Groteck
Business Media
На рынке СМИ с 1992 года

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

МАШИНОСТРОЕНИЕ, МЕТАЛЛУРГИЯ, НЕФТЕГАЗОВЫЙ КОМПЛЕКС, ЭНЕРГЕТИКА, ТРАНСПОРТ, ЖКХ, ТЕЛЕКОММУНИКАЦИИ, БЕЗОПАСНОСТЬ, СТРОИТЕЛЬСТВО, ПИЩЕВАЯ ИНДУСТРИЯ, МЕДИЦИНА, ФИНАНСОВЫЙ СЕКТОР, ОБРАЗОВАНИЕ И НАУКА, ИНДУСТРИЯ СЕРВИСА, ТОРГОВЛЯ, СЕЛЬСКОЕ ХОЗЯЙСТВО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННОЕ АГЕНТСТВО «МОНИТОР»
iCenter.Ru

№ 4 (88) апрель 2016

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ЗАКОНОДАТЕЛЬСТВО ЗАКОНОПРОЕКТЫ ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ ФИНАНСЫ ИНВЕСТИЦИИ ФОНДОВЫЙ РЫНОК БАНКРОТСТВО СЕРТИФИКАЦИЯ ЛИЦЕНЗИРОВАНИЕ СТАНДАРТЫ АУДИТ КАЧЕСТВО СОГЛАШЕНИЯ ПАРТНЕРСТВО СЛИЯНИЯ ПОГЛОЩЕНИЯ РЕОРГАНИЗАЦИИ КАДРОВЫЕ НАЗНАЧЕНИЯ КАДРОВЫЕ РЕШЕНИЯ УПРАВЛЕНИЕ ПЕРСОНАЛОМ ПРОБЛЕМЫ КОНФЛИКТЫ ИНЦИДЕНТЫ АРБИТРАЖНАЯ ПРАКТИКА ПРОЕКТЫ КОМПЛЕКСНЫЕ РЕШЕНИЯ ОПЫТ ВНЕДРЕНИЯ ТЕХНОЛОГИИ ОБОРУДОВАНИЕ ИНСТРУМЕНТЫ МАТЕРИАЛЫ ПРОДУКТЫ УСЛУГИ ОБЗОРЫ ИНДИКАТОРЫ РАЗВИТИЯ АНАЛИТИКА ЭКСПЕРТНЫЕ ОЦЕНКИ ДЕЛОВОЙ КАЛЕНДАРЬ ВЫСТАВКИ ФОРУМЫ

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ

ГЛАВНЫЕ НОВОСТИ

СОДЕРЖАНИЕ НОМЕРА:

ТЕХНОЛОГИИ. ОБОРУДОВАНИЕ. ПРОДУКТЫ. УСЛУГИ
Сертификация. Лицензирование. Стандарты

ПО и технические новинки

ПРОБЛЕМЫ. КОНФЛИКТЫ. ИНЦИДЕНТЫ
Проверки регуляторов

Утечки информации. Инциденты

ИНДИКАТОРЫ РАЗВИТИЯ
Российская практика

Зарубежная практика

РЕГУЛИРОВАНИЕ
Российское регулирование

Коллекторов могут лишить доступа к персональным данным должников

22 марта 2016, Россия, Москва, bankir.ru. Депутаты Госдумы обсудят законопроект, ограничивающий деятельность коллекторских агентств. Эту информацию подтвердил спикер нижней палаты Сергей Нарышкин. Как сообщает портал BFM.ru, документ вводит существенные ограничения: он прямо запрещает применять коллекторам физическую силу, а также угрожать ее применением и оказывать психологическое давление на должников.

Уставный капитал агентства должен составлять не менее 10 млн рублей, а коллекторская деятельность должна быть его основной деятельностью. Нельзя будет передавать коллекторам персональные данные должников без их согласия. Кроме того, последние смогут отказаться от общения с коллекторами. Все эти нормы могут ввести не только для коллекторов, но и для кредитных организаций. Юристы отмечают, что законопроект давно назрел, однако, по мнению правоведов, является слишком жестким.

«Коллекторы превращаются из тигров в таких вот, можно сказать, комаров, и фактически от комариного укуса должника ничего не изменится»,— прокомментировал ситуацию управляющий партнер адвокатского бюро КИАП Андрей Корельский. В то же время эксперты признают, что оставлять все, как есть, тоже неправильно, потому что, к сожалению, «последние случаи принимают все более радикальный характер».

Общественные заведения в РФ будут оштрафованы на 200 тыс. руб. за отказ идентифицировать посетителей

23 марта 2016, Россия, Москва, securitylab.ru. Владельцы кафе и ресторанов обязаны идентифицировать посетителей, использующих Wi-Fi.

Администрации ресторанов, библиотек и школ обязаны идентифицировать посетителей, использующих Wi-Fi. Минкомсвязи подготовило законопроект, устанавливающий штраф до 200 тыс. рублей за отказ идентифицировать пользователей. За повторное нарушение штраф составит 300 тыс. На данный момент документ находится на стадии согласования. Ранее законодательство предусматривало ответственность только для операторов связи. Им грозил штраф до 40 тыс. рублей.

Ведомство планирует дополнить Кодекс об административной ответственности статьей 13.32. Дополнение предусматривает наложение штрафов на юридических лиц и индивидуальных предпринимателей за нарушение порядка установления личности пользователей.

Идентифицировать посетителей, использующих Wi-Fi, а также их оборудование в общедоступных Wi-Fi-сетях операторов связи обязали два постановления правительства – от 31 июля и 12 августа 2014 года. Личность пользователя устанавливается с помощью удостоверяющего документа или номера сотового телефона.

Банк России может получить доступ к переписке пользователей

25 марта 2016, Россия, Москва, pikabu.ru. Соответствующие поправки рекомендованы ко второму чтению Комитетом Госдумы РФ по финрынку.

Комитет Госдумы РФ по финансовому рынку рекомендовал ко второму чтению поправки в закон «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком», позволяющие Центробанку получать доступ к переписке россиян. Как сообщает «КоммерсантЪ» со ссылкой на аналитика компании Mobile Research Group Эльдара Муртазина, подобный шаг позволит ЦБ эффективнее бороться с преступлениями в финансовой сфере. На расходах телекоммуникационных компаний нововведение не отразится.

Согласно проекту закона, операторы связи будут обязаны предоставлять по запросу Центробанка данные о получателях сообщений, времени соединения, сетевых адресах поднадзорных ЦБ организаций и их клиентов. В настоящее время доступ к подобной информации уже есть у ФСБ, поскольку все действующие на территории РФ операторы связи обязаны устанавливать на свои сети Систему технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ). Зачем такой доступ понадобился Центробанку, не совсем понятно. По мнению некоторых экспертов, вероятно, у законопроекта есть «второе дно».

Как отметил эксперт в сфере телекоммуникаций Максим Букин, установить, кто находился в такое-то время по такому-то адресу и отправил оттуда SMS, электронное письмо или сообщение в чате, без особого труда можно и сейчас. Вопрос в другом – как на самом деле будет использоваться закон в случае его принятия.

«Может быть, сформируется какой-то чудесный рынок дополнительных услуг, когда под прикрытием получения информации о том, что сказал инсайдер, мы будем пытаться за деньги получать информацию о том, кто вообще что-либо сказал», - предположил Букин.

Сенатор: проект о телемедицине могут внести в Госдуму до конца сессии

25 марта 2016, Россия, Москва, ria.ru. Законопроект о телемедицине, регламентирующий использование информационных технологий при оказании медицинской помощи в РФ, может быть внесён в Госдуму до конца весенней сессии, сообщила 25 марта зампред комитета Совета Федерации по конституционному законодательству Людмила Бокова.

"Принятие нового закона поможет дальнейшему развитию телемедицины в нашей стране и существенно повысит доступность медпомощи для жителей труднодоступных территорий. Для нас важно сегодня обеспечить это с помощью цифровых технологий, которые у нас развиваются и показали свое хорошее назначение. Необходимо, чтобы в законе они получили поддержку, а именно закрепили саму возможность оказания подобного рода услуг", — сказала сенатор в ходе "круглого стола", на котором была представлена концепция законопроекта.

Бокова, чьи слова цитирует пресс-служба Совфеда, сообщила, что сейчас сфера использования информационных технологий при оказании медпомощи в законодательстве никак не регулируется. В частности, пока не решены вопросы защиты персональных данных пациентов и ответственности медиков при постановке диагноза в ходе дистанционных консультаций.

Сенатор ответила, что сейчас технологиями телемедицины пользуются медики более 60 регионов. В будущем в каждом субъекте федерации планируется создать координационный центр телемедицины, который смог бы обеспечить связь сельских больниц с лучшими российскими клиниками, сказала Бокова.

Иванов: защита персональных данных не должна касаться погибших в ВОВ

29 марта 2016, Россия, Тульская обл., ria.ru. Глава администрации президента РФ Сергей Иванов считает необходимым исправить законодательство о защите персональных данных, чтобы оно не распространялось на воинов, погибших в годы Великой Отечественной войны.

"Обязательно с этим постараюсь разобраться", — заявил он на пленарном заседании Третьего съезда Общероссийского общественного движения "Поисковое движение России".

Главе администрации Кремля рассказали о том, что в одном из регионов отделение Поискового движения опубликовало в газете фамилии воинов, останки которых были найдены, чтобы отыскать их родственников. Региональное управление Роскомнадзора запретило впредь делать такие публикации без разрешения самих родственников, так как это нарушает законодательство о защите персональных данных.

Иванов жестко отреагировал. "При чем тут защитники Отечества, павшие 70 лет тому назад?" — заявил он. Иванов считает, что закон о защите персональных данных должен распространяться только на ныне живущих россиян. Приведенный случай он назвал примером "головотяпства и бюрократии".

РКН займется популяризацией ответственного отношения к персональным данным

01 апреля 2016, Россия, Москва, rspectr.com. Заместитель руководителя Роскомнадзора Антонина Приезжева рассказала, что ведомство разработало Стратегию институционного развития и информационно-публичной деятельности в области защиты прав субъектов персональных данных. Презентация документа состоялась 31 марта в пресс-центре ТАСС с участием представителей РКН.

Основной целью Стратегии, которую ставит перед собой ведомство, является формирование ответственного отношения у граждан к своей конфиденциальной информации. Она разработана на период до 2020 года. По словам А. Приезжевой, Стратегия является "живым документом" и будет совершенствоваться в зависимости от появления новых угроз и вызовов.

Замглавы РКН отметила, что нарушение обработки персональных данных чаще всего связано с недостаточным уровнем информирования как самих граждан, так и операторов, занимающихся обработкой информации. По этой причине Стратегия, как сообщила А. Приезжева, носит в первую очередь просветительский характер.

Начальник управления по защите прав субъектов персональных данных РКН Юрий Контемиров обратил внимание, что в России уже удалось создать эффективный механизм для защиты прав граждан в этой области. В частности, он выделил наличие отраслевого законодательства, регулятора, системы санкций, соответствующих европейской модели, и сложившуюся судебную практику.

Кроме того, спикер назвал другие главные направления деятельности Стратегии. Так, например, к ним относятся повышение качества образования и развитие международного сотрудничества в этой области.

"Мероприятия в рамках Стратегии направлены на минимизацию нарушения прав наших граждан и исключения тех нарушений, с которыми Роскомнадзор сталкивается в своей деятельности", - сообщил Ю. Контемиров.

РКН и ранее вел просветительскую деятельность касательно безопасности конфиденциальной информации россиян.

А. Приезжева напомнила, что в прошлом году ведомство запустило сайт персональныеданные.дети, провело конкурс для юных пользователей "Береги свои персональные данные", представило на телевидении социальный ролик и разработало комментарий к закону.

Роскомнадзор разработал Стратегию развития в области защиты прав субъектов персональных данных до 2020 года

01 апреля 2016, Россия, Москва, garant.ru. Несмотря на почти 10-летний срок действия Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее – закон о персональных данных) установленные им требования к обработке сведений по-прежнему систематически нарушаются операторами, а многие лица, являющиеся субъектами персональных данных, не знают ни объема своих прав, гарантированных законом (гл. 3 закона о персональных данных), ни способов их защиты. Результаты проводимых Роскомнадзором как уполномоченным органом по защите прав субъектов персональных данных контрольно-надзорных мероприятий показывают, что основными проблемами в этой области являются:

- сбор операторами избыточных сведений персонального характера, запрашиваемых у субъектов персональных данных, необходимость получения которых не обусловлена целями обработки;

- практика "сознательного правонарушения", когда операторы осознанно идут на нарушение требований законодательства, считая, что проще уплатить незначительный штраф (ст. 13.11 КоАП РФ), чем действовать по закону;

- наличие у ряда операторов внутренних документов, определяющих порядок обработки персональных данных, положения которых противоречат нормам закона о персональных данных;

- отсутствие у субъектов персональных данных возможности удалить свои данные, ранее предоставленные операторам, в том числе при использовании интерактивных сервисов (при осуществлении покупок в интернет-магазинах, пользовании социальными сетями и т. д.).

В целях обеспечения защиты прав граждан на неприкосновенность частной жизни, личную и семейную тайну и создания условий для соблюдения закона о персональных данных операторами Роскомнадзор разработал Стратегию институционального развития и информационно-публичной деятельности в области защиты прав субъектов персональных данных на период до 2020 года (далее – Стратегия). Вчера (31 марта) Стратегия была презентована ведомством на специально организованной информационным агентством России "ТАСС" пресс-конференции.

Как отметила заместитель руководителя Роскомнадзора Антонина Приезжева, разработать единый шаблон для обработки персональных данных невозможно, поскольку в этом случае не будет учтена профессиональная специфика организаций, составляющих операторское сообщество (кредитные организации, коллекторские агентства, страховые компании, турфирмы, медицинские учреждения, образовательные организации, управляющие компании в сфере ЖКХ, интернет-сайты и др.). Также очень сложно отследить нарушения каждого отдельного оператора. Поэтому в качестве одного из важнейших направлений деятельности Роскомнадзора Стратегия называет взаимодействие с профессиональными объединениями операторов.

В частности, определено, что ведомство будет поддерживать инициативы последних по разработке отраслевых стандартов и кодексов профессионального поведения и привлекать эти объединения к разработке инструкций по обработке персональных данных в конкретных отраслях. Соответственно, объединения операторов и СРО в области обработки персональных данных будут следить за деятельностью своих участников, что поможет избежать или по крайней мере сократить количество правонарушений с их стороны. При этом предлагается создать систему рейтингирования как непосредственно операторов, так и профессиональных объединений и СРО.

Начальник Управления по защите прав субъектов персональных данных Роскомнадзора Юрий Контемиров подчеркнул, что эффективность отраслевых стандартов подтверждается, например, реализацией утвержденных Банком России в 2010 году рекомендаций по выполнению законодательных требований при обработке персональных данных в организациях банковской системы РФ. До принятия документа нарушения в деятельности банков по обработке персональных данных выявлялись в 70 -80% проводимых ведомством проверок, а к настоящему времени этот показатель уменьшился до 40%.

В качестве мер по повышению правовой грамотности населения Стратегия предусматривает, в частности, оптимизацию деятельности существующего Портала персональных данных (pd.rkn.gov.ru), проведение дважды в год дней открытых дверей для консультирования субъектов персональных данных и операторов, занимающихся обработкой данных, по вопросам применения соответствующего законодательства, создание тематических рекламных роликов и их трансляцию на рекламных билбордах, а также перед началом показа фильмов в кинотеатрах и на интернет-сайтах, предоставляющих доступ к легальному кинематографическому контенту.

Особое внимание уделено вопросу защиты персональных данных несовершеннолетних граждан, в том числе в Интернете. Предлагается, например, ввести в школах факультативные занятия по информационной грамотности, на которых детям будут объяснять, как максимально защитить свои персональные данные в сети, избежать взлома аккаунта и распространения личных данных, и обеспечить информирование несовершеннолетних популярными среди них интернет-сайтами о необходимости ответственно относиться к своим личным данным.

Ответственное отношение к личным данным определяется Стратегией как понимание необходимости бережной обработки персональных данных, осознание последствий, которые информационные технологии могут оказать на личную жизнь, репутацию и психологическое состояние субъекта персональных данных. Информация о ходе реализации Стратегии будет отражаться в ежегодном отчете Роскомнадзора, который он направляет Президенту РФ, Федеральному Собранию РФ и в Правительство РФ.

