, как это сейчас происходит с бумажными медицинскими картами). Передача данных о пациенте в иные информационные системы происходит только при получении согласия гражданина в соответствии с законодательством о персональных данных, при этом обмен сведениями осуществляется по защищенным каналам связи. Важной чертой обработки информации в медицинских информационных системах является разграничение прав доступа к информации. Так, например, к персональным данным пациента имеет доступ только лечащий врач. Кроме того, медицинские информационные системы обеспечивают учет и регистрацию всех действий пользователей», — сказали «МК» в Минздраве.

Из комментария Минздрава следует, что он не возражает против того, чтобы граждане давали свое личное письменное согласие на передачу любой медицинской информации в единую базу данных. Впрочем, эксперты настаивают на том, что положение об этом необходимо прописать в новом законе. Иначе опасность разглашения врачебной тайны станет более чем реальной. К ОГЛАВЛЕНИЮ

КОМПАНИИ ОБЯЖУТ СООБЩАТЬ ОБ УТЕЧКАХ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ

23/06/17, iz.ru. Операторов персональных данных обяжут сообщать МВД, Роскомнадзору и пользователям о хакерском взломе и любой другой утечке клиентской информации. За умалчивание компании ждет административная ответственность. Соответствующий законопроект подготовлен заместителем председателя комитета Госдумы по информполитике Мариной Мукабеновой.

В Госдуме 22 июня прошло совещание на тему «Законодательное регулирование вопросов взаимодействия уполномоченных госорганов в сфере защиты персональных данных от киберинцидентов: проблемы и перспективы». В нем участвовали представители Роскомнадзора, МВД, Следственного комитета, Сбербанка, Ростелекома, Российской ассоциации электронных ком-му-ни-ка-ций (РАЭК), Регионального общественного центра интернет-технологий (РОЦИТ), Института развития интернета (ИРИ) и многих других организаций.

На заседании обсуждался проект изменений в закон «О персональных данных». Согласно тексту документа, операторы персональных данных в случае утечки таких данных обязаны будут в течение одного дня проинформировать об этом самих пострадавших, Роскомнадзор (надзирает за соблюдением указанного закона) и МВД. Если оператор персональных данных этого не сделает, то для него предусмотрена административная ответственность — штраф до 100 тыс руб.

Сегодня операторы данных не обязаны разглашать информацию об их утечке. По словам гендиректора компании InfoWatch Алексея Нагорного, каждая утечка — это удар по репутации компании, и о подобных инцидентах им проще умолчать.

— Что касается штрафных санкций, то 100 тысяч — это небольшие деньги, и некоторым компаниям будет проще умолчать, чем допускать репутационные риски, — объясняет Алексей Нагорный. — С другой стороны, пока не понятно, как будет рассчитываться штраф. Это сумма за каждого пострадавшего — либо за неуведомление об утечке в целом, не важно, какого объема она была. Если за каждую запись, то это существенный штраф, компании задумаются не только об уведомлениях, но и об усилении защиты данных. Если нет, то, с высокой долей вероятности, компании, располагающие большими массивами данных, никого не будут уведомлять.

Глава РАЭК Сергей Плуготаренко рассказал, что его ассоциация разделяет обеспокоенность государства в связи с утечками персональных данных граждан.

— Необходимость уведомления органа внутренних дел полагаем излишней, — добавил Плуготаренко. — Если информацию получит Роскомнадзор, и в инциденте будут признаки преступления, служба самостоятельно может направить обращение в органы МВД. Также следует увеличить срок уведомления — сейчас предлагается один

рабочий день. Закон «О персональных данных» по другим ситуациям предусматривает более длительные сроки.

По данным InfoWatch, в России количество утечек конфиденциальной информации в 2016 году выросло на 80% по сравнению с предыдущим годом. Всего в прошлом году зафиксировано около 1556 случаев утечек данных из компаний и организаций. Около 93% были связаны с кражей персональной и платежной информации.

К ОГЛАВЛЕНИЮ

Опыт и решения компаний

В ПОЧТА БАНКЕ ВНЕДРИЛИ БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ

24/05/17, oxpaha.ru. Процесс идентификации сотрудников Почта Банка теперь, кроме введения традиционных логина и пароля, включает фотографирование и анализ изображения с помощью биометрического оборудования. Для повышения уровня безопасности сотрудников крупного российского банка и предотвращения возможностей хищения конфиденциальной и секретной информации, руководство этого финансово-кредитного учреждения приняло решение внедрить систему биометрических проверок и контроля лиц, имеющих учетные записи в электронной системе Почта Банка.

Система биометрического распознавания сотрудников и агентов банка сравнивает эталонное изображение, сделанное во время первоначального входа в систему, с новым, и только после подтверждения личности гражданина, предоставляет ему доступ к определенным базам данных. В настоящее время система биометрической идентификации затронула более 50 тысяч сотрудников, а также начинает работать с клиентами этого финансово-кредитного учреждения. Ежедневно система идентификации обрабатывает сотни тысяч фотографий сотрудников, также агентов и клиентов Почта Банка, сравнивая их с фотографиями, хранящимися в базе данных о банковских мошенниках.

По словам Павла Гурина, члена правления Почта Банка, на сегодняшний день эта финансово-кредитная организация является первой и единственной в России, внедрившей систему биометрической идентификации лиц. Подобная система должна препятствовать проникновению в банк посторонних лиц, пытающихся похитить важную конфиденциальную и секретную информацию, а также надежно защитит вклады клиентов Почта Банка. К ОГЛАВЛЕНИЮ

ОАО «РЖД» НАМЕРЕНО РАЗВИВАТЬ ИНФОРМАЦИОННЫЕ СИСТЕМЫ НА ОСНОВЕ РЕШЕНИЙ «ИНТЕРНЕТА ВЕЩЕЙ» И BIGDATA

01/06/17, gudok.ru. В рамках Петербургского международного экономического форума «Российские железные дороги» и Фонд развития интернет-инициатив подписали соглашение о сотрудничестве в области информационных технологий. Подписи под документом поставили президент ОАО «РЖД» Олег Белозёров и президент ФРИИ Кирилл Варламов, сообщает пресс-центр «Российских железных дорог».

Сотрудничество компаний будет развиваться в области модернизации и развития информационных систем ОАО «РЖД», в том числе за счет использования технологий IoT («Интернет Вещей»), BigData («Большие данные»), развития программ поддержки новых технологических проектов и стартапов на железнодорожном транспорте.

Внедрение технологий «Интернета Вещей» (сбор и передачи информации о состоянии объектов без участия человека для последующей автоматической обработки) позволит осуществлять автоматическую диагностику и контроль параметров подвижного состава и объектов инфраструктуры в режиме онлайн. Использование высокотехнологичных IT-решений в области «Больших данных» (технология скоростной обработки огромных объёмов данных о состоянии инфраструктуры и подвижного состава) позволит совершенствовать системы управления железнодорожной инфраструктурой, перевозками, а также позволит повысить эффективность технологических процессов ОАО «РЖД» и сократить издержки. К ОГЛАВЛЕНИЮ

ТИНЬКОФФ БАНК СКОРО ПОЛНОСТЬЮ ПЕРЕЙДЕТ НА СОБСТВЕННУЮ СИСТЕМУ ДЛЯ РАСПОЗНАВАНИЯ ГОЛОСА КЛИЕНТОВ

02/06/17, banki.ru. В ближайшем будущем Тинькофф Банк полностью перейдет с внешней на собственную систему распознавания голоса клиентов, сообщил председатель правления кредитной организации Оливер Хьюз. Для этого уже собрано 5 млн голосовых слепков,

уточнил банкир на панельной сессии «Эволюция или революция: как технологии изменят мировой финансовый сектор?» ПМЭФ-2017.

Хьюз заметил, что Тинькофф Банк был первым банком в мире, внедрившим решение по распознаванию голоса в режиме онлайн совместно с компанией NICE Systems, которая специализируется на технологиях записи телефонных разговоров, обеспечении безопасности личных данных и системах видеонаблюдения. Это произошло еще летом 2014 года.

«Эта система оказалась интересной, но достаточно ограниченной и дорогой, негибкой. Соответственно, мы написали свою систему распознавания голоса. Она уже работает в фоновом режиме, на базе machine learning, это самообучающаяся система,— прокомментировал Хьюз. — Мы уже собрали пять миллионов голосовых слепков, и в скором времени переключим все (распознавание голоса) на свою собственную систему». К ОГЛАВЛЕНИЮ

АЭРОПОРТЫ ОСВАИВАЮТ ТЕХНОЛОГИЮ РАСПОЗНАВАНИЯ ЛИЦ

05/06/17, gazeta.ru. Американская авиакомпания в этом месяце начнет тестирование технологии распознавания лиц при посадке в самолет — при ее использовании пассажиру не придется показывать свой паспорт или посадочный талон, что сэкономит время проверки. Если эксперимент будет успешным, биометрические сканеры могут появиться во всех аэропортах США. В чем минусы данной технологии и какие еще страны также обратили внимание на ее потенциал — в материале «Газеты.Ru».

Путешествие самолетом всегда было сопряжено с определенными трудностями. Кроме предварительного получения визы или разрешения на въезд необходимо пройти несколько кордонов безопасности и на каждом предъявить документы, удостоверяющие личность.

К счастью, уже не за горами использование технологии распознавания лиц, которая, при корректной работе, должна сильно упростить путь пассажиров от дверей аэропорта до своего места на борту.

Проверка может обернуться слежкой

Небольшая американская авиакомпания JetBlue Airways объявила о намерении заменить традиционные посадочные талоны новейшей технологией. Эксперимент стартует 12 июня и продлится от 45 до 90 дней в зависимости от своей успешности.

Предполагается, что она будет работать следующим образом: пассажир становится в очередь на посадку, после чего его лицо сканируется и сравнивается с фотографией из базы данных Службы таможенного и пограничного контроля США.

В случае совпадения снимков пассажир сможет пройти на борт без предъявления билета или паспорта.

Представитель JetBlue Джоанна Герати заявила, что технология распознавания лиц должна упростить процедуру посадки в самолет и тем самым снизить напряжение от многочисленных проверок безопасности. «Самопосадка поможет избавиться от бумажных талонов и ручной проверки паспорта. Просто посмотрите в камеру — и вы можете идти дальше», — рассказывает Герати.

В перспективе эта технология будет работать на всей территории Соединенных штатов Америки и применяться ко всем пассажирам, а не только к иностранцам.

JetBlue полагает, что кроме экономии времени распознавание лиц поможет усилить безопасность в аэропорту. Однако активисты движения, выступающего за соблюдение гражданских прав на свободу частной жизни, считают, что такие эксперименты представляют собой угрозу приватности.

Джереми Скотт из некоммерческой организации Electronic Privacy Information Center полагает, что внедрение этой технологии не предусматривает механизмов, ограничивающих наблюдение за людьми.

«Будет ли эта программа использована для удостоверения личности человека или же станет еще одним тайным инструментом слежки, рассматривая каждого пассажира как потенциального преступника? Этому эксперименту необходима полная прозрачность, так как распознавание лиц может применяться как незаконный надзор, нарушающий наши конституционные права», — говорит Скотт.

Технология хороша, но ненадежна

Другая американская авикомпания — Delta Air Lines — тоже собирается использовать распознавание лиц для упрощения

аэропортовой рутины. На этот раз биометрический сканер будет применяться на стойках сдачи багажа.

После печати ярлыка, который прикрепляется на сумку или чемодан, пассажира пригласят к автомату, оборудованному технологией распознавания лица, для сканирования и сверки с фотографией в документах.

Delta вложила в автоматизированную стойку регистрации багажа $600 тыс. На эти средства в Международном аэропорту Миннеаполис/Сент-Пол этим летом будут установлены четыре подобных автомата.

Старший вице-президент Delta Гарет Джойс считает, что эта инвестиция поможет сэкономить время пассажиров. «Мы видим будущее, в котором сотрудники Delta будут освобождены от рутины, чтобы уделять клиентам больше времени и обеспечивать более качественный сервис», — заявил Джойс.

Кроме того, технологией заинтересовалась и Австралия. К 2020 году страна планирует ввести биометрическую проверку пассажиров во всех австралийских аэропортах, включая сканирование отпечатков пальцев и лица.

Несмотря на то что единой биометрической системы пока нет, потенциально в базу данных можно загрузить всю информацию о путешественниках, включая сведения о билетах, туристическую историю, возможные судимости и пр.

В будущем искусственный интеллект на основе этих данных сможет определять, представляет пассажир угрозу или нет. Испытания системы пройдут в аэропорту Канберры, столицы Австралии. Целью проекта является автоматизация проверки 90% пассажиропотока.

Свои испытания в этой области проводят финская авиакомпания Finnair, голландская KLM, а также международный аэропорт Париж – Шарль-де-Голль. В некоторых случаях система распознавания лиц будет только дублировать действия сотрудников службы безопасности, так как на настоящий момент она не показывает 100% результата и иногда неточна.

Биометрические показатели более защищенные, говорит руководитель отдела технического маркетинга ESET Russia Алексей Оськин, при этом автоматизация в данной сфере направлена на уменьшение времени обработки и, следовательно, очередей на контроле безопасности пассажиров.

«Сложность внедрения технологии определяется различными условиями, но решающим фактором всегда является стоимость. Если мы не ограничены в финансах, внедрять можно все что угодно», — считает Оськин.

Эксперт заявил, что, хотя теоретически подделать паспорт проще, чем отпечатки пальцев и узор радужки глаза, в сфере безопасности лучше всего использовать комплексный, многоуровневый подход с несколькими ступенями авторизации. К ОГЛАВЛЕНИЮ

РЖД И «ЛАБОРАТОРИЯ КАСПЕРСКОГО» БУДУТ ВМЕСТЕ БОРОТЬСЯ С КИБЕРУГРОЗАМИ

07/06/17, morvesti.ru. ОАО «Российские железные дороги» (РЖД) и «Лаборатория Касперского» в рамках работы бизнес-форума «Стратегическое партнерство 1520» заключили соглашение о сотрудничестве в сфере информационной безопасности.

Соглашение по информационной безопасности включает в себя антивирусную защиту, тестирование систем и средств на предмет киберзащищенности, защиту информационных систем от проникновения, мошенничества и утечек информации, использование решений для защиты индустриальных сетей, информирование об актуальных и сложных угрозах.

Сотрудничество двух компаний должно повысить уровень защищенности РЖД от существующих и потенциальных кибернетических угроз, а также снизить риски, возникающие в связи с увеличением степени цифровизации бизнеса.

Как сообщалось ранее, РЖД оказались в числе компаний, чьи компьютеры затронула глобальная хакерская атака 12 мая. Президент РЖД Олег Белозеров тогда сообщил, что вирусная атака WannaCry затронула системы РЖД, но никак не повлияла на работу сервисов компании.

Также хакерскому нападению подверглись системы МЧС, МВД, Сбербанка, «Вымпелкома» и «Мегафона». В этот день, по оценке «Лаборатории Касперского», было зафиксировано 45 тыс. попыток атак в 74 странах мира, причем основная часть пришлась на Россию. К ОГЛАВЛЕНИЮ

GOOGLE ПООБЕЩАЛ ПЕРЕСТАТЬ СКАНИРОВАТЬ ПОЧТУ РОБОТАМИ

26/06/17, d-russia.ru. Компания Google решила прекратить практику сканирования писем в почтовом сервисе Gmail для показа пользователям персонализированной рекламы, сообщила в корпоративном блоге старший вице-президент компании Диана Грин (Diane Greene).

«Содержание писем пользователей Gmail не будет использоваться или сканироваться для любой персонализации рекламы после этих изменений», — написала она.

На сегодняшний день, по данным Google, сервисом пользуются 1,2 миллиарда человек.

Отныне рекламные объявления для пользователей Gmail будут персонализироваться аналогично другим продуктам Google – на основе пользовательских настроек. «Пользователи могут изменять эти настройки в любое время, в том числе отключать персонализацию рекламы», — пишет вице-президент Google.

Ранее компания уже прекратила персонализировать рекламу на основе данных из корпоративного сервиса G Suite's Gmail (почта, работа с документами, хранение данных за абонентскую плату, имеет 3 миллиона корпоративных пользователей, по данным компании). Теперь сканирование переписки автоматизированными системами Google обещает прекратить и для бесплатной версии Gmail.

Как писал D-Russia.ru, в 2015 году тему нарушения тайны переписки со стороны компании Google поднял Антон Бурков, завкафедрой европейского права Гуманитарного университета в Екатеринбурге. Он подал иск в суд, где обвинил Google в том, что его почта, как и почта его партнёров по переписке, сканируется роботами Google. По мнению истца, это нарушает защищаемую конституцией тайну переписки.

Дело слушалось в апреле 2015 года в Замоскворецком районном суде Москвы, который вынес решение в пользу ответчика – ООО «Гугл», сочтя, что истец должен адресовать претензии самой компании Google, а не её российской дочке.

Бурков подал апелляцию на это решение, и 16 сентября 2015 года Мосгорсуд её удовлетворил, отменив решение предыдущей инстанции и постановив взыскать с ответчика 50 тысяч рублей.

«Наши автоматизированные системы сканируют почту, чтобы предотвратить появление спама и выявить вредоносные программы. Такие же системы используется и для показа релевантных рекламных объявлений. Ни один человек не вовлечен в этот процесс», — заявила пресс-служба ООО «Гугл».

Однако Мосгорсуд решил, что сканирование почты роботом нарушило неимущественное право истца. «Поскольку каждому гражданину гарантируется тайна как переписки, так и телефонных разговоров и другой корреспонденции, а потому мониторинг электронной корреспонденции может быть расценен как посягательства на конституционные права граждан», — говорилось в решении Мосгорсуда. К ОГЛАВЛЕНИЮ

ПО и технические новинки

ЯНДЕКС.БРАУЗЕР ПРЕДУПРЕДИТ О ПЕРЕХВАТЕ ЗАШИФРОВАННЫХ ДАННЫХ

12/05/17, yandex.ru. «Яндекс» объявил о том, что «Яндекс.Браузер» научился предупреждать о перехвате зашифрованных данных. Он показывает сообщение об опасности, если понимает, что в руки злоумышленников могут попасть пароли, платёжные данные и другая информация пользователя, которая передаётся по протоколу HTTPS. Браузер с такой функцией появился на рынке впервые.

Прежде чем передать зашифрованные данные, любой браузер запрашивает у сайта цифровой сертификат и проверяет его надёжность. Чаще всего для проверки используются данные о сертификатах, которые хранятся в операционной системе компьютера. Злоумышленники добавляют к этим данным свои — чтобы браузер доверял их сертификатам и передавал конфиденциальную информацию. Благодаря этому они и перехватывают трафик. Обычно данные злоумышленников попадают в компьютер незаметно для пользователя — например, вместе с какой-нибудь программой, скачанной с сомнительного сайта.

По данным исследований, от перехвата HTTPS-трафика страдает от 4% до 11% пользователей. Чтобы выявить «прослушку», «Яндекс.Браузер» проводит дополнительную проверку сертификатов, которые операционная система компьютера посчитала надёжными. Для этого используются данные нескольких авторитетных производителей операционных систем — эту информацию злоумышленники изменять не могут. Если надёжность сертификата не подтверждается, пользователь получает сигнал о том, что трафик может «прослушиваться» — поэтому лучше обратиться к специалисту, чтобы удалить данные злоумышленников и программу, которая их занесла.

Предупреждения о перехвате зашифрованных данных работают в версии «Яндекс.Браузера» для Windows. Этот механизм защиты стал частью технологии Protect, которая проверяет страницы и файлы на

вирусы, предупреждает о платных мобильных подписках, бережёт пароли и данные банковских карт.