В заключение эксперты, презентовавшие Стратегию, напомнили, что во многих случаях граждане могут сами предотвратить незаконную обработку своих персональных данных, соизмеряя объем запрашиваемых операторами сведений и цели обработки данных.

Зарубежное регулирование

В Германии суд запретил частным компаниям собирать лайки на «Фейсбуке»

10 марта 2016, Германия, lifenews.ru. Решение принято для того, чтобы защитить персональные данные пользователей.

Окружной суд Дюссельдорфа запретил частным компаниям лайки «Фейсбука» на их собственных сайтах из-за закона о защите персональных данных. Выяснилось, что, когда пользователь жмёт на «сердечко», он автоматически открывает доступ к своей личной информации.

Немецкий суд требует, чтобы организации предупреждали о считывании персональных данных либо отказались от лайков. В противном случае компаниям грозят крупные взыскания. Так, к примеру, бренд Peek & Cloppenburg, который и создал в Германии прецедент, может быть оштрафован на 250 000 евро за каждое подобное нарушение.

В США могут ввести контроль за использованием персональных данных для провайдеров

11 марта 2016, США, rns.online. Федеральное комиссия по связи США обнародовала детали инициативы ввести новые правила работы с личными данными пользователей для интернет-провайдеров, которые включают требование получать у клиентов разрешение на использование информации в различных случаях. Об этом сообщает The Wall Street Journal.

Новые правила направлены на регулирование деятельности кабельных компаний и провайдеров беспроводного доступа в интернет. Ожидается, что они будут вынесены на обсуждение Федеральной комиссии по связи США в течение марта и скорее всего будут предварительно одобрены.

Правила нацелены на защиту десятков миллионов интернет-пользователей от нежелательного использования их персональных данных. Инициатива регулятора предполагает, что поставщики услуг доступа в интернет должны будут получать согласие пользователей на использование их данных в различных целях, в том числе для показа таргетированной рекламы третьими лицами. Согласие пользователя не потребуется только для использования данных в целях маркетинга коммуникационных сервисов.

Чиновники указывают, что регулятор не намерен ограничивать целевую рекламу в интернете, но «потребители должны иметь возможность эффективного контроля над тем, как их персональная информация используется и кому предоставляется».

Тем не менее интернет-провайдеры опасаются, что новые нормы поставят их в неравные условия с такими интернет-компаниями, как Google и Facebook (их деятельность в области работы с персональными данными регулирует Федеральная торговая комиссия США).

Обама против защиты персональных данных смартфона

12 марта 2016, США, podrobnosti.ua. Правительство США в некоторых случаях должно иметь доступ к данным с мобильных телефонов граждан. Об этом заявил президент США Барак Обама.

По словам Обамы, абсолютная защита персональной информации может помешать властям предотвращать теракты, бороться с распространением детской порнографии и даже контролировать уплату налогов. "Все будут ходить со счетом в швейцарском банке в кармане", - считает Обама.

Президент заявил, что не может комментировать судебное разбирательство между ФБР и компанией Apple, которая отказывается взломать телефон террориста, причастного к убийству 14 человек в Сан-Бернардино. Ко всему, он высказался по поводу необходимости соблюдения баланса между гражданской свободой и интересами безопасности.

Президент США призвал не превращать мобильные телефоны в фетиш. По его словам, необходимо создать систему с надежным шифрованием, ключ к которой могло бы получить только определенный круг лиц и только в ситуациях, когда с этим согласно общество.

Правительства стран ЕС заставят IT-компании ослабить шифрование данных

28 марта 2016, Евросоюз, zakon.kz. За отказ предоставить расшифрованную информацию руководителям компаний может грозить тюремное заключение сроком до пяти лет.

Предъявленные ФБР компании Apple требования по разблокировке iPhone преступника стали причиной бурных дебатов на тему неприкосновенности частной жизни. Крупные компании (Apple, Google и Facebook) опасаются возможности дальнейших кибератак из-за ослабления шифрования. Более слабая защита безопасности данных может привести к утечке информации пользователей. Похищенные данные также могут использоваться спецслужбами недружественных стран.

В связи с недавними терактами многие европейцы согласны предоставить правоохранительным органам больше полномочий для получения доступа к их частной жизни. Противники такого решения считают защиту личных данных равной свободе выражения мнений.

В Великобритании завершается подготовка проекта закона «О следственных полномочиях» (Investigatory Powers Bill), заставляющего технологические компании обходить шифрование, когда речь идет о национальной безопасности. Проект закона разработан консервативной партией, имеющей достаточное парламентское большинство для введения в действие нормативных изменений. Документ заставит компании сохранять списки web-сайтов, посещенных пользователями в Великобритании в течение 12 месяцев. Разведывательные органы страны получат юридические полномочия для сбора больших объемов данных и взломов отдельных устройств. По словам представителей правительства, такие полномочия необходимы для защиты безопасности страны. Также власти смогут требовать от компаний ослабить шифрование для получения доступа к сообщениям.

29 марта французские политики обсудят предложения по обновлению законов о борьбе с терроризмом. В случае принятия поправок за отказ предоставить расшифрованную информацию правительству руководителям фирм грозит тюремное заключение сроком до пяти лет, а также штраф около $390 тыс. Поправки к законодательству являются ответом на теракты, произошедшие в ноябре 2015 года.

Нидерланды выступают против бэкдоров в шифровании, использующихся в сервисах крупных компаний. По мнению правительства Голландии, подобные лазейки делают зашифрованные файлы уязвимыми для преступников, террористов и иностранных разведок.

В Грузии предлагают создать ведомство по защите личных данных

31 марта 2016, Грузия, sputnik-georgia.ru. Инспектор по защите личных данных Тамар Калдани предлагает создать в Грузии ведомство, которое подготовит план действий по защите личных данных. Причиной создания новой структуры инспектор по защите личных данных, называет участившиеся случаи распространения кадров личной жизни в интернете.

"Нельзя терять время. Я прошу премьера и президента (Грузии) создать координирующее ведомство или группу, которая возьмет на себя ответственность за разработку комплексного плана и его быстрое осуществление. С нашей стороны, я выражаю готовность к искоренению практики грубого вмешательства в личную жизнь", — заявила Калдани в эфире "Рустави 2". Пора уже мобилизовать все ресурсы и разработать такой план, который будет отвечать всем существующим угрозам, добавила она. Инспектор считает, что правительство должно подключить к работе иностранных экспертов и ведомства других стран.

Рада приняла за основу закон о защите прав покупателей финуслуг

31 марта 2016, Украина, kamkrai.com. 31 марта парламентом принят за основу законопроект № 2456-д «О внесении изменений в некоторые законодательные акты Украинского государства относительно усовершенствования защиты прав покупателей финансовых услуг». За принятие законодательного проекта проголосовали 226 общенародных депутатов.

Документом также предлагается ввести единые требования по рекламе услуг, раскрытие информации банками и небанковскими финансовыми заведениями и идентичную ответственность за нарушение прав покупателей финансовых услуг и ввести ответственность финансовых учреждений за нарушение прав покупателей финансовых услуг. Также в законодательном проекте предусмотрена защита персональных данных и приватности пользователя финансовых услуг; создание и внедрение механизма досудебного решения споров относительно представления финансовых услуг; содействие конкуренции в сфере представления финансовых услуг.

Минимальный объем информации, которая должна предоставляться потребителю по каждому виду банковской деятельности (если это не урегулировано законодательством), определит Нацбанк. Украина же только начинает развитие актуальной для нашего времени системы защиты прав покупателей финансовых услуг. Законопроектом, в частности, предлагается дополнить закон «О финансовых услугах и национальном регулировании рынков финансовых услуг» нормами, которые предлагают регуляторам ясный список полномочий для реализации задачи защиты прав покупателей финансовых услуг, а еще право на применение к виновным лиц санкций за нарушение таковых прав.

ПРОЕКТЫ. КОМПЛЕКСНЫЕ РЕШЕНИЯ
Соглашения и партнерства. Сотрудничество. Профессиональное сообщество

Знаменитый российский антивирус обошелся «Яндексу» в 200 миллионов

23 марта 2016, Россия, Москва, so-l.ru. Компания Yandex (владелец российского поисковика «Яндекс») раскрыла в своем годовом отчете стоимость приобретения активов российского антивирусного разработчика «Агнитум».

За компанию в момент совершения сделки было выплачено 120 млн руб. Еще 80 млн руб. «Яндекс» может доплатить в будущем в случае выполнения продавцами определенных обязательств. Из этой суммы 60 млн руб. будут выплачены наличными, 20 млн руб. - в виде акций Yandex с ограничениям на продажу (restricted stock unit, RSU). Таким образом, общая сумма сделки по покупке активов «Агнитум» составила 200 млн руб. Сама сделка была заключена в декабре 2015 г.

Что выпускал «Агнитум»

«Агнитум» - компания из Санкт-Петербурга, основана в 1999 г. Первые продукты компании - Jammer и Tauscan - предназначались для обнаружения и защиты от компьютерных атак.

В 2002 г. «Агнитум» создал свой основной ставший чрезвычайно популярным продукт - ПО для защиты от атак Outpost Firewall, который состоит из бесплатной и платной версий (Outpost Firewall Pro). Позднее «Агнитум» выпустил собственный антивирус Outpost Security Suite и антиспам-фильтр Spam Terrier.

Также в портфеле компании были комплексное решение для защиты от интернет-угроз Outpost Security Suite Pro (вместе с бесплатной версией - Outpost Free Security Suit) и ПО для защиты корпоративных сетей Outpost Network Security. Кроме того, компания выпускала антивирусное решение Outpost AntiVirus Service, распространявшееся по подписке среди абонентов интернет-провайдеров. А в 2012 г. «Агнитум» приобрел активы, включая технологии и базу вирусных сигнатур венгереского антивирусного разработчика VirusBuster.

Зачем «Агнитум» был нужен «Яндексу»

В результате сделки с «Яндексом» в интернет-компанию перешли ключевые сотрудники «Агнитум». Целью покупки была интеграция разработок «Агнитум» в «Яндекс.Браузер». В частности, в браузер были интегрирована технология активной защиты Protect, которая отвечает за безопасность пользователей «Яндекс.Браузера». В ней сочетаются несколько механизмов: защита от кражи паролей, функция «Безопасный Wi-Fi», блокировка подозрительных сайтов и антивирусная проверка файлов».

"Лаборатория Касперского" и Краснодарский край договорились о сотрудничестве

24 марта 2016, Россия, Краснодарский край, oreanda.ru. "Лаборатория Касперского" и администрация Краснодарского края подписали соглашение о намерениях сотрудничать в сфере информационной безопасности. Это партнёрство позволит повысить защищённость IT-инфраструктуры региона, а также будет способствовать социальному и экономическому развитию Кубани.

Соответствующий документ был подписан губернатором Краснодарского края Вениамином Кондратьевым и генеральным директором "Лаборатории Касперского" Евгением Касперским, посетившим Краснодар в рамках деловой поездки.

Администрация Краснодарского края и "Лаборатория Касперского" нацелены на долгосрочное сотрудничество и планируют взаимодействовать в вопросах применения передовых технологий и методов защиты информации, а также обучения и консультирования специалистов, обеспечивающих поддержку IT-систем органов государственной власти в регионе.

"С каждым годом в регионе растёт число интернет-пользователей, но вместе с тем, растёт и количество заражённых вирусами компьютеров, а также кибератак. Наша задача - в таких условиях максимально защитить персональные данные жителей края. Нельзя, чтобы интернет из удобного канала коммуникации превратился в инструмент манипулирования. Дальнейшее развитие предоставления гос- и муниципальных услуг через интернет также не будет иметь смысла, если не будет защищённости от массовых кибератак. Рассчитываю, что взаимодействие будет конструктивным. В лице компании край получит партнёра, который, помогая сохранить, поможет и приумножить", - сказал Вениамин Кондратьев, губернатор Краснодарского края.

Евгений Касперский, генеральный директор "Лаборатории Касперского", заявил: "Защита информации - это очень важная и сложная проблема сегодня, которая остро стоит, в том числе, перед государственными органами. Им требуется качественная защита, так как риски в области информационной безопасности продолжат расти. Мы фиксируем всё больше целевых атак, и видим, что киберпреступники используют всё более сложные инструменты. Я рад, что мы стали партнёрами с родным для меня Краснодарским Краем, и что мы будем работать над повышением уровня защищённости информационных систем региональной Администрации".

В рамках своего визита в Краснодар Евгений Касперский также посетил Кубанский государственный университет, где выступил перед студентами с открытой лекцией об актуальных киберугрозах и способах противостояния им.

"Лаборатория Касперского" уже давно сотрудничает с администрациями ряда российских регионов в целях повышения уровня их информационной безопасности. В частности, соглашения о сотрудничестве заключены с правительствами Астраханской, Волгоградской, Нижегородской, Новосибирской, Омской и Мурманской областей, а также с администрациями Республики Татарстан, Республики Саха (Якутия) и Забайкальского края и с правительством города Санкт-Петербурга.

Компания «Астерит» в очередной раз подтвердила статус Microsoft Authorised Education Reseller

05 апреля 2016, Россия, Москва, press-release.ru. Компания «Астерит» – один из крупнейших поставщиков решений и услуг для построения эффективной и безопасной IT-инфраструктуры предприятия, вновь подтвердила статус Microsoft Authorised Education Reseller (AER).

Напомним, «Астерит» на протяжении многих лет тесно сотрудничает с организациями образовательной среды, реализуя программные продукты и внедряя решения, позволяющие не только отладить учебный процесс и сделать его более эффективным, но и оптимизировать ИТ-инфраструктуру самих учреждений, например, обезопасить сети от внешних угроз или организовать защиту персональных данных в соответствие с Федеральным законом ФЗ-152 «О персональных данных».

Продлив партнерский статус Microsoft Authorised Education Reseller (AER), компания «Астерит» в очередной раз подтвердила свои компетенции в области работы с образовательными учреждениями. Сегодня «Астерит» имеет полный набор необходимых ресурсов для того, чтобы помогать образовательным учреждениям в выборе и приобретении решений и программного обеспечения на базе академических версий продуктов Microsoft по самым выгодным для них ценам.

Статус Microsoft Authorised Education Reseller (AER) свидетельствует о том, что компания «Астерит» является высококвалифицированным партнером Microsoft, компетентно работающим с академическими программами лицензирования.

«Получение статуса Microsoft Authorised Education Reseller подтверждает компетенции компании «Астерит» как эксперта в работе с академическими программами лицензирования, а так же наш опыт и надежность. Благодаря этому статусу мы можем и дальше гарантировать образовательным учреждениям полный набор решений от компании Microsoft и квалифицированную помощь наших специалистов», - отмечает руководитель отдела проектов «Астерит» Михаил Пузин.

Опыт и решения компаний

«ДиалогНаука» провела тест на проникновение для ПАО «Запсибкомбанк»

09 марта 2016, Россия, Москва, dialognauka.ru. Компания «ДиалогНаука», системный интегратор в области информационной безопасности, выполнила работы для ПАО «Запсибкомбанк» по проведению теста на проникновение, позволяющего определить степень защищённости автоматизированной системы банка от внешних и внутренних атак со стороны потенциальных злоумышленников.

«ДиалогНаука» была выбрана в качестве исполнителя по итогам оценки специалистами ПАО «Запсибкомбанк» предложений нескольких российских компаний – поставщиков услуг в сфере информационной безопасности. В результате работ специалисты заказчика получили объективную информацию о состоянии защиты информационных систем банка и возможных шагах по ее дальнейшему совершенствованию и развитию.

ПАО «Западно-Сибирский коммерческий банк» (Запсибкомбанк) является одним из крупнейших по размеру активов региональным банком, занимающим лидирующую позицию среди банков Тюменской области. Основные направления деятельности — розничный бизнес, кредитование предприятий и физлиц, привлечение средств во вклады и расчетно-кассовое обслуживание. Банк предоставляет своим клиентам широкий спектр высокотехнологичных банковских услуг и выделяет как одну из основных задач обеспечение высокого уровня информационной безопасности автоматизированной банковской системы.