«Яндекс.Браузер» был запущен в 2012 г. Сейчас это второй по популярности компьютерный браузер у россиян и первый среди непредустановленных браузеров на мобильных устройствах. В апреле 2017 г. его дневная аудитория составила 20 млн пользователей, 7,5 млн из них пользуются мобильной версией. По данным за апрель, доля «Яндекс.Браузера» в России составляет 21% на компьютерах и 5% на мобильных устройствах. К ОГЛАВЛЕНИЮ

«АЛАДДИН Р. Д.» РАЗРАБОТАЛА РЕШЕНИЕ ПО ЗАЩИТЕ БАЗ ДАННЫХ, РАБОТАЮЩИХ ПОД СУБД ORACLE, MS SQL, TIBERO И POSTGRESQL

26/05/17, anews.com. Российская компания «Аладдин Р. Д.», специализирующаяся на информационной безопасности, разработала решение по защите баз данных, работающих под СУБД Oracle, MS SQL, Tibero (корейский аналог Oracle) и PostgreSQL. «Мы создали технологию изоляции данных, которые обрабатывают эти СУБД, от самих СУБД, — говорит гендиректор компании-разработчика Сергей Груздев. — В итоге мы на них работаем, но что хранится в базах, СУБД не видят, и данные не могут утечь. Мы научились корректно вписываться в продукт, перехватывать нужные нам функции».

По словам Груздева, идея решения родилась от осознания того, что широко распространенные в России СУБД зарубежных вендоров быстро заместить на какие-либо отечественные продукты и перенести на них все приложения и данные, просто нереально. «Но если мы не можем заменить саму СУБД, то мы можем нырнуть внутрь и заменить встроенные средства защиты, американской криптографии», — рассуждает он.

В «Аладдине» уверены, что данное решение поможет многим отечественным организациям привести их информационные системы, в том числе работающие с персональными данными, в соответствие с требованиями российского законодательства.

По мнению Груздева, разработка его компании прямых технологических аналогов в мире не имеет. «Наверное просто никто не ставил перед собой задачи цифровой изоляции обрабатываемых данных от самой СУБД», — полагает он.

Новое решение сейчас находится на сертификации в ФСБ по двум младшим классам криптозащиты (всего их шесть) — КС1 и КС2, а до конца 2017 г. компания намерена поднять класс сертификации до КС3.

В «Аладдине» заверяют, что их решение уже прошло пилотную апробацию в ряде проектов, преимущественно банковских, но конкретных клиентов назвать CNews оказались не готовы, из-за отсутствия разрешений со стороны последних.

В разговоре с CNews, Сергей Груздев рассказал, что многие наработки и алгоритмы для нового решения в компании уже были созданы ранее для обезличивания персональных данных. Для решения такой задачи не нужно было защищать сами данные, а достаточно было разрушить некоторые связи между ними. «Нельзя же все шифровать, произойдет деградация производительности, — поясняет Груздев. — Достаточно устранить понимание, о ком именно эти конкретные данные.

Что касается отношения к новой разработке для СУБД со стороны вендоров этих СУБД, то, в частности в российском Oracle к ней, как можно заключить со слов Груздева, изначально отнеслись с энтузиазмом — она может помочь компании не лишиться клиентов из-за политики импортозамещения, но позже все же охарактеризовали «Алладдин» отчасти как своего конкурента. К ОГЛАВЛЕНИЮ

КАЖДАЯ ПЯТАЯ IT-СИСТЕМА УЯЗВИМА ИЗ-ЗА СТАРОГО СОФТА

14/06/17, kommersant.ru. IT-системы российских промышленных компаний, госструктур, банков и телекоммуникационных операторов в 20% случаев содержат критически опасные уязвимости, связанные с необновленным ПО, показало исследование Positive Technologies. При этом обновления, которые игнорируются компаниями, зачастую выпущены уже много лет назад. Получить полный контроль над критически важными ресурсами компаний от лица нарушителя даже с минимальными знаниями удалось более чем в половине проведенных тестов.

IT-системы крупных российских структур, среди которых промышленные компании, госорганы, банки и телекоммуникационные операторы, в 40% случаев содержат критически опасные уязвимости,

связанные с недостатками конфигурации, следует из отчета Positive Technologies за 2016 год. 27% систем обладают критически опасными уязвимостями, связанными с ошибками в коде веб-приложений, 20% — уязвимостями из-за неустановки обновлений софта.

При этом информация о самой старой из обнаруженных уязвимостей, а также обновление, решающее проблему с ней, были опубликованы более 17 лет назад. «Уязвимость связана с тем, что DNS-сервер поддерживает рекурсию запросов. В результате эксплуатации данной уязвимости злоумышленник может проводить атаки на отказ в обслуживании»,— утверждают авторы отчета. Средний возраст наиболее устаревших неустановленных обновлений по системам, где такие уязвимости были обнаружены, составляет девять лет, следует из отчета.

В ходе тестов, проведенных Positive Technologies в 2016 году, выяснилось, что в 55% случаев внешний нарушитель, обладающий минимальными знаниями и довольно низкой квалификацией, способен преодолеть периметр и получить доступ к ресурсам в локальной сети компании. Для этого в среднем необходимо найти только две уязвимости в используемом компанией ПО.

«В 77% работ сетевой периметр удалось преодолеть из-за уязвимостей веб-приложений, а в 23% — из-за уязвимостей, связанных с использованием словарных паролей»,— рассказали в компании. В результате более чем в половине случаев от лица внешнего нарушителя удалось получить полный контроль над критически важными ресурсами компаний, такими как система Active Directory, СУБД, ERP-система и др.

В целом объекты критической инфраструктуры, к которой, согласно законопроекту, рассматриваемому Госдумой, предлагается отнести IT-системы банков, телеком-операторов и промышленных предприятий, в 2016 году подверглись 70 млн кибератак, сообщал в январе представитель ФСБ. При этом объем средств, похищенных хакерами только из российских банков, по данным Group-IB, составил за тот же период 5,53 млрд руб. В банке данных угроз безопасности информации, который с марта 2015 года ведет Федеральная служба по техническому и экспортному контролю, на данный момент находится информация о 16,5 тыс. уязвимостей в ПО, используемом при создании государственных IT-систем и автоматизированных систем управления

производственными и технологическими процессами критически важных объектов.

Системное или прикладное ПО без необходимых обновлений стоит примерно в девяти из десяти компаний, уверен руководитель аналитического центра Zecurion Владимир Ульянов. «Причин для этого много. В некоторых компаниях боятся, что после обновления какой-то компонент откажется работать или начнет работать неправильно. Принцип “работает — не трожь” до сих пор одна из главных догм системных администраторов»,— поясняет господин Ульянов. Он добавляет, что большое количество оборудования, разнообразие используемых систем, территориально удаленные филиалы и устаревшие системы также приводят к тому, что какие-то компоненты не обслуживаются IT-специалистами должным образом.

К ОГЛАВЛЕНИЮ

ЗА РАЗРАБОТКУ «НАЦИОНАЛЬНОЙ БИОМЕТРИЧЕСКОЙ ПЛАТФОРМЫ» «РТ ЛАБС» ПОЛУЧИТ ПОЧТИ 248 МЛН РУБ

20/06/17, d-russia.ru. «Ростелеком» опубликовал информацию о работах над «национальной биометрической платформой», которые будет выполнять его «дочка» «РТ Лабс». Стоимость работ оценена более чем в 247,6 миллиона рублей. Работы должны быть завершены не позднее 22 декабря 2017 года.

Напомним, в начале июня «Ростелеком» объявил о планах создания технологии, именуемой национальной биометрической платформой (НБП), которая «позволит банкам осуществлять биометрическую идентификацию клиентов-физических лиц с использованием ЕСИА для дистанционного открытия счетов и оказания иных банковских услуг».

Как следует из технического задания, «объектом автоматизации является деятельность по организации и проведению удаленной идентификации пользователей в кредитных организациях (КО) и/или инфраструктуре электронного правительства посредством сличения биометрических данных».

Чтобы получить возможность прохождения удалённой идентификации через «дистанционные каналы обслуживания» (онлайн и через мобильные приложения), гражданин должен хотя бы единожды

лично обратиться в КО, имеющую право на биометрическую регистрацию. Список таких организаций составляет Банк России.

Биометрическая регистрация сопровождается идентификацией гражданина в ЕСИА. «Биометрические образцы» (см. ниже) передаются в НБП с помощью Единой системы межведомственного информационного взаимодействия (СМЭВ). Также в подсистему хранения данных НБП отправляется дополнительная небиометрическая информация, связанная с идентификатором гражданина в ЕСИА.

Процедура удаленной идентификации по «биометрическим образцам» включает последовательное прохождение аутентификации – сначала в ЕСИА по логину/паролю, потом посредством НБП.

Если гражданин решает отозвать своё согласие на обработку относящихся к нему персональных данных, все относящиеся к нему «биометрические шаблоны», находящиеся в НБП, помечаются как неактивные. С ними в дальнейшем не производится никаких действий. Однако шаблоны сохраняются. Они не передаются какой-либо второй стороне, за исключением случаев, предусмотренных законодательством РФ.

Техническая сторона дела в 59-страничном ТЗ отражения не нашла. Непонятно, как именно «Ростелеком» намерен идентифицировать граждан: то ли по радужной оболочке глаза, то ли по ладонному рисунку вен, то ли по трёхмерному изображению лица, то ли по отпечатку пальца, то ли как-либо ещё – скажем, по «поведенческим характеристикам индивида», упомянутым в ТЗ.

Вместо этого документ оперирует тремя десятками взаимосвязанных общих терминов вроде «биометрического шаблона», «биометрического образца» (определяется как «аналоговое или цифровое представление биометрических характеристик») и пр. В этих терминах можно описать любую биометрическую технологию, от примитивной антропометрии до анализа ДНК.

Аутентификация человека, по замыслу «Ростелекома», проводится удалённо (в этом и состоит смысл НБП): либо через веб-интерфейс, либо в мобильном приложении. Идентифицируемый субъект передаёт НБП «биометрическую пробу» (этот термин «Ростелеком» определяет так: «биометрические признаки, введённые в алгоритм для использования в качестве объекта сравнения с биометрическим контрольным шаблоном»; иными словами, данные, полученные неким приспособлением, снимающим с человека только

ему присущие биометрические признаки, привычный пример – сканер отпечатка пальца в смартфоне). «Биометрическая проба» уходит в удалённую базу шаблонов для сравнения с образцом, и если сравнение удачно, человек получает положенные ему банковские услуги. Или, что тоже допустимый вариант применения НБП, его идентифицируют с какой-либо иной целью.

Ответственность за достоверность идентификации «Ростелеком» на себя не берёт, он делит её с правительством и Центробанком. «НБП возвращает положительный результат, если степень схожести превышает установленный правительством РФ по согласованию с ЦБ минимальный порог», сказано в техническом задании. К ОГЛАВЛЕНИЮ

УТЕЧКИ ИНФОРМАЦИИ. Инциденты

ОСТОРОЖНО: БЕСПЛАТНЫЕ БИЛЕТЫ В СОЦСЕТЯХ – НОВЫЙ ВИД МОШЕННИЧЕСТВА

05/06/17, hi-tech.mail.ru. В выходные в социальных сетях появилось множество постов «Аэрофлот дарит 2 билета» (или Emirates — это интернациональный вариант), ссылки в которых ведут на сайт с «розыгрышем бесплатных билетов». Hi-Tech Mail.ru решил разобраться, как работает эта «акция».

Во-первых, оказалось, что авиакомпания «Аэрофлот» не имеет к конкурсу никакого отношения. Во-вторых, участие в этой акции повлечет за собой риск заражения вирусами, а также включения нежелательных платных услуг для смартфона. «Акция» уже приобрела глобальный характер, поэтому пользователям рекомендуется быть максимально осторожными и предупредить своих друзей.

Схема обмана

1. Любые «бесплатные» акции в 99% случаев используются мошенниками для обмана и нанесения вреда. Это, наверное, самое главное, что нужно помнить в любой сомнительной ситуации!
2. После нажатия на ссылку «Аэрофлот дарит 2 билета», прежде, чем пользователь попадет на сайт с «бесплатными билетами», его проведут через несколько рекламных сайтов, где он рискует заразиться трояном или другой вредоносной программой.
3. Ссылка ведет не на сайт авиакомпании, а на фишинговый (фальшивый) сайт с поддельным доменным именем и другими признаками обмана. Это первое, что должно насторожить любого пользователя (если сам факт дарения билетов не насторожил).
4. Частью мошеннической схемы является необходимость ее дальнейшего распространения, и здесь пользователь сам поработает на мошенников: чтобы принять участие в розыгрыше ему придется сделать рассылку ссылки своим контактам и сделать репост на своей странице. При этом мошенники могут предложить авторизоваться

через личный аккаунт в сети. В результате, пользователь вовлечет своих друзей в мошенническую схему и добровольно отдаст мошенникам свои данные.

5. После того, как пользователь добровольно поработает на мошенников: подпишется на платные услуги, сделает репост, вовлечет друзей, отдаст свои данные, возможно заразит свой компьютер, посмотрит рекламу, он им больше не нужен и они вежливо попрощаются с ним: «К сожалению, вы не выиграли. Повезет в другой раз».

Потенциальный вред

Если ссылка была открыта на смартфоне, то, вероятно, теперь его хозяин подписан на платные услуги за 30 рублей в день, а настольный компьютер или ноутбук может быть заражен вредоносной программой. Мошенники могут украсть деньги, если на зараженном устройстве используется онлайн банкинг, а также компьютер могут подключить к ботнету для организации автоматических DDoS-атак, рассылки спама, майнинга биткоинов, и проч. Также, хакеры могут украсть информацию, если посчитают ее ценной, ведь в руки мошенников может попасть переписка в мессенджерах, фотографии и другие личные данные, пишут эксперты.

Единственный способ защиты

Если вам «посчастливилось» поучаствовать в этом «розыгрыше» не откладывая просканируйте систему антивирусом, он выявит часть заражений, кроме того, поставьте все обновления безопасности и обновите систему. А главное — никогда и ни за что не принимайте участия в «халявных» розыгрышах и не открывайте подозрительные ссылки — смотрите пункт 0 выше!

Комментарии

Эксперт «Лаборатории Касперского» по веб-контенту Надежда Демидова специально для Hi-Tech Mail.ru разобрала схему работы «конкурса»:

«Мошенники, под видом бесплатной раздачи авиабилетов от крупных авиаперевозчиков, пытались подписать пользователей на платные услуги. Для этого были созданы сайты, на которых

используется символика крупных авиаперевозчиков. В России мошенники использовали бренд «Аэрофлот». Аналогичные атаки наблюдаются якобы от имени компании Emirates и AirFrance. На сайте пользователя поздравляют с выигрышем двух билетов и просят совершить ряд действий, в результате которых жертва подписывается на платную услугу стоимостью 30 рублей в день и распространяет информацию в социальной сети.

На всех мошеннических ресурсах данной схемы размещены ссылки на статистику посещения сайта. Из статистики видно, что атака распространилась очень широко и направлена, в основном, на пользователей смартфонов».

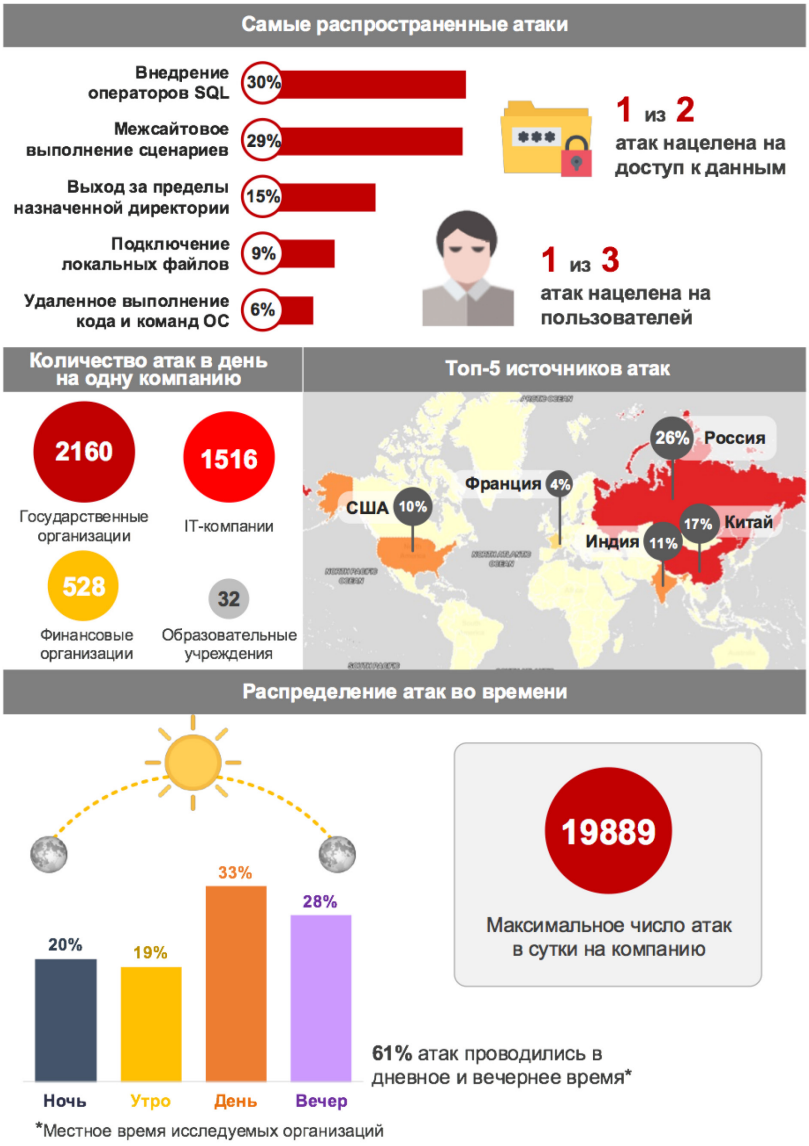
Компания «Аэрофлот» официально предупредила на своей официальной странице в Facebook, что не имеет отношения к «акции» и не разыгрывает бесплатные билеты:

«Друзья, в интернете стремительно распространяется информация от имени 'Аэрофлота' о фейковом конкурсе. Официально заявляем, что наша авиакомпания не имеет отношения к этому розыгрышу. Нам важно ваше доверие, поэтому помните, что актуальные и достоверные сведения о текущих акциях мы размещаем только на нашем сайте www.aeroflot.ru и в официальных сообществах в соцсетях. Будьте внимательны и не участвуйте в сомнительных промоакциях, размещённых на сторонних ресурсах от имени нашей компании». К ОГЛАВЛЕНИЮ

ХАКЕРАМ БОЛЬШЕ ВСЕГО ИНТЕРЕСНЫ ВЕБ-ПРИЛОЖЕНИЯ ГОСУЧРЕЖДЕНИЙ (ИССЛЕДОВАНИЕ)

19/06/17, d-russia.ru. По среднему числу атак на веб-приложения, зарегистрированных в течение одного дня, на первом месте находятся государственные учреждения, за ними следуют IT-компании и финансовые организации. Замыкают рейтинг образовательные учреждения, свидетельствуют данные исследования компании Positive Technologies.

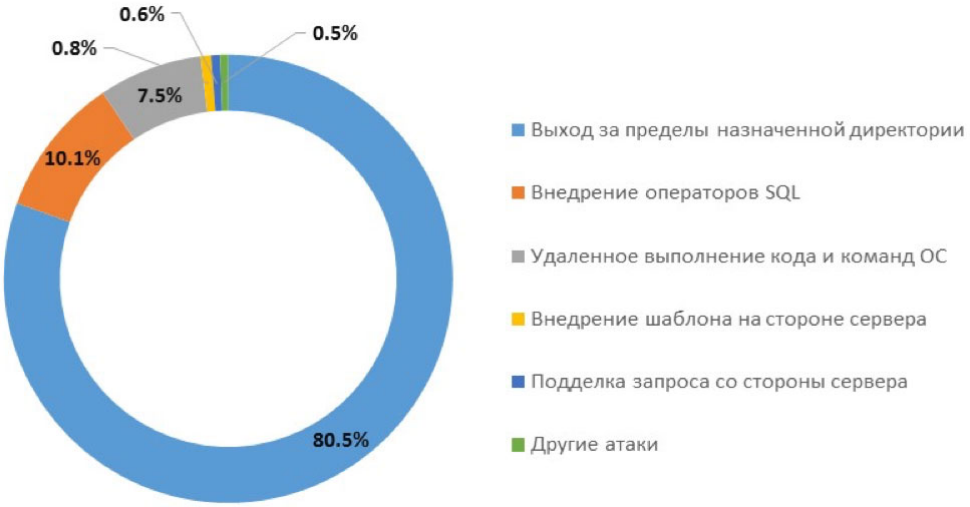
Исследование описывает самые популярные атаки на веб-приложения по результатам пилотных проектов по внедрению межсетевого экрана уровня приложений PT AF за первый квартал 2017 года.