Для решения этой задачи в частности необходима независимая и объективная оценка текущего состояния защиты от внешних и внутренних угроз со стороны потенциальных злоумышленников. Именно поэтому руководством ПАО «Запсибкомбанк» было принято решение провести тест на проникновение, который после анализа предложений от возможных поставщиков услуг был доверен консультантам компании «ДиалогНаука».

Тестирование на проникновение представляло из себя моделирование атак потенциальных злоумышленников на информационные активы ПАО «Запсибкомбанк». Были смоделированы атаки, направленные на выявление организационных, эксплуатационных и технологических уязвимостей в инфраструктуре банка. Дополнительно была проведена базовая оценка существующих процессов обеспечения информационной безопасности и разработан перечень мероприятий по повышению уровня ИБ ПАО «Запсибкомбанк».

По результатам теста на проникновение консультантами «ДиалогНауки» был подготовлен отчет, который включал в себя описание границ аудита, использованных методов и средств, перечень выявленных уязвимостей и недостатков, ранжированных по уровню риска их использования потенциальными злоумышленниками. Были описаны предпринятые сценарии проникновения и достигнутые результаты, проведена оценка рисков ИБ и процессов обеспечения ИБ банка. В заключение были представлены рекомендации по устранению выявленных уязвимостей и совершенствованию процессов обеспечения ИБ ПАО «Запсибкомбанк», а также план работ по совершенствованию процессов обеспечения ИБ.

КОМПЕТЕНТНО: Виктор Чеснов, ПАО «Запсибкомбанк», вице-президент

<<< ИТ-инфраструктура финансовой организации выполняет основную роль в деле обеспечения непрерывности процессов банка и сервисов для клиентов. А тест на проникновение позволяет оценить, насколько эффективна на практике защита этой инфраструктуры от атак реальных хакеров. Поэтому мы считаем важным данный проект. По результатам теста на проникновение мы получили исчерпывающую информацию о текущем состоянии периметра защиты корпоративной системы и о возможных шагах по ее совершенствованию. Уверен, что это будет способствовать в будущем повышению уровня информационной безопасности банка. >>>

Avito перенесла в Россию всю IT-инфраструктуру согласно закону о персональных данных

14 марта 2016, Россия, Москва, tass.ru. "С января 2016 года все серверное оборудование Avito полностью введено в коммерческую эксплуатацию в дата-центре DataSpace1 в Москве", - отмечается в сообщении компании.

Владелец сайта бесплатных объявлений - интернет-компания Avito перенесла из Швеции в Россию всю свою IT-инфраструктуру для соответствия закону, предусматривающему хранение персональных данных россиян в РФ. Об этом говорится в сообщении компании.

"С января 2016 года все серверное оборудование Avito полностью введено в коммерческую эксплуатацию в дата-центре DataSpace1 в Москве", - отмечается в сообщении. "Все данные пользователей онлайн-площадки Avito хранятся исключительно на территории России в полном соответствии с требованиями к хранению персональных данных", - подчеркнули в интернет-компании.

В пресс-службе Avito ТАСС пояснили, что компания не собирается выкупать этот дата-центр. Расходы на аренду ЦОД и перенос данных в Avito не комментируют.

Дата-центр DataSpace, запущенный в 2012 г., был выбран на конкурсной основе по совокупности экономических, технических и эксплуатационных характеристик. "DataSpace способен решать сервисные и проектные задачи, возникающие в связи с постоянным развитием портала", - пояснил вице-президент по продуктам и технологиям Avito Дмитрий Ковалев, слова которого приводятся в сообщении.

Закон о хранении персональных данных, вступивший в силу 1 сентября 2015 г., обязывает компании хранить и обрабатывать персональные данные граждан РФ на территории России. Часть международных компаний (например, eBay и AliExpress) уже заявили о том, что соответствуют новому закону. Однако другие игроки рынка, которые попадают под действие закона (в частности Google и Facebook), до сих пор не комментируют данный вопрос.

Facebook, Google и WhatsApp усилят шифрование данных

15 марта 2016, США, rusbenelux.com. Крупнейшие американские ИТ-компании, включая Facebook, Google и WhatsApp, планируют усилить защиту пользовательских сообщений в противовес желанию властей иметь возможность получать к ним доступ при необходимости.

Усиление защиты

Facebook, Google, WhatsApp и Snapchat планируют предпринять дополнительные меры для защиты пользователей от перехвата сообщений и усилить шифрование, как и Apple. Об этом сообщает Guardian со ссылкой на осведомленные источники. По их словам, WhatsApp планирует сделать соответствующий анонс уже в ближайшие несколько недель.

Что планирует сделать WhatsApp

В настоящее время компания шифрует сообщения между пользователями приложения на Android и iOS. К этому она планирует добавить шифрование голосовых вызовов, поддержка которых появилась в 2015 г. Кроме того, в WhatsApp планируется добавить шифрование групповых чатов, сообщили два источника. Все это затруднит и без того нелегкую задачу властей по получению доступа к переписке преступников и подозреваемых, отмечает Guardian.

На зло властям

Сообщение о намерении WhatsApp усилить защиту появилось спустя несколько дней после того как стало известно, что власти США обсуждают пути получения доступа к переписке пользователей WhatsApp. Напомним, что компания начала шифровать чаты с 2015 г. Никаких официальных шагов в отношении мессенджера Министерство юстиции США пока не предприняло.

Facebook, Snapchat и Google

Facebook следует в том же направлении, что и WhatsApp. Компания планирует усилить защиту сообщений в своем Facebook Messenger. У The Guardian нет подробностей о том, что именно делает компания, а также о том, какие шаги предпринимает Snapchat.

Что касается Google, в 2014 г. она анонсировала проект под названием End to End, который должен был предложить людям простой способ обмена сообщениями со сквозным шифрованием (когда никто, кроме отправителя и получателя, не может их прочесть). Проект долгое время находился в стадии стагнации и сейчас, по всей видимости, Google вновь начала проявлять к нему интерес.

Арест топ-менеджера Facebook

В начале марта 2016 г. полиция бразильского Сан-Паулу арестовала на несколько суток вице-президента местного филиала Facebook за отказ дать доступ к переписке WhatsApp. В компании Facebook этот случай назвали «вопиющим». В ответ на запрос правоохранительных органов руководство Facebook заявило, что оно не может выполнить просьбу властей физически, так как WhatsApp является другой компанией, доступа к серверам которой она не имеет.

Напомним, что в 2014 г. WhatsApp был приобретен компанией Facebook за $19 млрд.

Противостояние Apple и ФБР

16 февраля 2016 г. суд в США обязал Apple помочь ФБР получить доступ к информации, хранящейся во внутренней памяти iPhone 5c, владелец которого, радикально настроенный исламист, в декабре 2015 г. в американском городе Сан-Бернардино застрелил 14 человек (он был убит в перестрелке с полицией). Агенты утверждают, что данные на его телефоне очень важны для расследования.

Однако генеральный директор AppleТим Кук (Tim Cook) публично отказался предоставить доступ. Он заявил, что это поставит под угрозу частную жизнь всех пользователей, и добавил, что власти заставляют его не только сообщить пароль к смартфону убийцы, но и встроить в iOS «черный ход», который в будущем позволит правоохранительным органам самостоятельно получать доступ к данным в случае необходимости, не прибегая к помощи кого бы то ни было (власти США настаивают на такой возможности не первый год).

Отказ Apple вызвал широкую поддержку в индустрии. Упомянутые выше Facebook, Snapchat и Google, а также другие представители высокотехнологичной индустрии — Amazon, Microsoft и Twitter — поддержали ее позицию.

На днях по поводу конфликта высказался президент США Барак Обама (Barack Obama). Он заявил, что нельзя лишать правительство возможности обеспечивать безопасность граждан. Поэтому американским компаниям не следует выпускать такие мобильные устройства, к которым власти не могут получить доступ в случае серьезной необходимости.

Актуальная защита данных с "ТСС"

15 марта 2016, Россия, Москва, spbdnevnik.ru. В современном мире нельзя пренебрегать безопасностью персональных данных. В противном случае, может пострадать не только частное имущество, но и целый бизнес. Промышленный шпионаж достаточно развит, поэтому ИСПДн (информационная система персональных данных) должна охраняться на высшем уровне. Раньше каждая компания самостоятельно заботилась о том, чтобы сведения оставались внутри фирмы, но после 2006 года вмешалось законодательство, и теперь система охраны должна соответствовать многочисленным нормам. Ее взялись обеспечивать многие организации, но преуспеть удалось далеко не многим.

Одной из самых заметных за границей и на территории стала фирма "ТСС". Многолетний опыт позволил сотрудникам не только помогать в установке сертифицированных систем безопасности, но и стал разрабатывать свои новейшие методы, которые получили одобрение Федерального законодательства. Если предприятие не соблюдает меры, установленные законом, предусмотрены большие штрафные санкции и даже полная ликвидация компании.

Даже устанавливая систему, которая соответствует сертификации, ни один владелец бизнеса не защищен от некоторых прорех. В связи с этим, компания "ТСС" разработала современные инструменты регулирования, которые разграничивают доступ на две серии: Diamond ACS и VPN/FW. Для того чтобы определить, какая из систем подходит для защиты информации наиболее точно, следует сначала провести полный аудит уже существующих проектов. После того, как были собраны необходимые данные, сотрудники готовят специальную документацию, которая носит организационный и распорядительный характер. Только потом происходит установка необходимого оборудования и ПО, которые смогут обеспечить высокий уровень защиты.

Когда установлены все компоненты, создается система, с помощью которой будет осуществляться контроль за правильным функционированием и разграничение доступа для разной аппаратуры.

Специалисты компании "ТСС" обязательно проводят обучение персонала, чтобы не возникало сбоев и проблем в работе оборудования. Заключительным этапом становится аттестация всей системы, что соответствует требованиям безопасности. Легкость интеграции с уже установленным ПО и оборудованием позволяет максимально масштабировать принимаемые решения.

Heineken внедрила DLP

18 марта 2016, Россия, Москва, tadviser.ru. Российское подразделение международного концерна HEINEKEN N.V., лидирующей международной пивоваренной компании в мире - ООО «Объединенные пивоварни Хейнекен», работает на российском рынке с февраля 2002 года, когда был приобретен первый завод в Санкт-Петербурге. На сегодняшний день в составе компании 8 заводов, атакже офисы отдела продаж, расположенные в разных регионах России. Все офисы объединены в единую локальную сеть средствами MPLS.

Ежегодно компания проводит корпоративные аудиты информационной безопасности на соответствие глобальной политике по ИБ, базирующейся на требованиях ISO 27001, со стороны глобального офиса Хейнекен в Амстердаме. Корпоративная политика информационной безопасности HEINEKEN требует обеспечения контроля за утечками конфиденциальной информации.

В целях выполнения требований корпоративной политики, а так же требований Федерального закона № 152 «О персональных данных», специалисты по ИБ ООО «Объединенные пивоварни Хейнекен» в 2010 году рассмотрели ряд решений, решающих проблему контроля доступа к внешним устройствам хранения и передачи данных.

Как рассказывает Сергей Вениаминович Поточкин, Менеджер по Информационной безопасности ООО «Объединенные пивоварни Хейнекен», «Дизайн нашей инфраструктуры определял, что система контроля портов и устройств должна базироваться на локальных агентах, устанавливаемых на конкретных компьютерах. Также система должна быть произведена российским производителем и требовать минимальных ресурсов при поддержке. На момент выбора такой системы в 2010 г DeviceLock являлся оптимальным решением для нашей компании».

Кроме того, для противодействия утечкам информации через электронную почту, мессенджеры, файлообменные сервисы и другие каналы сетевых коммуникаций, ООО «Объединенные пивоварни Хейнекен» также использует решение NetworkLock в составе комплекса DeviceLock DLP.

Важным фактором при выборе NetworkLock стала архитектурная особенность продукта – возможность контролировать все потоки данных (как сетевые коммуникации, так и подключаемые устройства) на уровне одного локального агента, устанавливаемого непосредственно на контролируемых компьютерах. В перспективе специалисты ИБ компании рассматривают возможность использования технологий контентной фильтрации, предоставляемых комплексом DeviceLock DLP.

«Развертывание DLP-системы на основе комплекса DeviceLock DLP мы проводили собственными силами с использованием Microsoft SCCM, при этом DLP-политики и настройки системы распространялись через групповые политики домена Active Directory. Сегодня мы используем связку DeviceLock + NetworkLock, данные с которых поставляются на единый управляющий сервер. Как результат - есть контроль за информацией, возможность расследования и предотвращения инцидентов с утечками конфиденциальной информации», резюмирует С.В.Поточкин.

«Федеральная пассажирская компания» совместно с «Инфосистемами Джет» построила комплексную систему ИБ

22 марта 2016, Россия, Москва, iksmedia.ru. «Федеральная пассажирская компания» (ФПК) и компания «Инфосистемы Джет» создали комплексную систему контроля и мониторинга ИБ на базе системы аналитики Solar inView компании Solar Security.

К Solar inView подключены несколько ключевых источников данных, таких как кадровые системы, DLP-решение Solar Dozor, средства мониторинга MaxPatrol.

Это позволило ИБ-службе оперативно оценивать текущее состояние ИБ и определять причины возникновения инцидентов в режиме реального времени, а также отслеживать динамику изменений в системе защиты, сообщили в «Инфосистемах Джет». Сроки выявления, реагирования и устранения инцидентов сократились с нескольких дней до нескольких часов.

Эксперты «Инфосистем Джет» проанализировали процессы обеспечения и управления ИБ, существующие источники данных, выделили наиболее критичные и часто используемые, а также определили способы извлечения данных. По итогам обследования была выполнена модернизация комплекса по защите от утечек информации: подключен дополнительный функционал контроля информационных объектов, позволяющий более точно описывать в политике объекты поиска (документы, тексты), снижая общее количество ложных срабатываний.

Модернизированный комплекс позволяет обеспечить контроль сообщений сотрудников по следующим каналам: корпоративная почта, веб-почта, социальные сети, форумы, мессенджеры, облачные хранилища данных, файлы, размещенные на общих локальных файловых ресурсах. Охват DLP-системы расширен с 1500 до 3000 пользовательских рабочих станций, рассказали в компании.

Модернизированный комплекс позволяет обеспечить контроль сообщений сотрудников по следующим каналам: корпоративная почта, веб-почта, социальные сети

Для системы визуализации, разноуровневой аналитики и мониторинга эффективности ИБ Solar inView были проанализированы данные от источников с точки зрения формата, возможностей для преобразования и связываемости друг с другом. Это позволило разработать набор высокоуровневых показателей эффективности.

Для каждой из подключаемых систем реализован набор фильтров, позволяющих создавать различные виды отчетов, отображаемых в виде интуитивно понятных диаграмм, гистограмм, графиков и таблиц, с возможностью детализации по каждому объекту до нужного уровня (количество уровней не ограничено).

«Внедрение системы и ее интеграция с выделенным пулом источников данных прошли поэтапно, без прерывания функционирования систем безопасности, что позволило специалистам ФПК работать с системой уже на этапе ее внедрения», — отметил Игорь Шелест, ведущий системный архитектор компании «Инфосистемы Джет».

Денис Назаренко, руководитель отдела по работе с партнерами компании Solar Security, со своей стороны заявил: «Компания “Инфосистемы Джет” является одним из наших ключевых партнеров и обладает глубокой экспертизой по продуктам Solar inView и Solar Dozor. Знания и опыт специалистов партнера позволяют им самостоятельно выполнять сложные интеграционные проекты на базе продуктов Solar Security в инфраструктуре заказчика».

КОМПЕТЕНТНО: Алексей Земцов, «Федеральная пассажирская компания», начальник отдела информационной и внутренней безопасности Управления корпоративной безопасности

<<< Различные сценарии анализа данных - от статистического отслеживания трендов, выявления корреляций, проверки гипотез и т.п. до анализа типа “что, если...” и многомерного интерактивного анализа данных “вглубь” - позволяют нам объективно оценить, насколько внедряемые меры безопасности соответствуют требованиям бизнеса. Мы можем не только выявлять узкие места, находить причины их возникновения и устранять, но и планировать развитие системы обеспечения ИБ в долгосрочной и краткосрочной перспективе. >>>

Google и Microsoft создают электронную почту, которую нельзя прослушать

22 марта 2016, Россия, Москва, rublacklist.net. Крупнейшие провайдеры электронной почты совместно с независимыми специалистами по информационной безопасности предложили создать новое расширение для почтового протокола SMTP, которое позволило бы повысить уровень защиты электронной почты, дополнительно защитив ее от перехвата.