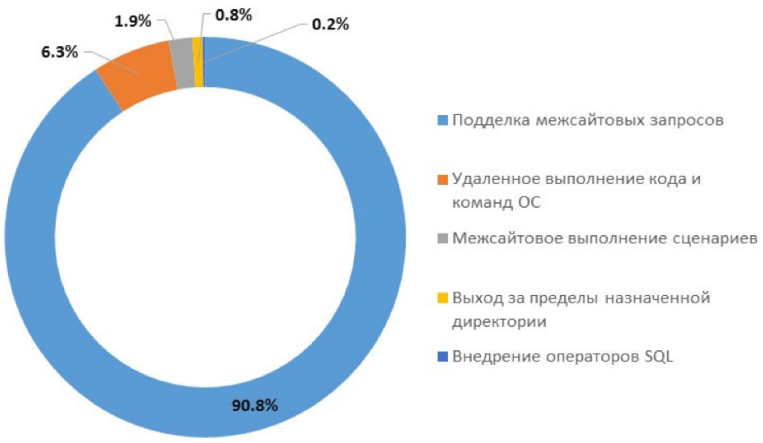
Среднее число зарегистрированных инцидентов информационной безопасности в день в госучреждениях составляет 2160, в IT-компаниях — 1516, в финансовых компаниях — 528 инцидентов и 32 атаки в образовательных учреждениях.

Целью половины атак на государственные учреждения являлся доступ к важным данным. Наиболее ценным информационным ресурсом в государственных учреждениях являются персональные данные, поэтому атаки направлены либо на пользователей приложений, либо на получение доступа к базам, где хранится такая информация.

Задачей злоумышленников при атаке на финансовые организации является кража денежных средств. Большинство атак направлены либо на получение доступа к чувствительным данным, либо на получение контроля над сервером.

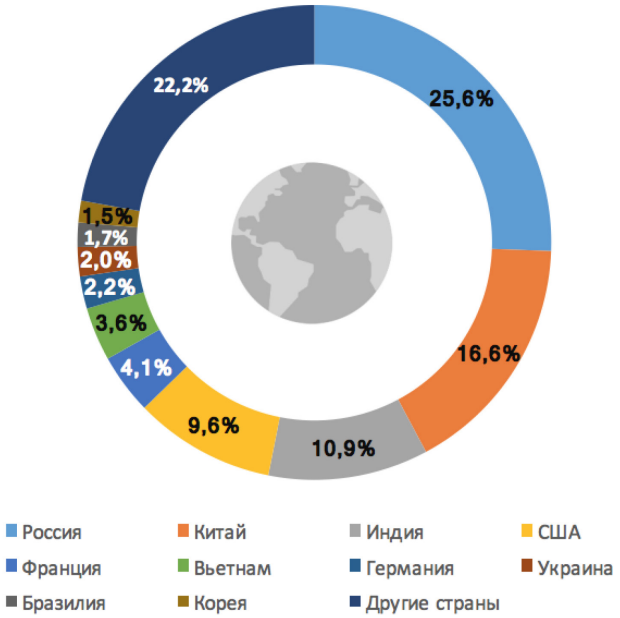


Нарушителями в сфере образования часто являются сами учащиеся, которые стремятся либо получить доступ к данным, например, к экзаменационным материалам, либо изменить текущую информацию, например, результаты экзаменов или стипендиальные списки. Об этом свидетельствуют и результаты предыдущих исследований Positive Technologies.



Наиболее часто в первом квартале 2017 года встречались атаки «Внедрение операторов SQL» и «Межсайтовое выполнение сценариев», каждая составляет примерно треть от общего числа зафиксированных атак. Если атака «Внедрение операторов SQL» используется для получения доступа к чувствительной информации или выполнения команд ОС и дальнейшего проникновения в систему, то атака «Межсайтовое выполнение сценариев» направлена на пользователей приложений. Возможность проведения атак на пользователей вышла на первое место в рейтинге самых распространенных угроз веб-приложений в прошедшем году.

Источниками атак на веб-приложения чаще всего были Китай и Россия. Такое распределение атакующих связано с тем, что большая часть пилотных проектов проводилась для российских компаний.



«Для эффективного обнаружения и предотвращения атак рекомендуется использовать межсетевой экран уровня приложений. Это позволит выявлять и останавливать даже длительные цепочки целевых атак, — говорит аналитик Positive Technologies Екатерина Килюшева. — Важно, чтобы межсетевой экран поддерживал ряд защитных техник, таких как блокировка запроса к веб-приложению или ответа от веб-приложения, маскирование ответа для предотвращения утечек, блокировка сессии пользователя или разрыв соединения, блокировка IP-адреса злоумышленника с помощью встроенных средств, передача IP-адреса внешнему межсетевому экрану либо провайдеру».

Для повышения эффективности работы защитных инструментов должно быть организовано их взаимодействие с внешними системами сбора и анализа событий (SIEM) и оповещение средств защиты от DDoS сетевого уровня. Кроме того, при организации системы защиты необходимо учитывать, в какие промежутки времени наблюдаются всплески активности злоумышленников, и уделять повышенное внимание сетевым аномалиям, выявленным в это время.

К ОГЛАВЛЕНИЮ

ХАКЕРЫ ОРГАНИЗОВАЛИ ФИШИНГОВУЮ РАССЫЛКУ ПОД ВИДОМ ПИСЕМ О ШТРАФАХ ГИБДД

22/06/17, securitylab.ru. Эксперты компании Group-IB сообщили о фишиноговой атаке, в рамках которой ее организаторы рассылали извещения о штрафах ГИБДД под видом уведомлений от портала госуслуг.

Письма выглядят как официальные и не вызывают сомнений у среднестатистических пользователей. К письму прикреплено фото автомобиля- «нарушителя», а в шапке уведомления находится логотип Электронного правительства. Кроме прочего, письмо содержит отметку о проверке на наличие вредоносного ПО и его отсутствии. Особое внимание акцентируется на том, что при оплате штрафа в течение короткого времени возможна скидка в размере 50%.

Как пояснил агентству RNS глава IB-Group Илья Сачков, приклепленный к сообщению файл не является вредоносным, но при переходе по любой активной ссылке в письме пользователь попадает на фишинговый сайт https://mail.ru-attachment-viewer.info/, с помощью которого злоумышленники крадут важные данные пользователей для их последующей монетизации.

За последние несколько месяцев это не первый случай, когда хакеры используют схему вредоносной рассылки от имени госструктур. В феврале нынешнего года о спам-рассылке от его имени предупредил Роскомнадзор, а месяц спустя Следственный комитет РФ сообщил об учащении случаев распространения фальшивых писем якобы от ведомства. К ОГЛАВЛЕНИЮ

ИНДИКАТОРЫ РАЗВИТИЯ. Российская практика

РОСКОМНАДЗОР ОШИБОЧНО ЧАСТИЧНО ЗАБЛОКИРОВАЛ ДОСТУП К ПОРТАЛУ РЖД И ДРУГИМ РЕСУРСАМ

03/06/17, runews24.ru. Причиной массовых перебоев в доступе к сервису через Wi-Fi стала блокировка портала dymoff.space, который использовался для «прикрытия» IP-адресов других популярных ресурсов.

В связи с этим возникли проблемы с доступом в Telegram, «ВКонтакте», «Одноклассники», Pikabu, «Первый канал», Facebook, РЖД и другие сайты.

Владельцы заблокированного сайта, используя уязвимость системы блокировок Роскомнадзора, смогли добавить к блокируемым другие порталы без их ведома. Роскомнадзор проинформирован о существующей проблеме.

«Владелец одного из ресурсов, попавших под блокировки, воспользовался очевидной ошибкой в самой системе блокировок и сделал так, чтобы провайдеры, исполняющие решение РКН о блокировке его ресурса, одновременно блокировали еще кучу сайтов», — сказал сотрудник Фонда борьбы с коррупцией Леонид Волков.

«Практически любой может заблокировать любой ресурс в сети, используя совершенно законное распоряжение Роскомнадзора», — добавил журналист Александр Плющев. К ОГЛАВЛЕНИЮ

ЕЖЕНЕДЕЛЬНО СБЕРБАНК ФИКСИРУЕТ СВЫШЕ 5 ТЫС. АТАК С ПРИМЕНЕНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

04/06/17, securitylab.ru. Каждую неделю Сбербанк фиксирует порядка 5-5,5 тыс. атак с использованием социальной инженерии, когда клиентов обманом вынуждали раскрывать персональные данные, информацию о счетах или переводить средства на неизвестные счета. Об этом сообщил зампред правления банка Станислав Кузнецов на Петербургском экономическом форуме.

По мнению Кузнецова, активность мошенников усиливается и для решения проблемы необходимы изменения в законодательстве.

«Мы почему-то стесняемся говорить о том, что у нас недостаточно сил правоприменения и правоохранения для того, чтобы противодействовать угрозам», - цитируют «Известия» слова зампреда.

Потенциальный ущерб от подобных кибератак составляет порядка 700 млн рублей, отметил Кузнецов.

Ранее стало известно , что до ухода на летние каникулы Госдума может рассмотреть проект поправок в Уголовный Кодекс РФ, предусматривающий ужесточение наказания за хищение электронных денег и кражу средств с банковских карт. К ОГЛАВЛЕНИЮ

GOOGLE И FACEBOOK ИЩУТ СПЕЦИАЛИСТОВ ПО ПЕРЕГОВОРАМ С РОССИЙСКОЙ ВЛАСТЬЮ

09/06/17, cnews.ru. Google и Facebook подыскивают менеджеров по общественной политике, которые взяли бы на себя общение с российскими чиновниками от лица компаний. Кроме того, эти сотрудники должны будут сплотить вокруг Google и Facebook целые коалиции по продвижению свободы интернета.