Новое расширение для SMTP

Группа независимых исследователей совместно с пятью компаниями — Google, Microsoft, Yahoo, Comcast и LinkedIn — предложили стандартизировать новое расширение для протокола SMTP, которое сделает электронную почту более защищенной от перехвата. Свое предложение они направили в организацию Internet Engineering Task Force (IETF).

Появление STARTTLS

Разработанный в 1982 г. протокол для отправки электронной почты SMTP не поддерживает шифрование. Он был изобретен тогда, когда интернет только развивался, и необходимости в защите переписки между всего лишь несколькими тысячами подключенных к сети компьютеров не было. В 2002 г. для SMTP было разработано расширение STARTTLS, позволившее отправлять письма в зашифрованном виде.

После того как в 2013 г. Эдвард Сноуден (Edward Snowden) рассказал о приемах Агенства национальной безопасности США, шифрование набрало популярность. В 2014 г. соцсеть Facebook, отправляющая миллиарды почтовых уведомлений в день, выяснила, что 58% этих уведомлений проходят по защищенным каналам. К августу того же года эта цифра возросла до 95%.

Недостаток STARTTLS

Расширение STARTTLS используется и по сей день, но оно не гарантирует защиту данных, так как содержит в себе ряд изъянов, позволяющих хакерам успешно выполнить свою работу. Используя недостатки расширения, злоумышленник может фальсифицировать почтовый сервер и убедить приложение на ПК или другой почтовый сервер отправить сообщение в виде простого текста. Сделать это можно путем принудительного отказа от шифрования (в штатном режиме такая необходимость может возникнуть тогда, когда принимающий сервер не поддерживает шифрование) либо путем использования поддельного сертификата.

Функция STS

Поэтому авторы инициативы предложили создать расширение STS (Strict Transport Security), которое обеспечит надежную проверку подлинности участников соединения. В теории STS аналогично расширению HSTS для HTTPS. Как и HSTS, оно должно обеспечить зашифрованный обмен служебными сообщениями между сторонами. STS будет гарантировать безопасное соединение и определит поведение серверов на тот случай, когда подлинность одного из них проверить не удастся. Что будет предприниматься в этом случае, не уточняется.

Правила STS будут задаваться посредством специальных DNS-записей, которые будут добавляться к домену провайдера почтового сервиса. Предполагается, что это позволит защитить пользователей электронной почты от атак вида «человек посередине», когда злоумышленник имеет возможность фальсифицировать второго участника соединения и получить его данные.

Статус обсуждения

Пока расширение STS представлено в виде черновика стандарта со сроком действия до 19 сентября 2016 г. По мере возникновения интереса, работа над стандартом будет продолжена. Черновики в IETF не имеют никакого официального статуса и могут быть удалены в любой момент. Официальный статус появляется только после того, как за разработку берется рабочая группа либо когда документ приобретает внутренний статус Requests for Comments.

Yahoo внедряет метод беспарольной авторизации

24 марта 2016, США, threatpost.ru. В очередной попытке избавиться от паролей (хотя бы в рамках приложений одной компании) Yahoo разработала и представила стабильную версию метода аутентификации под названием Account Key. Эта функция, представляющая собой разновидность системы двухэтапной аутентификации (без первого этапа), позволяет пользователям Yahoo входить в приложения Finance, Fantasy, Mail, Messenger и Sports с устройств iOS и Android. При попытке входа в приложение пользователь получает push-уведомление, через которое он может залогиниться в аккаунт одним нажатием.

Пользователи обычно не выходят из учетных записей в мобильных приложениях, но в приложениях Yahoo им нужно будет проходить аутентификацию при каждом запуске программы, получая push-уведомления.

Компания не скрывает, что хочет отказаться от использования паролей. «Пароли могут создавать проблемы: их легко забыть или перепутать, а слабые пароли нередко попадают в руки киберпреступников», — написал в корпоративном блоге Ловлеш Чхабра (Lovlesh Chhabra), менеджер по продукту в Yahoo.

Компания начала продвигать идею «паролей по запросу» примерно год назад. Как и при применении Account Key, пользователи могли отказаться от пароля и задействовать мобильный телефон для аутентификации. После запуска программы пользователи могли выбрать опцию доставки пароля к сервисам Yahoo в текстовом сообщении.

В октябре компания анонсировала технологию Account Key, в некоторой степени повторяющую особенности «пароля по запросу», и заявила, что новый механизм — следующий этап миссии по упразднению паролей на пути к «беспарольному» будущему. Поборники приватности давно критикуют пароли как устаревшую идею, но пока неясно, насколько далеко будущее, о котором мечтает Yahoo.

В 2011 году Mozilla уже пыталась привлечь жителей Сети к использованию своей системы аутентификации Persona. Децентрализованная система использовала для аутентификации пользователя email-адрес; тогда разработчики уверяли, что это позволит не вводить пароль при входе в каждый веб-сервис. Хотя Mozilla выпустила бета-версии Persona в 2012 и 2013 годах, позже компания признала, что из-за низкого количества пользователей и ограниченных ресурсов этот инструмент будет выведен из эксплуатации к 30 ноября.

Спустя почти четыре года после масштабной утечки, скомпрометировавшей учетные данные более 450 тыс. пользователей, Yahoo последовательно развивает средства обеспечения приватности. В конце прошлого года Боб Лорд (Bob Lord), директор по информационной безопасности, заявил, что компания последует примеру Twitter и будет уведомлять пользователей о возможных атаках со стороны спецслужб. Очевидно, партнерские отношения Yahoo с независимой программой Bug Bounty HackerOne также оказались довольно плодотворными.

С момента запуска программы в 2013 году Yahoo закрыла 2875 обнаруженных уязвимостей и выплатила исследователям более $1 млн, включая щедрую премию в $10 тыс., которая досталась финскому хакеру Йоуко Пюннонену (Jouko Pynnonen) за обнаружение в январе этого года критической уязвимости в Yahoo Mail.

ICQ зашифрует аудио- и видеозвонки

29 марта 2016, Россия, Москва, izvestia.ru. Компания Mail.Ru Group работает над протоколом шифрования аудио- и видеозвонков для своего мессенджера ICQ. Об этом «Известиям» рассказали несколько источников в компании. В пресс-службе ICQ от комментариев отказались.

— Шифровка и расшифровка аудио- и видеообщения будут производиться на конечных устройствах пользователей, т.е. даже если во время работы будет задействован сервер, то посмотреть или послушать на нем ничего не удастся, — рассказал собеседник «Известий».

Для шифровки данных командой мессенджера был выбран протокол Диффи–Хеллмана. Он позволяет двум пользователям (в своих примерах изобретатели их называют Алисой и Бобом) получить общий секретный ключ, используя открытый канал связи, к которому может подключиться злоумышленник (его представляют как Еву). Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования. Принцип работы такого протокола был представлен еще в 1976 году.

— Сейчас шифрование аудио- или видеоразговоров через мессенджер не происходит, в результате становится возможным проведение атаки «человек посередине», — сообщил источник, близкий к Mail.Ru Group.

«Человек посередине» — это тип перехвата данных, при котором злоумышленник подключается к каналу обмена данными (например, к Wi-Fi-роутеру) между пользователями или между пользователем и сервером. Далее из всего трафика передаваемой информации злоумышленник выбирает нужный и слушает, о чем собеседники говорят, или видит, чем они обмениваются.

Ведущий аналитик Технического центра Интернет Александр Венедюхин объяснил, что протокол Диффи–Хеллмана от такой атаки не защищает.

— Злоумышленник, перехватив канал, каждой стороне выдает себя за другую сторону. Иными словами Алиса не может в рамках Диффи–Хеллмана определить, что обменялась сообщениями и выработала общий секретный ключ именно с Бобом, а не с Евой, — объяснил Венедюхин. — Это хороший протокол. На нем всё практически работает. Просто для защиты от «человека посередине» нужен дополнительный механизм, позволяющий Алисе и Бобу определить, что они именно между собой разговаривают. Обычно для этого служит механизм электронно-цифровой подписи.

По мнению бывшего гендиректора координационного центра национального домена сети интернет Андрея Колесникова, у ICQ есть техническая возможность сделать так, чтобы никто, в том числе и администрация сервиса, не смог подслушать или подсмотреть общение двух пользователей.

— Самое главное в вопросах безопасности — это вопрос веры. Пользователь должен решить, доверяет или нет, — отметил Андрей Колесников. — Так же, как и в случае с Telegram. Павел Дуров (основатель мессенджера Telegram. — «Известия») говорит, что они никому и ничего не раскрывают. Раз его мессенджером пользуются, значит, ему доверяют.

В России сейчас большую популярность набирает мессенджер Telegram, который своей главной фишкой декларирует безопасность, благодаря отличному шифрованному протоколу. Его создал бывший гендиректор «ВКонтакте». Свой сервис разработчики охарактеризовали так: «сверхбыстрый, простой, безопасный и абсолютно бесплатный». В этом продукте используется протокол передачи данных Mobile Telecommunication Protocol (MTProto), разработанный братом Павла Дурова Николаем, бывшим техническим директором «ВКонтакте».

Как писали ранее «Известия», «ВКонтакте» готовит выпуск своего мессенджера, который будет работать над урезанной версией протокола MTProto собственной разработки. Он позволит ускорить отправку и прием сообщений.

Директор по внешним коммуникациям Rambler&Co Матвей Алексеев уверен, что шифрование общения — это отчетливый тренд.

— Это правильное решение с точки зрения компании, любой барьер на пути злоумышленников для пресечения несанкционированного доступа к общению — это хорошо, — считает Матвей Алексеев. — После заявлений Джулиана Ассанджа и Эдварда Сноудена люди поняли, что их могут читать где угодно. И, учитывая поступающую информацию о взломах различных сервисов с приватными данными, тренд внедрения протоколов безопасности понятен и значим.

Mail.Ru Group приобрела ICQ у американской AOL в июле 2010 года за $187,5 млн. В свою очередь, AOL приобрела ICQ (тогда — израильская компания Mirabilis) в 1998 году. Сумма сделки составила примерно $400 млн.

АКБ "Российский Капитал" (ПАО) защищает данные с помощью DeviceLock DLP

30 марта 2016, Россия, Москва, itsec.ru. АКБ "Российский Капитал" (ПАО) - универсальный банк с широкой филиальной сетью, входящий в ТОП-50 российских банков, который оказывает услуги для всех категорий клиентов, а также входит в перечень кредитных организаций, имеющих право работать с предприятиями стратегического значения, согласно Федеральному закону 213-ФЗ.

С 2009 года основным акционером банка является Государственная корпорация "Агентство по страхованию вкладов". Банк включает в себя порядка 140 внутренних структурных подразделений: филиалов, дополнительных офисов и операционных касс в 27 регионах России.

Система обеспечения информационной безопасности банка построена в соответствии со стандартом Банка России СТО БР ИББС.

В 2011 году АКБ "Российский капитал" после рассмотрения ряда систем защиты информации от утечек начал пилотную эксплуатацию программного продукта DeviceLock разработки российской компании Смарт Лайн Инк. Как рассказывает Начальник Управления ИБ АКБ "Российский Капитал" Антон Сергеевич Сергеев, "Выбор продукта делался из целого ряда аналогов. DeviceLock показал существенно большую функциональную оснащенность".

В 2015 г. Управление ИБ Банка расширило область применения DLP-решения от Смарт Лайн Инк, начав в дополнение контролю периферийных устройств и портов использование компонента NetworkLock комплекса DeviceLock DLP в целях контроля передачи данных по каналам сетевых коммуникаций. Как результат, "Управление ИБ Банка "Российский Капитал" удовлетворено результатами внедрения комплекса DeviceLock DLP, благодаря этому решена задача несанкционированной утечки конфиденциальной информации", - заключает Антон Сергеев.

«Ростелеком» в 2016 году продолжит развивать инфраструктуру электронного правительства в Кузбассе

31 марта 2016, Россия, Кемеровская обл., news.vse42.ru. ПАО "Ростелеком" и Департамент информационных технологий Кемеровской области подписали Государственный контракт на оказание услуг по эксплуатации региональной части инфраструктуры электронного правительства.

По условиям заключенного контракта, "Ростелеком" предоставит собственную телекоммуникационную инфраструктуру для исполнительных органов государственной власти и органов местного самоуправления и обеспечит безопасность и защиту персональных данных, сервисную и техническую поддержку, а также круглосуточную консультационную поддержку пользователей региональной инфраструктуры "электронного правительства".

"Ростелеком" совместно с Администрацией Кемеровской области активно реализует государственную программу "Информационное общество", – отметил директор Кемеровского филиала компании Константин Ярыгов. – На сегодняшний день в электронный вид переведены 94 государственные и муниципальные услуги, и это далеко не предел. Мы готовы по заказу администрации региона и дальше расширять этот список услугами, востребованными населением".

ТЕХНОЛОГИИ. ОБОРУДОВАНИЕ. ПРОДУКТЫ. УСЛУГИ
Сертификация. Лицензирование. Стандарты

Антивирусы линейки Dr.Web 10.0 успешно прошли сертификационные испытания в испытательной лаборатории НПО «Эшелон»

21 марта 2016, Россия, Москва, cnews.ru. Средства антивирусной защиты линейки Dr.Web 10.0 успешно прошли сертификацию ФСТЭК России. Полученный сертификат подтверждает, что средства антивирусной защиты линейки Dr.Web 10.0 позволяют обеспечивать защиту систем, работающих с персональными данными, государственной тайной и другой информацией, доступ к которой должен быть ограничен в соответствии с требованиями законодательства РФ.

Сертификат ФСТЭК России №3509 выдан 27.01.2016 года и действителен три года – до 27.01.2019. Сертификационные испытания проводились испытательной лабораторией НПО «Эшелон».

За последние несколько лет эксперты лаборатории НПО «Эшелон» провели испытания более 600 продуктов ведущих российских и зарубежных производителей: «Код безопасности», «Анкад», Check Point Software Technologies Ltd., Cisco Systems Inc, ESET, IBM, McAfee, Microsoft и др.

СУБД «Линтер Бастион» рекомендована для применения с ОС «Роса»

21 марта 2016, Россия, Москва, tadviser.ru. Российские компании «НТЦ ИТ Роса» и «Релэкс» завершили тестирование СУБД «Линтер Бастион» на совместимость с сертифицированными операционными системами «Роса Никель», «Роса Кобальт» и «Роса Хром». Результаты тестирования показали полную работоспособность «Линтер» в средах ОС «Роса». Компании-производители рекомендуют свои продукты для применения в автоматизированных системах коммерческих организаций, органов государственного управления и предприятий ОПК в качестве базового системного программного обеспечения.

По словам представителей «Релэкс», использование разработанных в России системы управления базами данных и операционных систем позволит предприятиям создавать и применять решения, отвечающие требованиям российского законодательства. Это стало наиболее актуально после вступления в силу федерального закона №188-ФЗ от 29 июня 2015 г. «О внесении изменений в федеральный закон "Об информации, информационных технологиях и о защите информации"».

Система управления базами данных «Линтер Бастион» полностью разработана в России и сертифицирована ФСТЭК России и Министерством обороны РФ. Благодаря должной защищенности «Линтер Бастион» позволяет строить информационные системы любого уровня безопасности, в том числе предназначенные для обработки и хранения секретной информации.

Все модули защиты СУБД реализованы в соответствии с требованиями основных руководящих документов ФСТЭК России и соответствуют требованиям федеральных законов №149-ФЗ «Об информации, информационных технологиях и о защите информации», №152-ФЗ «О персональных данных» и Доктрине информационной безопасности Российской Федерации (утвержденной Президентом РФ 09.09.2000 № Пр-1895).

Семейство операционных систем «Роса Кобальт» сертифицировано ФСТЭК России для работы с конфиденциальной информацией, включая персональные данные. Семейство «Роса Хром» сертифицировано ФСТЭК России и рекомендуется для обработки сведений, составляющих государственную тайну с грифом не выше «секретно». Наконец, ОС «Роса Никель» сертифицирована Восьмым управлением ГШ ВС РФ и рекомендуется для обработки сведений, составляющих государственную тайну с грифом не выше «секретно».

Минкомсвязи пустило в Реестр российского ПО софт без лицензий ФСТЭК

22 марта 2016, Россия, Москва, zoom.cnews.ru. Экспертному сообществу удалось убедить Минкомсвязи в том, что отсутствие лицензии ФСТЭК не является поводом не включать программный продукт в Реестр российского софта. Определение «отечественности» ПО и его лицензирование, необходимое для использования в госорганах, признаны независимыми друг от друга задачами.

Письмо Минкомсвязи

Минкомсвязи распространило среди государственных и муниципальных заказчиков письмо от 15 марта 2016 г. за подписью главы ведомства Николая Никифорова с разъяснениями о применении Реестра российского ПО в части соблюдения требований по защите информации. Текст документа приводит ассоциация разработчиков программных продуктов «Отечественный софт».

Министерство обращает внимание респондентов на необходимость самостоятельного принятия решений об установлении требований по защите информации, содержащейся в их информационных системах, в том числе, при выборе из Реестра общесистемного, прикладного, специального ПО, ИТ, а также средств защиты информации. Эти решения госзаказчики должны принимать, ориентируясь на соответствующие требования Федеральной службы по техническому и экспортному контролю (ФСТЭК), федеральный закон «Об информации, ИТ и о защите информации» и постановление Правительства о защите персональных данных.

Что это означает

Суть сообщения Минкомсвязи разъяснила CNews президент группы компаний InfoWatch Наталья Касперская. Она отмечает, что среди критериев попадания в Реестр есть подпункт, который гласит, что если программа относится к средствам защиты информации, то на нее обязательно нужна лицензия ФСТЭК.

«Однако на определенном этапе стало понятно, что этот подпункт избыточен, ведь госкомпании в любом случае обязаны получать лицензию ФСТЭК на использование систем защиты информации, — говорит Касперская. — Получается, что по этому подпункту экспертный совет должен запрашивать данные о лицензиях у компаний-разработчиков, а компании должны эти данные собрать и предоставить. Если лицензий у них нет, то их программные продукты не попадают в реестр, и таким образом мы, по сути, ограничиваем свободную конкуренцию. Но для попадания в реестр важно соблюдение критериев "отечественности", а не наличие лицензий внутренних контролирующих органов».

По словам Касперской данное противоречие и привело к тому, что у АРПП «Отечественный софт» появилось предложение разделить зоны ответственности: экспертный совет должен заниматься формированием реестра, а ФСТЭК — выдавать лицензии. «Это две разные задачи, и я считаю данное предложение абсолютно правильным», — заключает топ-менеджер.

Дополнения экспертов

Исполнительный директор ассоциации разработчиков программных продуктов «Отечественный софт» Евгения Василенко добавляет к этому, что быть законодательно закрепленным ориентиром для госзаказчиков (которым лицензии ФСТЭК могут потребоваться) — это хоть и важнейшая, но не единственная задача Реестра. В будущем на Реестр сможет опираться государство, например, при оказании поддержки отечественным разработкам, причем в тех сферах, где использование этих решений не будет сопряжено с регулированием со стороны ФСТЭК.

«Сертификация не имеет прямого отношения к определению происхождения софта. Она занимает значительное время и требует существенных затрат, — говорит Василенко. — Эти факторы не должны затруднять работу экспертного совета и процедуру формирования Реестра».

Избыточность обязательных требований по сертификации на конкретном примере поясняет эксперт по информационной безопасности компании «Аладдин Р. Д.» Сергей Котов. «Если в программном продукте реализована функция доступа по паролю для разных ролей пользователя, скажем, для главного бухгалтера и счетовода (функция разграничения доступа), требуется ли для такого ПО сертификат ФСТЭК на средство защиты от несанкционированного доступа? — задается он вопросом. — Ответ простой: если продукт является средством защиты информации и применяется в органах госвласти, то требуется. Если функция другая, например, бухгалтерский учет, то нет, хотя, при желании, можно попытаться получить».

По убеждения Котова, во втором случае эффект от сертификата вряд ли можно считать сопоставимым с теми трудозатратами на корректную реализацию функции, которые позволят этот сертификат получить.

«И никаких противоречий с требованиями регуляторов в документе Минкомсвязи нет — обычное разъяснение для тех госорганов, которые “не в теме”, а больше, как мне кажется, попытка подстелить соломку на поролоновые маты — экологично…», — завершает свою мысль Котов.

В данном случае его мнение разделяет и генеральный директор компании «Код безопасности» Андрей Голов. «Никифоров просто подчеркивает, что каждый в своей области должен соблюдать требования министерства и регулятора, и эти требования не противоречат друг другу, — говорит он. — Так что ничего нового не происходит».

Решение Veeam Backup & Replication v8 успешно прошло сертификационные испытания в испытательной лаборатории НПО «Эшелон»

23 марта 2016, Россия, Москва, club.cnews.ru. Решение Veeam Backup & Replication v8 успешно прошло сертификацию ФСТЭК России. Полученный сертификат подтверждает соответствие техническим условиям (ТУ) и четвертому уровню контроля отсутствия недекларированных возможностей (НДВ-4). Полученный сертификат позволяет применять решение для защиты информации в государственных информационных системах до первого класса защищенности включительно, а также в информационных системах персональных данных до первого уровня защищенности включительно, для которых актуальны угрозы первого, второго или третьего типа.

Сертификат ФСТЭК России №3482 выдан 23.12.2015 года и действителен три года – до 23.12.2018. Сертификационные испытания проводились испытательной лабораторией НПО «Эшелон».

Veeam Backup & Replication включает множество полезных функций:

- восстановление отдельных файлов, приложений и ВМ целиком;
- быстрый поиск и восстановление объектов Microsoft Exchange, SharePoint и Active Directory;
- восстановление баз данных SQL по транзакциям, на любой момент времени;
- использование аппаратных снимков HPE и NetApp. Улучшенные RPO и до 20 раз более быстрое резервное копирование;
- быстрый безопасный перенос бэкапов в облако с Veeam Cloud Connect;
- автоматическая проверка возможности восстановления данных из каждого бэкапа и реплики;
- встроенная WAN-акселерация. Перенос резервных копий на удаленную площадку до 50 раз быстрее, чем при обычном копировании файлов;
- режим передачи данных Direct Storage Access и встроенная дедупликация данных;
- аварийное переключение на реплику и обратно в один клик без влияния на работу пользователей.

Росстат гарантирует конфиденциальность персональных данных всех участников общенациональной бизнес-переписи

25 марта 2016, Россия, Москва, saratovmer.ru. Сплошное федеральное статистическое наблюдение представляет собой полномасштабное исследование уровня развития сектора малого (в том числе микро) и среднего предпринимательства в России. Руководителям предприятий и индивидуальным предпринимателям понадобится заполнить форму наблюдения с вопросами, касающимися их хозяйственной деятельности, на условиях полной конфиденциальности и гарантий защиты информации.

Бизнес может быть спокоен – Саратовстат гарантирует полную конфиденциальность данных, защиту информации, предоставленной участниками Сплошного наблюдения, отсутствие фискального характера Сплошного наблюдения. Исключается передача сведений в налоговые и иные государственные органы и контролирующие организации.

В этой связи следует напомнить, что в случае, если должностные лица, а также лица, которые в силу своего служебного положения или рода осуществляемой деятельности имели доступ к содержащимся в формах федерального статистического наблюдения первичным статистическим данным, допустили их утрату, незаконное разглашение или распространение либо фальсифицировали эти данные или содействовали их фальсификации, указанные лица несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Как известно, «Сплошное статистическое наблюдение субъектов малого и среднего предпринимательства» пройдет по всей стране в первом квартале 2016 года по итогам 2015-го и участие в нем обязательно. По предварительным данным, на сегодняшний день в списках респондентов значится около 16 тысяч средних предприятий, 2,8 миллиона малых и 3.5 миллиона индивидуальных предпринимателей.

Это уже вторая после 2010 года подобная перепись. И Росстат традиционно строго охраняет персональные данные участников бизнес-переписи. И это при том, что попытки получить доступ к ним время от времени предпринимаются. Конечно, запросы есть. И со стороны губернаторов, федеральных органов исполнительной власти, со стороны бизнеса, прокуратуры, судебных органов. Но существует закон, который обязывает Росстат соблюдать конфиденциальность данных. Кстати, по индивидуальным предпринимателям они деперсонифицируются уже при вводе информации в систему данных.

Исключение, возможно лишь в случае, когда респондент сам письменно дал разрешение запрашивающей стороне получить такую информациюо себе. Однако статистики все же вправе отклонить подобный запрос, если при этом могут быть раскрыты персональные данные других респондентов.

Итоги «Сплошного статистического наблюдения субъектов малого и среднего предпринимательства» Росстат выложит на своем сайте www.gks.ru. Все данные в ходе проведения Сплошного наблюдения предполагается получитьот субъектов малого предпринимательства до 1-го апреля 2016 года. Предварительные итоги всей этой работы будут подведены, оформлены и опубликованы в декабре 2016-го, а окончательные – с подробными данными по всей стране –в июне 2017-го.

«Сибпро» подтвердил соответствие системы защиты данных требованиям ФСТЭК РФ

31 марта 2016, Россия, Москва, iemag.ru. Компания Softline объявила о проведении аттестации объекта информатизации в компании «Сибпро». В результате заказчик смог подтвердить соответствие программно-аппаратных средств требованиям ФСТЭК РФ в сфере обеспечения ИТ-безопасности.

«Сибпро» занимается изготовлением защищенной от подделок полиграфической продукции для субъектов РФ и стран СНГ. Изготовление данной продукции осуществляется с соблюдением всех режимных условий и требований, предъявляемых к предприятиям такого профиля. Компании было необходимо провести оценку соответствия программно-аппаратных комплексов требованиям ФСТЭК РФ. Реализацией проекта занялась Softline, обладающая подтвержденными полномочиями на проведение аттестации объектов информатизации и опытом в сфере обеспечения ИТ-безопасности.

Специалисты компании произвели сбор необходимых данных о составе аттестуемых средств объекта информатизации, включающем в себя программно-аппаратные комплексы, после чего разработали программу и методику испытаний. Аттестационные мероприятия включали в себя экспертно-документальный метод и проверку комплекса функций защиты информации от несанкционированного доступа при помощи тестирующих средств, сертифицированных ФСТЭК. В ходе проверок технических и программных средств организации были изучены процессы хранения и обработки защищаемых сведений, произведен анализ информационных потоков и вероятных каналов утечки данных, методы распределения ответственности за выполнение требований в части их защиты и уровень подготовки кадров.

Помимо этого, был проведен ряд испытаний подсистем управления доступом, регистрации и учета. По результатам мероприятий заказчику был передан комплект аттестационной документации, аттестат соответствия системы требованиям ИТ-безопасности, который подтвердил эффективность имеющейся у «Сибпро» системы защиты данных, рассказали в компании.

«Успешное прохождение аттестации является важным этапом в деятельности нашей организации, так как соответствие всем требованиям в сфере информационной безопасности и лицензионным требованиям на изготовление защищенной полиграфической продукции позволит привлечь новых заказчиков в государственном и коммерческом секторах рынка. Специалисты Softline тщательно провели необходимые исследования и в короткие сроки предоставили полный пакет документов», — отметил Сергей Мезенцев, начальник отдела информационных технологий компании «Сибпро».

КОМПЕТЕНТНО: Денис Поршин, Softline, менеджер по продаже решений

<<< Аттестация объектов информатизации является неотъемлемой частью работ по обеспечению ИТ-безопасности. Она позволяет в реальных условиях эксплуатации оценить соответствие применяемого комплекса мер по обеспечению защиты информации требуемому уровню. Высокая степень подготовки сотрудников клиента в области ИБ, отсутствие несоответствий требованиям и каких-либо замечаний значительно ускорило прохождение аттестации. >>>

Сеть дата-центров «Селектел» успешно прошла ежегодный аудит на соответствие требованиям стандарта PCI DSS

31 марта 2016, Россия, Москва, iemag.ru. Стандарт PCI DSS задает требования к обработке и хранению персональных данных держателей платежных карт. Он разработан крупнейшими платежными системами Visa, MasterCard, American Express, JCB и Discover. Наличие у дата-центров сертификата PCI DSS говорит об их надежности и возможности предоставить клиентам безопасную среду для хранения конфиденциальной информации.

«Селектел» получил сертификат соответствия стандарту PCI DSS в марте 2015 года. В текущем году эксперты независимого аудитора SRC Security подтвердили, что провайдер оказывает услуги согласно этому стандарту. Решение было вынесено на основании оценки систем физической и информационной безопасности, управления доступом к сети и мониторинга, а также аппаратного обеспечения дата-центров.

КОМПЕТЕНТНО: Петр Смирнов, «Селектел», заместитель генерального по развитию и эксплуатации инфраструктуры дата-центров

<<< Одним из приоритетов для нас является обеспечение информационной и физической безопасности данных клиентов. Сертификация по стандарту PCI DSS подтвердила, что мы реализовали в наших дата-центрах всестороннюю систему защиты конфиденциальной информации. Прохождение ежегодного аудита свидетельствует о стабильно высоком качестве оказываемых услуг. Это дополнительно повышает доверие к бренду со стороны международных и российских компаний. >>>

ПО и технические новинки

Управление защитой через «умные» часы: новые возможности Kaspersky Internet Security для Android

09 марта 2016, Россия, Москва, ict-online.ru. «Лаборатория Касперского» выпустила новую версию решения Kaspersky Internet Security для Android. Обновленный продукт позволяет управлять защитой смартфонов и планшетов с устройств, работающих на Android Wear, таких как «умные» часы. С помощью часов можно получать уведомления, например, о найденных на мобильном устройстве угрозах, а также отправлять команды — включение функции «Сирена» для поиска гаджета, запуск проверки файлов на онлайн-угрозы, обновление антивирусных баз. Кроме того, новое решение полностью совместимо с Android 6.0.

«Android продолжает оставаться наиболее атакуемой мобильной платформой, поэтому владельцам устройств, работающих на этой операционной системе, следует задумываться об их безопасности. Мы, в свою очередь, постоянно работаем над совершенствованием защиты и стараемся оперативно реагировать на изменяющиеся потребности пользователей. К примеру, набирающая обороты популярность умных часов на базе Android Wear заставила нас задуматься об обеспечении их совместимости с защитным решением. И эта мера значительно повысила удобство использования наших продуктов владельцами современных гаджетов Android», — говорит Алексей Чиков, старший менеджер по продуктам «Лаборатории Касперского».

Kaspersky Internet Security для Android продолжает надежно защищать от всех видов мобильных угроз, в том числе от программ-вымогателей и мобильных банковских троянцев, атакам которых в 2015 году российские пользователи подвергались чаще других.

Кроме того, продукт включает в себя инструменты удаленного управления устройством на случай потери или кражи, фильтрацию нежелательных звонков и сообщений, защиту персональных данных на устройстве от посторонних глаз. Решением также можно управлять удаленно через единый портал My Kaspersky, например, для включения функции «Анти-Вор» и обновления антивирусных баз.

СИБРУС – платформа для корпоративной связи

10 марта 2016, Россия, Москва, irkutskmedia.ru. Работа коллектива может быть продуктивной, когда налажены внутренние коммуникации. Тогда решения принимаются быстро, а задачи закрываются вовремя. В некоторых компаниях для ведения дел используют только электронную почту и телефон, в других – целый ряд программ и инструментов, каждый из которых выполняет отдельную задачу. К примеру, с помощью электронной почты передают документацию, по видеосвязи обсуждают вопросы с филиалами, а в чатах решают срочные вопросы.

При этом часто случается, что работники отвлекаются и путаются, стараясь быстро переключиться с одного вида общения на другой.

Прибавим к этому тот факт, что нередко программы «подвисают», ломаются и тем самым затрудняют все бизнес-процессы в компании. Практика последних лет показывает, что для того, чтобы все дела в организации решались лучше, быстрее и эффективнее, стандартных методов и систем уже недостаточно – появляется огромная потребность в более продвинутых средствах коммуникации. Одним из подобных современных инструментов является СИБРУС.