Google и Facebook ищут сотрудников

Google и Facebook одновременно начали поиски сотрудников, которые помогли бы им вести диалог с российскими властями. Google подыскивает такого работника в московское представительство, Facebook – в варшавское.

Кого ищет Google

Google предлагает будущему сотруднику занять должность менеджера по общественной политике и связям с правительством. В его обязанности будет входить руководство публичными кампаниями, главными темами которых станут ИТ-инновации, открытый интернет, приватность и интеллектуальная собственность. Менеджер будет непосредственно контактировать с российскими чиновниками.

Также от сотрудника ожидается, что он создаст сеть торговых ассоциаций, отраслевых партнеров, некоммерческих организаций и т. д., которая будет поддерживать интересы пользователей и открытый

интернет. В числе прочего менеджеру придется выступать на крупных публичных мероприятиях. Работать сотрудник будет как с московским филиалом, так и с глобальным отделом общественной политики.

На должность могут претендовать лица, имеющие степень бакалавра или эквивалентный опыт работы в политических структурах, правительстве, аналитических центрах, общественных группах или в сфере корпоративной государственной политики. Предпочтение отдается соискателям со знанием технического сектора или ключевых проблем интернета, таких как конфиденциальность данных, свобода слова, доступ и безопасность в сети. Однако компания допускает, что сотрудник уже на месте будет разбираться с техническими вопросами и регулировками. Другие требования: блестящий русский и английский, аналитические и коммуникативные навыки, энтузиазм, умение работать в команде и т. п.

Кто нужен в Facebook

Facebook подыскивает просто менеджера по общественной политике, «связи с правительством» в названии не отражены. Должность локализуется в Варшаве, но работать придется по российскому направлению. Сотрудник будет прорабатывать стратегию компании в сфере общественной политики, отслеживать затрагивающие Facebook изменения в российском законодательстве и регулировках, встречаться с чиновниками и политиками. Как и в случае с Google, менеджер должен выстроить коалицию с другими организациями в поддержку политики компании. Он будет консультировать команды, разрабатывающие новые продукты и сервисы Facebook, по вопросам общественной политики, а также представлять соцсеть на публике, в том числе перед СМИ.

Список требований у Facebook получился длиннее, чем у Google. Диплом базового или более продвинутого уровня здесь является обязательным, также нужен опыт работы в профильной сфере, желательно в чиновничьих и промышленных кругах одновременно. Более того, требуется «знакомство с работой с политиками и чиновниками, в том числе самого высокого уровня».

Кроме того, обязательным является опыт работы спикером в медиа, желательно на радио и телевидении, а также опыт написания и публикации статей, речей и презентаций. Дополнительным преимуществом станет знание российского законодательного процесса

и регуляторной деятельности. Список требований дополняют отличный русский и английский, вера в социальные выгоды интернета и Facebook и т. п.

Google, Facebook и российские правила

В июле 2014 г. в России были приняты поправки к закону «О персональных данных», которые обязывают иностранные компании, имеющие дело с персональными данными россиян, хранить эти данные на территории России. Новые правила вступили в силу с 1 сентября 2015 г. За их выполнением следит Роскомнадзор. Сайты тех компаний, которые не выполняют закон, могут быть заблокированы в России по требованию ведомства. Также компания может быть оштрафована на сумму до 300 тыс.

Google начала договариваться с российскими дата-центрами о хранении данных примерно за полтора года до вступления в силу новых поправок. Весной 2015 г. выяснилось, что часть информации компания хранит в дата-центрах «Ростелекома». Без согласия партнеров Google не раскрывает их имена. Согласно некоторым источникам, компания завозит в арендованные дата-центры собственные стойки и сервера, оплачивая только помещение.

В апреле 2017 г. стало известно, что Роскомнадзор до конца года не планирует проверять Facebook на предмет перемещения данных россиян в Россию. Ведомство ежегодно проводит встречи с сотрудниками компании, однако соцсеть пока не выразила готовности перенести информацию в российские дата-центры.

Google приходится иметь дело с российскими чиновниками и по другому поводу. В феврале 2015 г. российская компания «Яндекс» обвинила Google в нарушении закона о защите конкуренции. На основании этой жалобы Федеральная антимонопольная служба (ФАС) инициировала разбирательство, которое длилось 2 года. В апреле 2017 г. тяжба завершилась тем, что Google обязалась отказаться от предустановки своих приложений для Android на эксклюзивной основе, не мешать предустановке приложений конкурентов и не создавать экономических стимулов для предустановки своей поисковой системы в качестве поисковика по умолчанию в Google Chrome. К ОГЛАВЛЕНИЮ

МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

15/06/17, infowatch.ru.

Использование паролей

1. Не используйте один пароль для всех сервисов, которыми вы пользуетесь. Рекомендуется использовать разные пароли для разных сервисов;
2. Используйте пароли длиной не менее 8 символов с содержанием строчных и прописных букв, а также цифр и спецсимволов (@, &, % и т.д.). Альтернативной хорошей практикой является использование парольных фраз, состоящих из не менее чем 20 символов, например, «ForestWinterSnowstorm» – их легко запомнить и трудно подобрать;
3. Не сохраняйте пароли в веб-браузерах и клиентах электронной почты;
4. Не передавайте пароли знакомым и не отправляйте по электронной почте;
5. Тщательно храните пароли. Нельзя оставлять записанный пароль на видном месте, клеить его на монитор и т.д.

Защита рабочих станций и собственных устройств

1. Все файлы, скачанные из сети Интернет, перед открытием проверяйте антивирусной программой;
2. При получении по электронной почте писем от неизвестных вам лиц, содержащих ссылки и картинки, рекомендуется сразу удалять, не переходя по ссылкам и не открывая приложенные документы;
3. Пользуйтесь лицензионным антивирусным ПО, настройте автоматическую проверку загруженных из сети файлов и подключенных носителей информации;
4. При возникновении признаков появления вирусов на компьютере проведите полную проверку антивирусным ПО;
5. Всегда устанавливайте последние обновления операционных систем;
6. Для защиты от вирусов шифровальщиков регулярно создавайте резервные копии ценных для вас данных.

Безопасность при осуществлении платежей

1. По возможности, следует использовать дополнительное подтверждение операций, например, с помощью SMS или иным способом (например, по телефону);
2. Не переходите по ссылкам, полученным от недоверенных лиц. При получении писем или сообщений от банков удостоверьтесь, что это именно банк пишет вам;
3. Будьте внимательны при осуществлении платежей в сети Интернет. Проверяйте наличие https в адресной строке браузера и точность адреса.

Использование сети Интернет и социальных сетей

1. Не пользуйтесь незащищенными Wi-Fi-сетями;
2. С осторожностью относитесь к нестандартным сообщениям в сети Интернет (особенно в социальных сетях). Помните, что любые нестандартные просьбы могут быть мошенничеством;
3. Не используйте бесплатную почту и чаты для передачи критически важной информации.

Защита важной информации

1. Используйте шифрование при передаче критически важной информации;
2. С осторожностью относитесь к хранению информации в облаке. Следует шифровать данные для хранения их в облаке либо сделать выбор в пользу хранения информации локально;
3. Не берите смартфон на важные переговоры;
4. Не используйте мобильное устройство для конфиденциальной переписки.

«Интернет вещей»

1. В случае необходимости использования устройств «Интернета вещей» (системы умного дома, управляемые через Интернет электроприборы, замки и т.д.) учитывайте, что на данный момент эти технологии еще не имеют серьезной защиты. И не забудьте поменять стандартный пароль к панели управления ими;
2. С осторожностью относитесь к Smart TV, помните, что это устройство двусторонней коммуникации. К ОГЛАВЛЕНИЮ

РЕГУЛИРОВАНИЕ БОЛЬШИХ ДАННЫХ НЕ ЗА ГОРАМИ

19/06/17, cio.ru. Евросоюз готовит нормативный документ, устанавливающий правила работы с Большими Данными. Российские регулирующие органы могут последовать этому примеру.

Большие Данные, включающие в себя информацию о конкретных людях, нуждаются в особой защите, однако правовых норм, регулирующих оборот данных именно этой категории, пока нет, как нет и юридически обоснованного понятия Больших Данных. Такая ситуация чревата рисками для предприятий. При этом ответственность за инциденты с персональными данными обычно несут ИТ-директора и руководители корпоративных служб информационной безопасности. В ближайшей перспективе в нашей стране могут появиться правовые нормы, регулирующие процессы обработки Больших Данных на предприятиях. Но снимут ли они остроту проблемы или добавят ИТ-директорам новых хлопот, пока не ясно.

Вопросов по теме хранения, использования и защиты Больших Данных, содержащих персональную информацию, пока больше, чем ответов. Так считают участники дискуссии, которая развернулась на форуме BIG DATA 2017, организованном издательством «Открытые системы». Как отметил российский интернет-омбудсмен Дмитрий Мариничев, в отрасли пока нет четкого понимания того, кому собственно принадлежат Большие пользовательские данные: государству, бизнесу, гражданам? А поскольку уже есть случаи утечки и несанкционированного использования таких данных, то очевидно, что их оборот необходимо регулировать. Однако непонятно, где провести границы госконтроля и как минимизировать нагрузку на бизнес. В значительной степени эта неразбериха объясняется отсутствием консенсуса по базовым понятиям. Если с определением персональных данных ситуация в целом довольно прозрачна (на то есть 152-ФЗ), то с Большими Данными – ясности нет никакой. Некоторые эксперты считают, что сам этот термин еще не устоялся.

«Это скорее технический и маркетинговый термин, а потому Большие Данные нельзя вводить в область правового регулирования. Но из этого не следует, что Большие Данные, как они понимаются многими экспертами, существуют в абсолютном правовом вакууме.

Поскольку многие данные, обрабатываемые средствами аналитики, могут рассматриваться как персональные, регулированию они подлежат», – убежден юрист НИУ ВШЭ Александр Савельев.

Другие специалисты вообще отрицают существование Больших Данных как предмета для регулирования.

«Никаких Больших Данных нет. Есть просто данные. Какая разница, много их или мало. Они есть, и их можно использовать для разных целей», – полагает заместитель директора по технологическому развитию ФРИИ Сергей Алимбеков.