СИБРУС – это российская разработка, которая представляет собой удобную платформу для связи внутри коллектива компании и с партнерами. Общение осуществляется через Интернет и локальную сеть. Главная задача СИБРУСа – ускорение и усовершенствование корпоративных процессов и защита информации, которой обмениваются работники организации.

Действительно ли так важен пункт – защита информации? Да, ведь из-за утечек информации, из-за которых конкуренты могут получить, к примеру, доступ к новым разработкам компании, фирма может тяжело пострадать – вплоть до банкротства, особенно в кризис, когда дела организации идут и так не лучшим образом. Не стоит думать, что небольшие утечки – вещь безобидная (к примеру, утечки персональных данных сотрудников). Разве это так страшно? И снова да – на практике именно такие «незначительные» потери являются наиболее частой причиной крупных неприятностей в делах компании.

Воспользоваться данными может не сам вор, но в его интересах найти заинтересованного покупателя из числа конкурентов. Он же может сделать секретную информацию общедоступной, а это уже высокие репутационные риски. Огромный ущерб от утечки информации может составить и упущенная прибыль.

Компания, присвоившая себе документацию на какой-либо товар и первая выпустившая его на рынок, автоматически получает возможность пожать все лавры, в то время как истинный разработчик окажется на втором месте. Более того, вор может обвинить разработчика в плагиате! Неудивительно, что продажи у разработчика будут значительно меньше предполагаемых изначально.

Платформа СИБРУС предлагает организациям комплексное решение для максимального усиления безопасности корпоративной связи. Эта система, к слову, обладает рядом других полезных функций, в числе которых, например, предоставление обширного набора средств прямых коммуникаций между пользователями для совместной работы. Плюсом решения так же является факт отсутствия контроля со стороны заграничных производителей ПО.

Механизмы безопасности в СИБРУС располагают двумя наборами инструментов для решения главных вопросов безопасного хранения и обмена данными: защита данных от перехвата, утечки, прослушивания и кражи через Сеть и защита от бытовых ошибок или чрезвычайных ситуаций при работе с системой. Для защиты информации платформа применяет стойкие алгоритмы, сочетающие симметричное и асимметричные шифрование. Защита обеспечивается на компьютере или мобильном устройстве пользователя, а также на сетевых каналах связи и серверах платформы.

Клиентское ПО доступно на компьютерах с операционными системами Windows, Linux и Mac OS и смартфонах под управлением Android и iOS. Серверное ПО доступно для Linux и Windows.

Запатентован российский многофункциональный чип для хранения персональных данных

15 марта 2016, Россия, Москва, bankir.ru. Разработчик решений для банковских карт, смарт-карт, идентификационных документов «Ангстрем-Т» получил свидетельство Федеральной службы по интеллектуальной собственности о государственной регистрации топологии двухинтерфейсного микроконтроллера многофункционального назначения. Отечественный чип будет использоваться в паспортно-визовых документах, SIM-картах, банковских картах и других изделиях, где необходимо хранение персональных или конфиденциальных данных. Одна из областей применения микроконтроллера — платежная карта «Мир». В настоящее время идет сертификация чипа на соответствие международному стандарту операций по банковским картам EMVCo и доработка операционной системы для ее использования с микроконтроллером, включая платежные системы НСПК, Visa, MasterCard.

Микроконтроллер по техническим характеристикам не уступает зарубежным аналогам, а на внутреннем рынке имеет ряд существенных преимуществ. С помощью такого чипа можно оплачивать проезд в общественном транспорте, приложив карточку к считывающему устройству. Микроконтроллер также обеспечивает высокую степень защиты данных от хакерских атак. Срок службы банковской карты с решением АО «Ангстрем-Т» — 25 лет. В течение этого времени данные могут быть перезаписаны 500 тысяч раз.

«Топология нового чипа — это полностью российская разработка на уровне мировых аналогов. Решения, использованные в этом микроконтроллере, позволят предложить заказчику цену ниже, чем у конкурентов»,— отметил коммерческий директор «Ангстрем-Т» Сергей Саркисов.

Микроконтроллер «Ангстрем-Т» доступен в нескольких вариантах: контактном, бесконтактном и комбинированном. Безопасность хранения персональных данных пользователя обеспечена поддержкой российских криптографических стандартов.

Solar Security выпустила DLP-агент для контроля рабочих станций на Linux

17 марта 2016, Россия, Москва, solarsecurity.ru. Компания Solar Security выпустила на рынок модуль контроля рабочих станций Dozor Endpoint Agent for Linux, являющийся частью DLP-системы Solar Dozor 6.0, предназначенный для работы с Astra Linux и GosLinux («Гослинукс»).

Разработка Dozor Endpoint Agent for Linux является важным этапом развития российской DLP-системы Solar Dozor 6.0, считают в компании. Создание модуля продиктовано, прежде всего, требованиями российского рынка, так как все большее количество организаций в рамках импортозамещения переходит на свободные ОС на базе Linux.

Dozor Endpoint Agent for Linux позволяет контролировать содержимое данных на съемных носителях, печать на локальных и сетевых принтерах, а также осуществляет аудит рабочих станций и подключенных сетевых хранилищ на предмет нарушения политик хранения конфиденциальных данных, используя контентные и контекстные атрибуты.

Модуль Dozor Endpoint Agent for Linux может использоваться в организациях, где есть повышенные требования к защищенным системам. В нем предусмотрена возможность блокировки передачи данных для должной защиты наиболее критичной информации, указали в Solar Security.

«Решение о создании Dozor Endpoint Agent for Linux было продиктовано, прежде всего, требованиями наших заказчиков, — отметила Галина Рябова, руководитель направления Solar Dozor компании Solar Security. — Мы видим большой потенциал в развитии этой темы. Мы начали с отечественных ОС, наиболее востребованных нашими клиентами. В перспективе мы планируем предоставить возможность использовать наше DLP-решение на других популярных операционных системах Linux».

EndpointSniffer от SearchInform поможет управлять доступом к информации и контролировать установку ПО

22 марта 2016, Россия, Москва, tadviser.ru. Компания SearchInform презентовала обновленную версию платформы EndpointSniffer, которая позволит задавать индивидуальные правила защиты компьютеров и информации, размещенной на них.

Управление доступом к папкам и дискам

По словам разработчиков, теперь платформа позволяет заблокировать доступ к определенным папкам и их содержимому всем пользователям, за исключением указанных. Управление доступом осуществляется с помощью настройки правил «Доступ к папкам».

Аналогично обновленная система позволяет управлять доступом к логическим дискам и их содержимому. Настройка правил позволяет разрешить доступ ко всем дискам определенных рабочих станций только указанным пользователям. Остальным пользователям доступ ко всем дискам (за исключением системного) будет блокирован. Ограничение доступа также распространяется на подключенные диски, имеющие логическое имя (например, F:), пояснили в компании.

Возможность управления доступами будет полезна службам ИБ: офицеры безопасности смогут «закрывать» папки и диски с конфиденциальными данными для всех, включая системных администраторов. При этом действия внутри этих папок/дисков в аудит не попадают.

«Если раньше агент “Контура информационной безопасности SearchInform” был предназначен для контроля информационных потоков (и сотрудников, соответственно), то теперь его развитие происходит и в направлении защиты, — отметил технический директор SearchInform Иван Мершков. — В любой организации есть люди, которые работают с конфиденциальными данными высшего уровня, и запрет доступа к ним и к их компьютерам делает систему безопасности еще более надежной. Взять, скажем, топ-менеджера или офицера безопасности, на компьютерах которых всегда масса файлов, закрытых для третьих лиц. Можно просто следить за тем, чтобы информация не попала в “левые руки”, а можно запретить доступ и исключить возможность утечки».

Контролируемая установка ПО

Обновленная платформа позволяет также блокировать установку нежелательного ПО на рабочие станции. Агент делает снимок системы, фиксируя список установленных программ. При попытке новой инсталляции (в том числе и через MSI-пакет) происходит блокировка. В целом такая возможность оптимизирует работу ИТ-отдела. Прежде всего, обновление ориентировано на топ-менеджмент и ИБ-департаменты, информация на рабочих станциях которых представляет особую ценность, указали в SearchInform.

RSA обновила свое решение для управления учетными данными и их авторизации

24 марта 2016, Россия, Москва, nnit.ru. Компания RSA, подразделение информационной безопасности EMC, объявила о появлении инновационных возможностей по аутентификации и управлению учетными данными в решении RSA Via. Эти новые функции призваны помочь организациям поддерживать баланс между безопасностью и удобством пользователей при аутентификации учетных данных, а также лучше управлять процессами привилегированного доступа.

По словам разработчиков, новые возможности аутентификации, встроенные в RSA Via Access, помогут обеспечить нужные уровни авторизации пользователя при различных запросах.

Дополнительные функции RSA Via Lifecycle и Governance были разработаны для того, чтобы увеличить прозрачность предоставления доступа к привилегированным системам и защититься от целевых атак. Эта комбинация предлагает заказчикам более широкий выбор средств авторизации учетных данных, а также предоставляет возможность оптимизировать управление рисками, утверждают в EMC.

Баланс безопасности и комфорта

Для обеспечения защиты от продвинутых угроз организациям необходимо лучше выстраивать соответствие между рисками доступа к системе и уровнями авторизации учетных данных. Теперь RSA Via Access может автоматически соотносить методы аутентификации с уровнем риска для каждого запроса на доступ, позволяя администраторам устанавливать требования к авторизации учетных данных на основе политик безопасности.

Например, доступ к наиболее важным активам компании может потребовать наличие ключей RSA SecurID или методов биометрической аутентификации, тогда как работа с менее критичными активами может требовать меньшего уровня авторизации, пояснили в компании.

«RSA Via Access специально был разработан, чтобы предоставить администраторам выбор, какой уровень авторизации нужен для разных сценариев, в зависимости от контекста, такого как место доступа и используемое устройство. Все это помогает избежать компрометации системы безопасности», — подчеркнули в EMC.

Организациям также нужно соблюдать баланс между требованиями к безопасности и удобством пользователя. По утверждению разработчиков, RSA Via Access позволяет использовать больший набор методов аутентификации, соизмеримо важности каждого приложения. Благодаря разнообразию методов аутентификации, пользователи получают возможность подтверждения своих учетных данных тем способом, который наиболее удобен для них, вместо попытки подобрать «один размер для всех».

В дополнение к проверке пользователя по отпечатку пальца TouchID и пространственных движений устройством tap or shake, RSA Via Access теперь поддерживает новые биометрические возможности, благодаря интеграции Eyeprint IDTM, технологии от EyeVerify. Эта новая технология использует уникальный рисунок сосудов глаза, а также другие микропризнаки, чтобы авторизовать пользователя, подтвердив соответствие биометрического шаблона на доверенном устройстве. Сервер RSA Via Access также был сертифицирован FIDO и теперь поддерживает устройства стандарта FIDO U2F, которые предоставляют компании и пользователям еще ряд дополнительных методов аутентификации и делают этот процесс более удобным.

Управление и администрирование рисков привилегированного доступа

Администраторы с возможностью привилегированного доступа владеют ключами ко всем наиболее ценным активам организации и критически важным системам. Но обширные возможности RSA Via Lifecycle and Governance, а также другие функции системы помогают компаниям систематически контролировать и управлять доступом этих привилегированных пользователей на протяжении всего жизненного цикла учетных данных.

RSA Via Lifecycle and Governance теперь может работать вместе с решением CyberArk Privileged Account Security, обеспечивая необходимый уровень прозрачности и предоставляя инструменты управления привилегированным доступом. В дополнение к этому в RSA Via Lifecycle and Governance была встроена функция обслуживания учетных записей для управления жизненным циклом привилегий пользователей, начиная с приема на работу, включая смену позиций и заканчивая увольнением.

«Не всем видам доступа нужен один и тот же уровень авторизации. Организациям необходимо сфокусироваться на балансе между авторизацией учетных данных и сохранением удобства для пользователей, который может быть нарушен из-за подхода к авторизации в режиме “один размер для всех”, — отметил Джим Дачарм (Jim Ducharme), вице-президент по инжинирингу и управлению продуктами в RSA. — Новые возможности технологии RSA Via позволяют соотнести различные уровни риска, связанные с активами, к которым пользователь хочет получить доступ, с соответствующими уровнями авторизации. Это позволит организациям поддерживать инновационные опции аутентификации и поможет избежать компромисса между авторизацией и удобством работы».

«В организациях обычно имеется 3-4 более привилегированные учетные записи, чем записи обычных пользователей, что увеличивает возможную плоскость атак при помощи взлома учетной записи, которую киберпреступники могут захватить и контролировать. Совместимость проактивных возможностей обнаружения и защиты CyberArk Privileged Account Security и RSA Via Lifecycle and Governance помогает сократить возможности для атак, управляя выдачей, контролем и сертификацией привилегий, делать это централизовано и единообразно», — заявил Адам Босниан (Adam Bosnian), исполнительный вице-президент по глобальному развитию бизнеса в CyberArk.

Доступность

Новые версии RSA Via Access и RSA Via Lifecycle and Governance с новыми функциями будут доступны уже в первом квартале 2016 г.

Новая технология Kaspersky Lab упрощает управление шифрованием корпоративных данных

25 марта 2016, США, expert.com.ua. Kaspersky Lab запатентовала в Бюро по регистрации патентов и торговых марок США технологию для облегчения контроля доступа пользователей к зашифрованным данным. Она входит в состав корпоративных продуктов компании и упрощает использование метода полного шифрования диска, применяемого организациями для обеспечения дополнительного уровня безопасности бизнес-данных.

Контроль доступа требует при полном шифровании диска установки отдельного профиля каждому пользователю. Новая технология решает проблемы, связанные с использованием одного и того же компьютера в разное время разными сотрудниками и наличием нескольких профилей на одном устройстве. Она помогает распознавать, какой из пользователей активен в данный момент, создавать отдельные профили и настраивать необходимые политики безопасности.

КОМПЕТЕНТНО: Константин Каманин, Kaspersky Lab, эксперт по информационной безопасности

<<< Новая технология значительно облегчает решение задач, которые встают перед IT-специалистами при внедрении шифрования. Например, проверяет, выполнено ли полное шифрование диска и соответствует ли полученный пользователем доступ полагающимся ему привилегиям безопасности. Эта технология наряду с другими нашими решениями позволяет повысить безопасность информационной системы предприятия при минимуме усилий. >>>

«Лаборатория Касперского» и WISeKey выпускают защищенное приложение для хранения ценных данных

29 марта 2016, Россия, Москва, ib-bank.ru. «Лаборатория Касперского» и швейцарская компания WISeKey, специализирующаяся на информационной безопасности, объявили о выпуске защищенного приложения WISeID Kaspersky Lab Security. Эта совместная программа объединяет в себе лучшие технологии компаний-разработчиков и позволяет владельцам мобильных гаджетов общаться и проводить денежные транзакции в безопасной среде.

Приложение WISeID Kaspersky Lab Security создает надежно защищенное облачное хранилище для персональных данных пользователя, в частности, для его логинов, паролей и данных банковских карт, и обеспечивает безопасную синхронизацию информации между мобильными устройствами и компьютером.

Само хранилище защищено технологиями шифрования, и доступ к нему можно получить только с помощью мастер-пароля, известного лишь самому пользователю. Для дополнительной защиты приложение использует распознавание лица как метод аутентификации пользователя.

В основе WISeID Kaspersky Lab Security лежат защитные технологии «Лаборатории Касперского», входящие в инструментарий Kaspersky Mobile Security SDK. Именно с их помощью в приложении обеспечивается сетевая безопасность, защита самого устройства и распознавание угроз.

«Мобильные угрозы развиваются и усложняются крайне быстрыми темпами, а злоумышленники неустанно ищут новые способы получения персональных и финансовых данных пользователей. Несмотря на то, что мобильные платформы сегодня обеспечивают разработчикам приложений определенный уровень безопасности, этого все равно недостаточно для надежной защиты от уловок киберпреступников. Именно поэтому мы работаем над созданием специальных приложений, обеспечивающих надлежащий уровень безопасности пользователей мобильных устройств. Мы рады, что партнерство cWISeKey позволило нам сделать еще один шаг на пути защиты важной для пользователя информации», – отметил Александр Карпицкий, руководитель управления технологического лицензирования и сервисных проектов «Лаборатории Касперского».

Вышла новая версия системы распознавания паспорта РФ Smart PassportReader 2.0

29 марта 2016, Россия, Москва, mskit.ru. Компания Smart Engines, российский разработчик технологий распознавания, спустя год после выхода первого решения для распознавания паспорта гражданина РФ для мобильных и стационарных устройств, представляет второе поколение системы - Smart Passport Reader 2.0. В новой версии реализованы распознавание паспорта как в портретной так и альбомной ориентации для мобильных устройств, а также распознавание разворота паспорта с помощью вебкамер.

Важной особенностью версии 2.0 является поддержка уникальной российской архитектуры микропроцессора “Эльбрус”, наряду с ARMv7-v8 (AArch32 и AArch64), x86 и x86_64. Решение на базе Эльбрус позволит использовать технологию распознавания паспорта РФ для задач создания программно-аппаратных комплексов по обработке персональных данных с повышенными требованиями по информационной безопасности и технологической независимости.

Развитие алгоритмов распознавания и синтаксической/геометрической межкадровой интеграции позволило повысить качество и скорость распознавания. В частности, удалось существенно повысить качество распознавания паспортов РФ с бледно напечатанными данными. Проведенные работы по оптимизации архитектуры и программного кода ядра распознавания обеспечили улучшение поддержки многоядерных конфигураций для многоядерных мобильных и стационарных процессоров.

Smart PassportReader 2.0 позволяет на фотографии, скане или в видеопотоке распознавать как 2-ую и 3-ью страницы паспорта по отдельности, так и целый разворот паспорта, на сервере, десктопе или мобильном устройстве под управлением наиболее распространенных ОС семейства Windows, Linux, Solaris, MacOS, iOS, Android. При этом система умеет сама находить и идентифицировать паспорт, исправлять искажения (геометрические, освещенность, наклоны, поворот и др.), после чего автоматически распознает соответствующие поля.

Smart PassportReader доступен в виде SDK, который дает возможность разработчикам интегрировать функции распознавания в информационные системы. SDK включает в себя набор библиотек программных интерфейсов (API), документацию и примеры интеграции для различных ОС. В новой версии реализованы функции извлечения не только текстовых данных, но и изображения документа целиком, данных о местонахождении полей, изображений текстовых и графических полей (фотография, подпись).

При этом для каждого текстового поля в системе есть возможность запроса оценки надежности его распознавания.

Для повышения удобства интеграции функциональности распознавания паспорта РФ в комплект SDK Smart PassportReader 2.0 включены компонента работы с видеокамерой для Windows/Linux и ActiveX-компонента для интеграции в различные информационные системы (например 1С). Эти нововведения, разработанные с учетом пожеланий пользователей, позволят разработчикам ПО сократить время на встраивание и отладку своих приложений.

Тестовые версии Smart PassportReader 2.0 предоставляются разработчикам по запросу. В ближайших планах компании обновление демонстрационных приложений в App store и Google play.

ПРОБЛЕМЫ. КОНФЛИКТЫ. ИНЦИДЕНТЫ
Проверки регуляторов

В Северной Осетии трое юрлиц привлечены к административной ответственности за нарушение законодательства в сфере обработки персональных данных

18 марта 2016, Россия, Сев. Осетия-Алания респ., rkn.gov.ru. Мировыми судьями Моздокского и Дигорского судебных районов РСО-Алания в результате рассмотрения материалов территориального Управления Роскомнадзора привлечены к административной ответственности трое юридических лиц: ООО «Долина», АМС Мостиздахского сельского поселения Дигорского района РСО-Алания и ООО «Лялс».

Указанные юридические лица не представили в адрес Управления по его запросу в 30-дневный срок сведения об обработке персональных данных, необходимые для реализации его полномочий, что явилось нарушением требований ч. 4 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В связи с этим в отношении нарушителей были составлены протоколы по ст. 19.7 КоАП РФ и направлены на рассмотрение в мировые суды по подведомственности.

Решением суда юридические лица признаны виновными. ООО «Долина» и ООО «Лялс» назначены штрафы по три тыс. рублей, АМС Мостиздахского сельского поселения Дигорского района РСО-Алания вынесено предупреждение.

Обзор: Проверки в СЗФО

15.03.2016, Россия, Санкт-Петербург, rkn.gov.ru: **При проверке Комитета по тарифам Санкт-Петербурга выявлены нарушения в сфере обработки персональных данных**

Управлением Роскомнадзора по Северо-Западному федеральному округу проведена плановая выездная проверка Комитета по тарифам Санкт-Петербурга на предмет соблюдения обязательных требований в сфере обработки персональных данных.

В ходе проверки выявлено нарушение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», выразившееся в отсутствии в поручении лицу, которому оператором поручается обработка персональных данных, обязанности соблюдения их конфиденциальности и обеспечения их безопасности, а также требований к защите обрабатываемых персональных данных (ч. 3 ст. 6 указанного Федерального закона).

По результатам проверки Управлением составлен акт и выдано предписание. Материалы проверки направлены в Прокуратуру Санкт-Петербурга для решения вопроса о возбуждении дела об административном правонарушении по ст. 13.11 КоАП РФ.

17.03.2016, Россия, Карелия респ., mngz.ru: **Роскомнадзор по Карелии провел плановое мероприятие систематического наблюдения**

В ходе мероприятия проанализирована информация, размещенная в информационно-телекоммуникационной сети "Интернет" на официальных сайтах операторов, являющихся государственными и муниципальными органами.

По итогам проведенного мероприятия систематического наблюдения в сети Интернет были выявлены признаки нарушения законодательства Российской Федерации в области обработки персональных данных: - непринятие оператором мер по опубликованию или обеспечению неограниченного доступа к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. По факту выявленных нарушений в адрес учреждений направлены требования о необходимости опубликования на официальном сайте документов, указанных в п. 2 Постановления правительства Российской Федерации от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных".

В ходе мероприятия проанализирована информация, размещенная в информационно-телекоммуникационной сети "Интернет" на официальных сайтах операторов, являющихся государственными и муниципальными органами.

По итогам проведенного мероприятия систематического наблюдения в сети Интернет были выявлены признаки нарушения законодательства Российской Федерации в области обработки персональных данных:

- непринятие оператором мер по опубликованию или обеспечению неограниченного доступа к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

По факту выявленных нарушений в адрес учреждений направлены требования о необходимости опубликования на официальном сайте документов, указанных в п. 2 Постановления правительства Российской Федерации от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных".

29.03.2016, Россия, Карелия респ., rkn.gov.ru: **В Карелии за непредставление в территориальное Управление Роскомнадзора информации в области персональных данных оштрафовано ООО «Олонец Камень»**

Мировым судьей судебного участка Олонецкого района Республики Карелия, в результате рассмотрения материалов, направленных территориальным Управлением Роскомнадзора, привлечено к административной ответственности ООО «Олонец Камень». Основанием для судебного решения явилось непредставление организацией государственному органу сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности.

Организация не представила в адрес Управления по его запросу в установленный законом 30-дневный срок необходимую информацию, нарушив тем самым требования Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». В отношении юридического лица был составлен протокол по ст. 19.7 КоАП РФ и направлен на рассмотрение в мировой суд по подведомственности, который назначил нарушителю штраф.

Обзор: Проверки в ЦФО

15.03.2016, Россия, Рязанская обл., rkn.gov.ru: **Управлением Роскомнадзора по Рязанской области выявлены нарушения законодательства в сфере персональных данных государственными органами Рязанской области**

Управлением Роскомнадзора по Рязанской области при проведении систематического наблюдения по выявлению нарушений законодательства в сфере персональных данных в сети Интернет проведен анализ правомерности размещения на сайтах государственных органов Рязанской области персональных данных граждан, а также наличия на сайтах в свободном доступе документов, предусмотренных нормативно-правовыми актами в сфере персональных данных.

В соответствии с ч. 2 постановления Правительства от 21.03.2011 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами», на сайте государственного или муниципального органа должны быть опубликованы документы, определяющие его политику в отношении обработки персональных данных. Управлением выявлено два сайта, на которых такие документы не размещены.

С 01.09.2015 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» дополнен п. 10.1 ч. 3 ст. 22, согласно которому оператор обязан представить в уполномоченный орган сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации: страна нахождения базы данных и адрес нахождения базы данных.

Информационное письмо, содержащее данные сведения, в Управление от четырех государственных органов не поступало. Управлением Роскомнадзора по Рязанской области в соответствии с полномочиями приняты меры по устранению допущенных нарушений.

16.03.2016, Россия, Москва, banki.ru: **«Бинбанк Кредитные Карты» оштрафован за передачу персональных данных клиента коллекторам**

В Москве коммерческий банк привлечен к административной ответственности за нарушение порядка обработки персональных данных клиента, сообщается на сайте прокуратуры города.

Коптевская межрайонная прокуратура провела проверку по обращению Управления Роскомнадзора по Самарской области в интересах гражданина по факту нарушения законодательства о персональных данных со стороны АО «Бинбанк Кредитные Карты». Установлено, что банк передал персональные данные жителя Самарской области в коллекторскую компанию для принудительного взыскания просроченной задолженности.

«Переписка гражданина с кредитной организацией ни к какому результату не привела, вместе с тем претензии коллекторской компании только увеличивались. Заявитель обратился в Управление Роскомнадзора по Самарской области, которое направило по территориальности информацию в Коптевскую межрайонную прокуратуру», — отмечается в релизе.

При проведении проверочных мероприятий было установлено, что кредитной организацией и коллекторской компанией персональные данные гражданина обрабатывались с нарушением федерального законодательства.

Коптевский межрайонный прокурор возбудил в отношении юридического лица дело об административном правонарушении по статье 13.11 КоАП. Речь идет о «нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)».

Постановлением мирового судьи судебного участка № 404 столичного района Коптево «Бинбанк Кредитные Карты» привлечен к административной ответственности в виде штрафа. Кроме того, межрайонный прокурор внес на имя председателя правления банка представление об устранении указанных нарушений. В итоге персональные данные, относящиеся к заявителю, изъяты из обработки.

25.03.2016, Россия, Рязанская обл., rkn.gov.ru: **Управлением Роскомнадзора по Рязанской области возбуждены административные производства в связи с нарушением требований Федерального закона «О персональных данных»**

Управлением Роскомнадзора по Рязанской области в адрес Администрации муниципального образования – Корневское сельское поселение Скопинского муниципального района Рязанской области, Администрации муниципального образования – Глебковское сельское поселение Рыбновского муниципального района Рязанской области были направлены мотивированные запросы с требованием представить необходимую для осуществления деятельности Управления информацию в сфере обработки персональных данных.

Согласно ч. 4 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператор обязан ответить на такой запрос в течение тридцати дней с даты его получения. В нарушение требований законодательства операторы не представили запрашиваемую информацию, что в соответствии со ст. 19.7 КоАП РФ является основанием для возбуждения административного производства.

В отношении указанных юридических лиц составлены соответствующие административные протоколы и направлены мировым судьям по территориальной подведомственности.

25.03.2016, Россия, Брянская обл., rkn.gov.ru: **В Брянской области ООО «Строй-Синтез» и ООО «Синтез-Т» наказаны за непредставление уведомления об обработке персональных данных**

Мировым судом Брянской области по материалам территориального Управления Роскомнадзора привлечены к административной ответственности ООО «Строй-Синтез» и ООО «Синтез-Т».

Ранее по факту непредставления организациями уведомления об обработке персональных данных, что является нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Управлением были составлены протоколы по ст. 19.7 КоАП РФ, материалы дел были переданы в суд. Суд постановил назначить указанным лицам наказания в виде предупреждения (ООО «Строй-Синтез») и штрафа в размере трех тыс. рублей (ООО «Синтез-Т»).

29.03.2016, Россия, Тверская обл., rkn.gov.ru: **В Тверской области проведены плановые выездные проверки на предмет соблюдения ООО «Ваш ломбард» и ООО «УК ЖЭУ» обязательных требований законодательства в области персональных данных**

Отделом по защите прав субъектов персональных данных и надзора в сфере информационных технологий Управления Роскомнадзора по Тверской области проведены плановые выездные проверки ООО «Ваш ломбард» и ООО «УК ЖЭУ» на предмет соблюдения обязательных требований законодательства в области персональных данных.

Выявлены нарушения обязательных требований ст. 7, ч. 1, ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», п. 13 постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Юридическим лицам выданы предписания об устранении нарушений.

Обзор: Проверки в СФО

14.03.2016, Россия, Омская обл., rkn.gov.ru: **Управлением Роскомнадзора по Омской области составлено 11 протоколов об административных нарушениях за непредставление сведений об обработке персональных данных**

Управлением Роскомнадзора по Омской области составлено 11 протоколов об административных нарушениях по ст. 19.7 КоАП РФ за непредставление сведений об обработке персональных данных, что является нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Протоколы составлены в отношении следующих юридических лиц: ООО «АКВАТИКА», ООО «Торговый дом «Александра», ООО «ИНТЕРНЕТ МАГАЗИН УЧЕТЭНЕРГО», ООО «ПОРТЬЕРНЫЙ ДОМ», ООО «ЛОМБАРД-АВИЛОН», ООО «Автомобильные приборы», ООО «КА «ЮККА», ООО «ЛОТОС-ОМСК», ООО «Аквасервис +», ООО «Интернет магазин», ООО «Учебный центр «Конкорди».

14.03.2016, Россия, Иркутская обл., rkn.gov.ru: **Газетой «Время» выполнено требование Управления Роскомнадзора по Иркутской области о прекращении обработки персональных данных в отношении гражданина**

Газетой «Время» в полном объеме выполнено требование Управления Роскомнадзора по Иркутской области о прекращении обработки персональных данных в отношении гражданина, обратившегося в Управление с жалобами на действия СМИ, связанные с опубликованием сведений, содержащих его персональные данные.

Установлено, что при публикации статей в газете, а также на информационном ресурсе www.angvremya.ru осуществлено распространение персональных данных заявителя без получения согласия субъекта персональных данных на данную обработку, в отсутствие правовых оснований. В связи с фактом нарушения требований ч. 1 ст. 6 Федерального закона «О персональных данных» Управлением в адрес издания было направлено требование о прекращении обработки (распространения) персональных данных заявителя.

14.03.2016, Россия, Иркутская обл., rkn.gov.ru: **В Иркутской области ряд юридических лиц привлечен к административной ответственности за непредставление сведений об обработке персональных данных**

Мировыми судьями рассмотрены материалы Управления Роскомнадзора по Иркутской области и вынесены постановления о признании виновными МУК «Культурно-спортивный центр» Максимовского МО, ООО «Регион-Финанс», Администрации Смоленского МО – Администрации СП, АКБ «Банк Москвы» (ОАО), ООО ТТК «Лидер».

Указанные организации не представили в адрес Управления в 30-дневный срок сведения об обработке персональных данных, необходимые для реализации его полномочий, что является нарушением ч. 4 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В связи с этим в отношении юридических лиц были составлены протоколы по ст. 19.7 КоАП РФ.

Судебными решениями организации признаны виновными и им назначены наказания в виде штрафа в размере трех тыс. рублей (АКБ «Банк Москвы» (ОАО)) и предупреждения (МУК «Культурно-спортивный центр» Максимовского МО, ООО «Регион-Финанс», Администрация Смоленского МО – Администрация СП, ООО ТТК «Лидер»).

30.03.2016, Россия, ФО Сибирский, rkn.gov.ru: **Управлением Роскомнадзора по Сибирскому федеральному округу выявлены нарушения Федерального закона «О персональных данных»**

Управлением Роскомнадзора по Сибирскому федеральному округу в ходе мероприятий систематического наблюдения в отношении страховых компаний и операторов связи Новосибирской области выявлены нарушения ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» со стороны АО «Д2 страхование», ООО «НСК-страхование», ЗАО «Зап-СибТранстелеком» и ООО «Айпистрим.ру».

Каждому юридическому лицу направлено требование об опубликовании в десятидневный срок на сайте документа, определяющего политику Оператора в отношении обработки персональных данных, и сведений о реализуемых требованиях к защите персональных данных, а также об обеспечении возможности доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Сведения о нарушениях направлены в органы прокуратуры.