Эту точку зрения разделяет и директор департамента универсальных платформ данных IBS Сергей Золотарев: «Мы давно решили для себя, что Больших Данных нет. Технически мы можем работать сегодня с любыми типами данных и в любом режиме».

Отрицающие само понятие Больших Данных эксперты одновременно поддерживают идею о необходимости регулирования просто данных. Эта необходимость уже перезрела, считает Алимбеков. А Золотарев подчеркивает, что именно вопрос прикладного использования данных сейчас ставится во главу угла и бизнесом, и государством, провозгласившим курс на цифровую экономику.

Владимир Журавлев, заведующий кафедрой УЦ «Информзащита», считает, что вопрос, как отделить Большие Данные от персональных, весьма актуален, поскольку бизнес может попасть под весьма жесткое законодательство. Он напомнил, что всего лишь за несоответствие письменной формы согласия на обработку персональных данных требованиям ФЗ-152 «О персональных данных» организация может быть оштрафована на 75 тыс. руб.

Вероятно, в перспективе вопросы регулирования оборота Больших Данных, содержащих персональные сведения, все же найдут свое решение, а ключевые, но не формализованные на данный момент понятия станут юридически значимыми. Как заявил эксперт по защите персональных данных и информационной безопасности DHL Express Алексей Мунтян, сейчас уже не стоит вопрос, будет или нет регулироваться оборот Больших и персональных данных. Это уже происходит.

Мунтян напомнил, что в январе 2017 года Еврокомиссия опубликовала план подготовки нового документа, посвященного электронным коммуникациям – E-privacy Regulation. И в нем явно и четко поднимается проблема регулирования Больших Данных.

«ЕК предлагает синхронизировать и гармонизировать новый европейский документ по защите персональных данных General Data Protection Regulation, который вступит в силу в мае 2018 года, с актом E-privacy Regulation. В этой связи там впервые обсуждаются такие термины, как метаданные, данные, касающиеся взаимодействия пользовательских устройств и технической инфраструктуры сервис-провайдеров. Фактически ЕС уже стоит на пороге регулирования Больших Данных в сфере электронных коммуникаций. Но этим дело не ограничится – это только первый шаг в регулировании Больших Данных», – заявил представитель DHL.

Российские регулирующие органы о ситуации, конечно, осведомлены, поэтому нам стоит ожидать аналогичных законодательных инициатив, считают эксперты.

Большинство из них приветствуют появление новых правил на строящейся дороге к цифровой экономике, но призывают сделать их эффективными.

Активную позицию заняли компании, оперирующие персональными данными миллионов своих клиентов. Это телекоммуникационные операторы и интернет-компании, опасающиеся излишней зарегулированности оборота данных со стороны государства. Ведь слишком жесткие правила вынудят их инвестировать избыточные средства в инфраструктуру обработки данных. Недавно «ВымпелКом», «МегаФон», МТС, «Ростелеком», Mail.Ru Group и «Яндекс» задумались о создании саморегулируемой организации под рабочим названием «Ассоциация Больших Данных». Представители перечисленных компаний уже ведут соответствующие переговоры. Они также выступают за открытость ассоциации для участников других отраслей – финансовой, страховой и пр.

Директор Российской ассоциации электронных коммуникаций Сергей Плуготаренко считает, что российский рынок не готов к исполнению законов, регулирующих работу с Большими Данными, в случае если они несут в себе какие-то новые ограничения. В интервью ТАСС он заявил, что обсуждать целесообразно лишь подходы к сбалансированному законодательству, стимулирующему переход к цифровой экономике и одновременно способному предотвращать негативные последствия от непрофессиональной или незаконной обработки Больших и персональных данных.

Для принятия таких сбалансированных правил необходим диалог между регулятором и отраслевым профессиональным сообществом. Это позволит заблаговременно донести до властей мнение бизнеса по вопросам регулирования Больших Данных, которые могут быть признаны персональными. К ОГЛАВЛЕНИЮ

НАС ВЗЛОМАЛИ. ВСЕ ПЛОХО. ЧТО ДЕЛАТЬ?

23/06/17, rb.ru. Когда происходит утечка данных, объявляйте всеобщую мобилизацию. В ликвидации последствий пригодятся почти все: технические специалисты, юристы, менеджеры и пиарщики.

Антон Соловей, руководитель экспертного направления Falcongaze, рассказал, как правильно координировать этот процесс, провести успешное внутреннее расследование и не потерять доверие клиентов.

Шаг 1. Оцениваем силы

Перед руководством стоит вопрос: справляться самим или пригласить специалистов. Если компания не имеет нужных ресурсов и кадров для устранения последствий, тогда на помощь приходят внешние организации, которые специализируются на расследовании инцидентов. Если компания подготовлена — есть команда и план реагирования — то ей и карты в руки.

При такой работе взаимодействует широкий круг сотрудников: офицеры безопасности, юристы, менеджеры по работе с клиентами и PR-отдел, но основная нагрузка ложится на службу безопасности.

Шаг 2. Ликвидируем последствия и восстановливаем работу системы

Служба безопасности занимается локализацией инцидента и ликвидацией последствий: удаляет вредоносные программы, отключает скомпрометированные учетные записи пользователей, выявляет и латает уязвимости.

После ликвидации последствий офицеры безопасности восстанавливают системы и проверяют нормально ли они функционируют. Этот процесс может включать восстановление систем из чистых резервных копий, воссоздание с нуля, замену поврежденных

файлов на чистые версии, установку исправлений, изменение паролей и ужесточение мер защиты периметра сети.

Крупномасштабные работы могут занять несколько месяцев. Целью ранних этапов должно стать повышение общей безопасности для предотвращения повторных инцидентов. На более поздних этапах следует сосредоточиться на долгосрочных изменениях (например, изменениях инфраструктуры), чтобы максимально защитить компанию.

3. Определяем объемы ущерба

Компания всегда может обратиться в суд с гражданским иском о возмещении убытков, тогда рассчитанный объем ущерба станет основой для взыскания средств с виновных. На объем ущерба влияет стоимость информации, но при условии проведенной ранее оценки, в противном случае руководство может рассчитать только размер упущенной выгоды.

Компания страдает прямо и косвенно: злоумышленники могут похитить данные о банковских картах и снимать деньги со счета — это прямой финансовый ущерб, косвенные последствия исходят от потери репутации и приводят к оттоку клиентов.

Чтобы определить стратегию для пиарщиков, необходимо удостовериться, были ли в массиве персональные данные сотрудников, партнеров и клиентов. В случае наличия такой информации — компании грозят не только репутационные риски, но и санкции со стороны государства, вплоть до уголовной ответственности.

4. Ищем виновника и собираем доказательства

Если атака произошла извне, то служба безопасности пытается провести ее атрибуцию. Если изнутри — то ищет инсайдера, при этом алгоритм поиска виновника при намеренной и ненамеренной утечках отличается.

– В первом случае офицеры безопасности очерчивают круг лиц, которые имели доступ к информации и возможные каналы передачи данных, чтобы зафиксировать на них потенциальные цифровые следы. В этом помогает DLP-система, которая фиксирует всю активность сотрудников за компьютерами. На основании собранных доказательств в совокупности со сведениями из иных источников, служба безопасности указывает на возможного виновника.

– Если произошла случайная утечка, офицеры безопасности выясняют, кто из сотрудников работал со скомпрометированной информацией. Они оценивают масштабы и скорость распространения потерянной информации, чтобы предсказать последствия. Служба безопасности определяет механизм утечки и принимает меры к ее ликвидации. В конце концов, определяются предпосылки инцидента и проводится работа над ошибками.

Приказ о подаче документов в суд принимают руководители. Важно соблюдать установленные процедуры сбора и обработки доказательств. Команда должна четко документировать и координировать работу с юристами и правоохранительными органами. В случае судебного разбирательства данные DLP-системы, как и другие технические сведения, помогут в деле установления виновного.

5. Оповещаем клиентов и партнеров

Если от утечки пострадали третьи лица, рекомендуется опубликовать сообщение — лаконично рассказать, что и когда произошло, какие меры предприняты, найдены ли виновные. Грамотное поведение и публикация результатов спасают репутацию компании.

Раскрытие информации помогает также применить санкции к злоумышленнику и попытаться вернуть средства, потерянные при утечке. А вот сокрытие происшествия рождает сплетни. И сохраняя молчание, компания негативно влияет на репутацию.

Кейс Yahoo

Компания Yahoo, и так находящаяся в долгой стагнации в связи с потерей доли на рынке и оттоком пользователей, сильно подмочила свою репутацию, когда долгое время не хотела подтверждать слухи об утечке 500 миллионов аккаунтов пользователей. Позднее компания все-таки признала факт утечки, однако заявила, что виновны в ней «правительственные хакеры».

Дополнительным ударом по репутации оказалось появившаяся буквально через несколько месяцев информация о новой утечке — на этот раз затронувшей миллиард аккаунтов.

Несмотря на то что новый инцидент подставил под удар гораздо большее количество пользователей, благодаря оперативному

реагированию и грамотной работе пиарщиков и технической поддержки тему удалось относительно быстро замять. Компания предупредила пользователей и сбросила для пострадавших пароли до того, как могла бы появится вызванная слухами паника, приводящая к значительному оттоку клиентов.

В российских реалиях, к сожалению, редко встречается грамотная и адекватная реакция на инциденты информационной безопасности. Чаще всего российские компании предпочитают отрицать сам факт утечки либо уходят в глубокое молчание и отказываются давать любые комментарии.

Кейс Heartbleed

В 2014 году огромный резонанс вызвала выявленная в криптографическом пакете данных OpenSSL уязвимость, получившая название Heartbleed (исчерпывающее объяснение уязвимости в виде комикса сделал Рэндалл Монро). Ошибке было подвержено около 17% всех защищенных веб-сайтов в интернете. К счастью, исправить уязвимость было довольно легко и большинство крупных интернет-сервисов устранили ее в первые же дни.

Однако сайт РЖД (как и обеспечивающий процессинг на сайте банк ВТБ-24) не уделили должного внимания проблеме и не смогли оперативно исправить уязвимость. Вследствие этого было скомпрометирована информация о более чем 200000 банковских карт (на тот момент РЖД являлся крупнейшим онлайн-продавцом России по обороту).

Несмотря на то, что РЖД и ВТБ-24 сперва никак не комментировали событие, а позже отрицали факт утечки, большинство банков приняло решение перевыпустить карты, которые клиенты использовали для покупок на сайте РЖД. В этом случае образцовой реакцией на инцидент можно назвать действия «Рокетбанка» — они уведомили клиентов и перевыпустили их карты сразу же после появления информации об утечке.

6. Делаем выводы

После надлежащего расследования в организации необходимы системные изменения. Для этого готовится отчет, в котором подробно

описываются причина и стоимость инцидента, а также меры для предотвращения будущих происшествий.

Важно усвоить урок и обновить политики и процедуры реагирования на инциденты, выявить недостающие шаги или неточности в процедурах. Утечка может стать импульсом для изменений, что не так уж плохо при меняющемся характере информационных технологий.

После серьезных нападений целесообразно проводить собрания. Отчеты с таких встреч — хороший материал для обучения новых членов команды, который показывает, как более опытные сотрудники реагируют на инциденты.

Итак, основные шаги при утечке информации:

1. Оценить силы: хватит ли людей и ресурсов и есть ли план реагирования;
2. Локализировать инцидент, ликвидировать последствия и восстановить работу системы;
3. Оценить объем ущерба;
4. Выработать тактику поведения при общении с прессой, сформировать необходимые варианты ответов для различных аудиторий;
5. Оповестить клиентов, регулирующие органы, акционеров; проинструктировать сотрудников;
6. Собрать доказательства и попытаться определить виновника;
7. Сделать выводы и улучшить работу службы безопасности.

К сожалению, для предотвращения утечек одной DLP-системы недостаточно: нужны юридические меры, как режим коммерческой тайны, соглашения о неразглашении конфиденциальной информации, и развитая корпоративная культура — система ценностей и благоприятная атмосфера в коллективе. К ОГЛАВЛЕНИЮ

ИНДИКАТОРЫ РАЗВИТИЯ. Зарубежная практика

РИСКИ КРАЖИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПУГАЮТ, И ЗАЩИЩАТЬСЯ ХЛОПОТНО

14/06/17, arsvest.ru. В последнее время практически ежедневно продолжают поступать тревожные новости об утечках информации и рисках, связанных с хищением персональных данных, однако бдительность и информированность пользователей оставляют желать лучшего. Как показало проведенное компанией Experian общенациональное исследование в США, люди не чувствуют себя защищенными от хищения персональных данных.

По данным исследования, людей одновременно беспокоят и риски кражи персональных данных, и сложности, связанные с защитой от этих рисков. У пользователей нет желания активно использовать передовые практики защиты персональных данных ввиду их сложности, неудобства и, как им представляется, низкой вероятности стать жертвой мошенничества.

84% респондентов признают, что их беспокоит безопасность их персональных данных, и в то же самое время почти две трети (64%) респондентов согласны с тем, что «постоянное беспокойство о безопасности персональных данных в интернете чересчур напрягает». Большинство опрошенных заявляют, что им трудно следить за финансовыми транзакциями (53%), а почти половина (48%) даже не осуществляет регулярную проверку своих финансовых отчетов на предмет наличия ошибок или подозрительной деятельности.

В 2016 г. более 15 млн американцев стали жертвами хищения персональных данных – на 16% больше, чем в предыдущем году 1.

Среди населения широко распространены заблуждения относительно хищения персональных данных и мошенничества.

«Люди зачастую предпочитают игнорировать проблемы вместо того, чтобы их решать, – говорит Наталия Фролова, директор по маркетингу, Experian в России и странах СНГ. Понимание рисков, информированность о существовании «темной сети» и постоянный

поиск новых способов мониторинга и минимизации мошенничества в наше время уже не роскошь, а необходимость. К сожалению, по данным исследования Experian, для большинства людей эти задачи не являются приоритетными, что облегчает жизнь мошенникам».

Ключевые результаты исследования:

1. Только половина (49%) респондентов допускают, что могут стать жертвой хищения персональных данных; из них 57% имеют годовой семейный доход в размере $100 000 или более, а у 45% семейный доход не достигает $50 000.
2. Значительное большинство респондентов (72%) полагает, что финансовых мошенников интересуют только «персональные данные богатых людей»!
3. В восприятии опрошенных, угроза номер один для безопасности персональных данных – это утечка данных. Угроза номер два – «фишинговые» электронные сообщения для обманного получения паролей.
4. Нередко пользователи производят поиск в интернете по своим персональным данным, чтобы узнать, не действует ли кто-то еще от их имени (26%).
5. Мониторинг банковских карт и кредитных отчетов был признан респондентами самым эффективным способом противодействия хищению персональных данных (58% и 55%, соответственно).
6. Большинство опрошенных знают, что такое хищение персональных данных: 52% респондентов сами оказывались жертвой, или это произошло с кем-то из их знакомых.
7. Те, кто стал жертвой кражи персональных данных, признают, что это оказало негативное воздействие на их краткосрочные и долгосрочные финансовые цели (37% и 27%, соответственно).
8. У 55% из тех, кто пострадал от хищения персональных данных во время поездки, ушло значительное время (от нескольких недель до года) на то, чтобы решить проблемы, связанные с мошенническим использованием их данных.

Рекомендации по контролю мошенничества и защите персональных данных:

1. Регулярно проверяйте свой кредитный отчет и следите за точностью указанной в нем информации.
2. Внимательно проверяйте выписки по счетам.
3. Защитите свой телефон паролем. Телефон открывает доступ к конфиденциальной информации и учетным записям. Задайте уникальный пароль для разблокирования устройства и активируйте программное обеспечение для удаленного поиска телефона и уничтожения информации в случае его потери или кражи.
4. Используйте диспетчер паролей для создания надежных паролей для личного кабинета и регулярно меняйте их.
5. Не заходите в свои финансовые аккаунты и не делайте покупки по интернету через общедоступный Wi-Fi и незащищенные сети.
6. Будьте осторожны, публикуя какие-либо сведения о себе в интернете (особенно в соцсетях). К ОГЛАВЛЕНИЮ

ПОЧЕМУ КОМПАНИИ НЕ ДОЛЖНЫ БОЯТЬСЯ ВВЕДЕНИЯ ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ДАННЫХ (GDPR)

15/06/17, securitylab.ru. Основная цель Общего Регламента по Защите Данных (GDPR) заключается в том, чтобы обеспечить защиту данных граждан ЕС, независимо от того, где они хранятся.

Регламент по Защите Данных, который имеет отношение к компаниям, находящимся на территории ЕС и за его пределами, вступит в силу 25 мая 2018 года. Он требует от компаний, которые обрабатывают данные граждан ЕС, защищать эти данные или испытать на себе последствия от несоблюдения требований Регламента — в первую очередь, штрафов , которые могут составлять до 4% от глобального годового дохода компании.

Но, несмотря на то, что крайний срок приведения системы защиты информации в организации в соответствие с требованиями Регламента стремительно приближается, компании не спешат предпринимать соответствующие меры.

«Когда дело доходит до соответствия Регламенту, наблюдается почти рефлексивная тенденция со стороны крупных предприятий либо ждать, пока что-то «утрясется», либо пытаться согласовать действия

некоторых правил уже после их введения. Кроме того, когда соответствие Регламенту воспринимается как нечто сложное, наблюдается фактически недоверие к тому, что это соответствие останется в силе», — отмечает Кен Крупа, технический директор компании MarkLogic, американский поставщик, чья база данных NoSQL используется Deutsche Bank, DHL, Raytheon, Dow Jones и многими другими предприятиями и государственными структурами США.

Общий Регламент по Защите Данных – это возможность для инноваций

GDPR, безусловно, соответствует категории внешне «трудного» регулирования, но этот регламент можно также отнести к категории инновационного альтер-эго, которое должно использоваться передовыми предприятиями.

«Уровень оперативности, особенно в отношении безопасности данных, конфиденциальности данных и управления данными, необходимый для соответствия Регламенту, может быть использован для достижения больших конкурентных преимуществ», — говорит он.

«Способность действовать в соответствии с заявленными или подразумеваемыми предпочтениями клиентов в реальном времени – независимо от того, имеет это отношение к конфиденциальности или нет — является основной заветной целью почти каждой инициативы, о которой вы только можете подумать. Поэтому руководители, ориентированные на будущее, должны спросить себя, почему бы им не использовать мандат GDPR, чтобы сделать что-то действительно инновационное с данными о клиентах?»

Кроме того, Регламент может, в конечном итоге, повлиять на законы о защите данных в других странах.

«Крупные организации являются многонациональными и, следовательно, многоюрисдикционными. Стратегии компаний в отношении данных должны учитывать многоюрисдикционную точку зрения на мир, поэтому в более широком смысле требования к защите данных в США окажутся подвержены влиянию GDPR», — отмечает Крупа.

«Окажет ли Регламент прямое влияние на законодательство США или нет, можно вынести на обсуждение, однако я считаю, что ответ на этот вопрос не станет решающим фактором. Теперь, когда вводится в

действие западное региональное регулирование, это, хотя бы косвенно, но все же затронет США».

Задача для директоров по управлению данными в компании

С точки зрения отдельных пользователей введение Общего Регламента по Защите данных – это замечательно.

«Как человеку, обладающему личными данными, которые нуждаются в защите, мне нравится идея, что в случае необходимости правовая основа будет на моей стороне», — отмечает Крупа.

«В то же время, если я поставлю себя на место директора по управлению данными, то мне следует беспокоиться о влиянии, которое окажет предоставление индивидуальных регулирующих прав сразу миллионам людей».

Одна из причин подобного беспокойства заключается в том, что предприятия обучены обходиться с конфиденциальными данными очень методично.

«Это означает, что для глобальных мыслителей все будет очень непросто. Однако те, кто относится к защите данных и управлению данными как к неотъемлемой части деятельности, ориентированной на данные, обретут преимущества, выходящие за пределы простого соблюдения нормативных требований. Именно поэтому в компании MarkLogic мы тратим много времени на внедрение безопасности и управление внутри базы данных. Именно эти действия наиболее эффективны», — заключил он. К ОГЛАВЛЕНИЮ