В Приамурье установлен владелец найденных на свалке медицинских карт

05 апреля 2016, Россия, Амурская обл., ria.ru. Медицинские карты, найденные в конце марта на свалке Благовещенска Амурской области, принадлежат женской консультации, сообщил РИА Новости начальник отдела по защите прав субъектов персональных данных регионального управления Роскомнадзора Иван Полица.

Как сообщалось ранее, 28 марта амурские спасатели во время занятий по горной подготовке увидели в куче мусора мешок с тетрадями, похожими на медицинские карты. На тетрадях были указаны фамилии, имена и отчества, телефоны, места прописки пациентов, вклейки с результатами УЗИ и другими исследованиями.

"Мы проводили свою проверку по информации, которая появилась в СМИ, выехали на свалку и застали там сотрудников женской консультации номер два города Благовещенска, медики собирали карты в коробки. Видно, что документы старые, последние записи в картах датированы 2008 годом, результаты проверки мы передадим в прокуратуру Амурской области", – сообщил Полица РИА Новости.

Прокурор Амурской области ранее поручил прокурору Благовещенска выяснить, как медицинские документы оказались на свалке. Как пояснил старший помощник прокурора региона Валентин Бурсянин, в данном случае имеет место нарушение врачебной тайны и закона о персональных данных.

По закону "Об основах охраны здоровья в Российской Федерации" предусмотрен запрет на любое распространение посторонним лицам информации о пациенте, содержание медкарт является врачебной тайной. Согласно закону, амбулаторные карты пациентов после окончания срока хранения в архиве должны уничтожаться по регламенту: сжигаться или измельчаться после составления соответствующего акта.

Обзор: проверки в УрФО

10.03.2016, Россия, Тюменская обл., rkn.gov.ru: **В Тюменской области по результатам плановой проверки Управления образования администрации Ярковского муниципального района выявлены нарушения в области персональных данных**

Управлением Роскомнадзора по Тюменской области, ХМАО-Югре и ЯНАО, в рамках планового выездного мероприятия по контролю в отношении Управления образования администрации Ярковского муниципального района на предмет соответствия обработки персональных данных требованиям законодательства, установлено, что обработка персональных данных осуществляется не в соответствии с нормативно-правовыми актами.

Выявлены нарушения ч. 1 ст. 6, ч. 3 и ч. 7 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- обработка персональных данных в случаях, непредусмотренных Федеральным законом;

- представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения;

- непредставление в уполномоченный орган сведений об изменении информации о месте нахождения базы данных информации, содержащей персональные данные граждан, представление которых предусмотрено п. 10.1 ч. 3 ст. 22 Федерального закона, вступившего в законную силу с 01.09.2015.

По результатам проверки выдано предписание. Для решения вопроса о возбуждении в отношении учреждения дела об административном правонарушении по ст. 13.11 КоАП РФ материалы направлены в Прокуратуру Ярковского района.

16.03.2016, Россия, Тюменская обл., rkn.gov.ru: **В Тюменской области в деятельности ОАО «Гостиница «Колос» выявлены нарушения обязательных требований в области обработки персональных данных**

Управлением Роскомнадзора по Тюменской области, ХМАО-Югре и ЯНАО проведена плановая проверка ОАО «Гостиница «Колос» на предмет соответствия обработки персональных данных требованиям законодательства. Выявлены нарушения ч. 1 и ч. 3 ст. 6, ч. 3 и ч. 7 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- обработка персональных данных в случаях, непредусмотренных Федеральным законом;

- отсутствие в поручении лицу, которому оператором поручается обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности, а также требований к защите обрабатываемых персональных данных;

- представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения;

- поручение иному лицу осуществлять обработку персональных данных без согласия субъекта персональных данных;

- непредставление в уполномоченный орган сведений о прекращении обработки персональных данных или об изменении информации, содержащейся в уведомлении об обработке персональных данных;

- непредставление сведений о месте нахождения базы данных информации, содержащей персональные данные граждан РФ, представление которых предусмотрено п. 10.1 ч. 3 ст. 22 Федерального закона, вступившего в законную силу с 01.09.2015.

По результатам проверки организации выдано предписание. Для решения вопроса о возбуждении дела об административном правонарушении, предусмотренного ст. 13.11 КоАП РФ, материалы направлены в прокуратуру Центрального АО г. Тюмени.

29.03.2016, Россия, Ханты-Мансийский АО, rkn.gov.ru: **В деятельности Департамента здравоохранения Ханты-Мансийского автономного округа – Югры выявлены нарушения обязательных требований в области обработки персональных данных**

Управлением Роскомнадзора по Тюменской области, ХМАО – Югре и ЯНАО проведена плановая выездная проверка Департамента здравоохранения Ханты-Мансийского автономного округа – Югры на предмет соблюдения обязательных требований в области обработки персональных данных.

В ходе проверки выявлены следующие нарушения:

- п. 7 постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» - несоответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства;

- ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» - обработка персональных данных в случаях, не предусмотренных Федеральным законом.

По результатам проверки Департаменту здравоохранения Ханты-Мансийского автономного округа – Югры выдано предписание об устранении выявленных нарушений. Материалы проверки направлены в прокуратуру Ханты-Мансийского автономного округа – Югры для решения вопроса о возбуждении дела по ст. 13.11 КоАП РФ.

01.04.2016, Россия, Тюменская обл., rkn.gov.ru: **В деятельности ГАПОУ ТО «Тюменский колледж водного транспорта» выявлены нарушения в области обработки персональных данных**

Управлением Роскомнадзора по Тюменской области, ХМАО-Югре и ЯНАО проведена плановая выездная проверка государственного автономного профессионального образовательного учреждения тюменской области «Тюменский колледж водного транспорта» (ГАПОУ ТО «Тюменский колледж водного транспорта») на предмет соответствия обработки персональных данных требованиям законодательства. При проведении мероприятия выявлены следующие нарушения обязательных требований в области обработки персональных данных:

- ч. 1 ст. 6 и ч. 3 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (обработка персональных данных в случаях, непредусмотренных Федеральным законом «О персональных данных»; несоблюдение обязательных требований при обработке специальных категорий персональных данных (сведения о судимости));

- п. 7 постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (несоответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства).

По результатам проверки учреждению выдано предписание. Для решения вопроса о возбуждении дела об административном правонарушении, предусмотренного ст. 13.11 КоАП РФ, материалы направлены в прокуратуру Ленинского АО города Тюмени.

01.04.2016, Россия, Свердловская обл., rkn.gov.ru: **В Свердловской области в деятельности ряда организаций выявлены нарушения законодательства в области персональных данных**

Управлением Роскомнадзора по Уральскому федеральному округу в ходе мероприятий систематического наблюдения установлено, что рядом организаций, оказывающих услуги в сфере ЖКХ, а также организаций, осуществляющих продажу товаров дистанционным способом, не приняты меры по обеспечению неограниченного доступа к документам, определяющим политику оператора в отношении обработки персональных данных, и сведениям о реализуемых требованиях к защите персональных данных.

В адрес ТСЖ «Чкалова 250», ООО «УК «ИРЮМ», ЕМУП «СУЭРЖ», ООО УЖК «АРДО», ООО УЖК «АЛЬФА», а также Интернет-магазинов ИП Естехина П. А., ООО «Кронс», ООО «СПОРТКОМ», ООО «Биг Медиа Компани», ООО «БУКИ» направлены письма с требованием об устранении нарушения ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Для решения вопроса о возбуждении дел по ст. 13.11 КоАП РФ материалы систематического наблюдения направлены в органы прокуратуры.

05.04.2016, Россия, Тюменская обл., rkn.gov.ru: **В Тюменской области в деятельности ООО ТК «Планета-Тур» выявлены нарушения обязательных требований в области обработки персональных данных**

Управлением Роскомнадзора по Тюменской области, ХМАО – Югре и ЯНАО проведена плановая выездная проверка ООО ТК «Планета-Тур» на предмет соответствия обработки персональных данных требованиям законодательства.

Выявлены нарушения ч. 1 ст. 6, ч. 3 и ч. 7 ст. 22 Федерального закона «О персональных данных»: обработка персональных данных в случаях, непредусмотренных данным Федеральным законом; представление уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения; непредставление сведений об изменении информации о месте нахождения базы данных информации, содержащей персональные данные граждан РФ, представление которых предусмотрено п. 10.1 ч. 3 ст. 22 Федерального закона, вступившим в законную силу с 01.09.2015.

По результатам проверки ООО ТК «Планета-Тур» выдано предписание.

Для решения вопроса о возбуждении дела об административном правонарушении по ст. 13.11 КоАП РФ материалы направлены в Прокуратуру Центрального округа г. Тюмени.

05.04.2016, Россия, Ханты-Мансийский АО, 72.rkn.gov.ru: **В ХМАО – Югре ряд юридических лиц оштрафован за непредставление сведений об обработке персональных данных**

На основании материалов Управления Роскомнадзора по Тюменской области, ХМАО – Югре и ЯНАО мировыми судьями гг. Нижневартовск, Сургут, Лянтор привлечены к административной ответственности ООО «ПМ Консалтинг», ООО «Бурение Консалтинг», ООО ТК «Маркетинг», ООО «ВисцераТерэ Консалтинг».

Ранее Управлением были направлены запросы о предоставлении информации в адреса указанных юридических лиц, однако в течение 30 календарных дней с даты получения запроса организации не представили необходимую информацию, тем самым нарушив требования ч. 4 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В отношении данных организаций были составлены протоколы об административных правонарушениях, предусмотренных ст. 19.7 КоАП РФ, и направлены по подведомственности в суды.

Мировые судьи признали нарушителей виновными и назначили им штрафы в размере трех тыс. рублей каждому.

Обзор: Проверки в ПФО

16.03.2016, Россия, Саратовская обл., stroysar.ru: **«СпецАТХ» уличили в разглашении персональных данных**

Прокуратура Саратова провела проверку по обращению руководителя управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Саратовской области по вопросу нарушения действующего законодательства о персональных данных МУП БКО «СпецАТХ».

Установлено, что в адрес Управления поступило обращение гражданина с информацией о нарушении его прав, как субъекта персональных данных. В адрес заявителя поступил платежный документ от ООО «СарРЦ» за коммунальные услуги, предоставляемые МУП БКО «СпецАТХ». Данный платежный документ содержал в себе персональные данные заявителя: ФИО, адрес проживания.

Согласно статье Федерального закона «О персональных данных» обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора.

МУП БКО «СпецАТХ» не представило надлежащего доказательства исполнения Закона.

«Таким образом, персональные данные заявителя получены МУП БКО «СпецАТХ» от третьих лиц в отсутствие правовых оснований, определенных статьями Федерального закона «О персональных данных», - сообщает прокуратура города.

15 марта прокуратура внесла представление в адрес руководителя МУП БКО «СпецАТХ», которое находится на рассмотрении

31.03.2016, Россия, Башкортостан респ., rkn.gov.ru: **В деятельности Администрации городского округа город Кумертау Республики Башкортостан выявлены нарушения при обработке персональных данных**

Управлением Роскомнадзора по Республике Башкортостан проведена плановая проверка за соблюдением Администрацией ГО г. Кумертау РБ требований законодательства в сфере защиты прав субъектов персональных данных.

В ходе проверки выявлены следующие нарушения:

- обработка специальной категории персональных данных (сведения о судимости) работников, не относящихся к муниципальным служащим, в анкете, предоставляемой работнику для заполнения при трудоустройстве, без письменного согласия либо иного законного основания, что является нарушением ч. 3 ст. 10 Федерального закона «О персональных данных»;

- обработка персональных данных (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы (наименование и адрес организации, должность), домашний адрес (адрес регистрации, фактического проживания)) близких родственников работников, не относящихся к муниципальным служащим, без письменного согласия субъектов персональных данных, что является нарушением ч. 1 ст. 6 указанного Федерального закона.

Материалы проверки направлены в органы прокуратуры по территориальной подведомственности в целях принятия мер прокурорского реагирования.

31.03.2016, Россия, Чувашская респ., rkn.gov.ru: **В адрес глав администраций Большеалгашинского и Нижнекумашкинского сельских поселений Шумерлинского района Чувашской Республики внесены представления об устранении нарушений законодательства в области персональных данных**

Управлением Роскомнадзора по Чувашской Республике – Чувашии проведено плановое мероприятие систематического наблюдения в сети Интернет в отношении органов местного самоуправления.

На официальных сайтах Большеалгашинского и Нижнекумашкинского сельских поселений Шумерлинского района Чувашской Республики выявлены признаки нарушения законодательства в области персональных данных в части неопубликования операторами документов, определяющих политику в отношении обработки персональных данных, и сведений о реализуемых требованиях к защите персональных данных, что является нарушением ч. 2 ст. 18.1 Федерального закона «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211.

Материалы проверки были направлены в прокуратуру для принятия мер прокурорского реагирования в части внесений представлений об устранении выявленных нарушений в отношении администраций Большеалгашинского и Нижнекумашкинского сельских поселений Шумерлинского района. Шумерлинской межрайонной прокуратурой проведена проверка, по результатам которой в адрес глав администраций внесены представления об устранении нарушений законодательства и привлечения виновных лиц к дисциплинарной ответственности.

31.03.2016, Россия, Чувашская респ., rkn.gov.ru: **Управлением Роскомнадзора по Чувашской Республике – Чувашии возбуждены дела в отношении трех юридических лиц, несвоевременно представивших уведомления об обработке персональных**

Специалистами Управления Роскомнадзора по Чувашской Республике – Чувашии составлено три протокола по ст. 19.7 КоАП РФ в отношении ООО «Яхтинг», ООО «Яхтинг-Сервис» и ООО «Яхтинг-Экспорт». Ранее Управлением в адрес указанных организаций были направлены письма о предоставлении сведений по уведомлению уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных.

В соответствии с ч. 4 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса. Запрашиваемая информация в установленный законодательством срок представлена не была.

Материалы дел в отношении юридических лиц, нарушивших требования законодательства, направлены мировым судьям.

04.04.2016, Россия, Саратовская обл., rkn.gov.ru: **В Саратовской области за непредставление в территориальное Управление Роскомнадзора информации в области персональных данных оштрафовано ООО Медицинский центр «Стандарт»**

Мировым судьей Саратовской области, в результате рассмотрения материалов, направленных Управлением Роскомнадзора по Саратовской области, привлечено к административной ответственности ООО Медицинский центр «Стандарт». Основанием для судебного решения явилось непредставление государственному органу сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности.

Так, организация не представила в адрес Управления по его запросу в установленный законом 30-дневный срок необходимую информацию, нарушив требования ч. 4 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». В отношении юридического лица был составлен протокол по ст. 19.7 КоАП РФ и направлен на рассмотрение в мировой суд, который назначил виновному штраф в размере трех тыс. рублей.

05.04.2016, Россия, Чувашская респ., rkn.gov.ru: **В деятельности администрации Московского района г. Чебоксары выявлены нарушения законодательства в области персональных данных**

Управлением Роскомнадзора по Чувашской Республике – Чувашии проведена плановая выездная проверка администрации Московского района г. Чебоксары Чувашской Республики за соответствием обработки персональных данных требованиям законодательства.

В ходе проверки установлено, что оператором в нарушение требований ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152–ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 не представлены следующие нормативно-правовые акты: Правила рассмотрения запросов субъектов персональных данных или их представителей; Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных»; Правила работы с обезличенными данными в случае обезличивания персональных данных.

В нарушение п. 15 постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об обработке персональных данных, осуществляемой без использования средств автоматизации» оператором также не представлен перечень мер, необходимых для обеспечения сохранности персональных данных и исключающих несанкционированный к ним доступ, а также порядок их принятия, перечень лиц, ответственных за реализацию указанных мер.

Кроме того, в нарушение ч. 3 ст. 6 Федерального закона «О персональных данных» в договоре с ПАО «Сбербанк России» по выплате денежных средств работникам отсутствует обязанность сторон по соблюдению условий конфиденциальности, безопасности персональных данных и требований к защите обрабатываемых персональных данных.

Юридическому лицу внесено предписание об устранении нарушений.

05.04.2016, Россия, Татарстан респ., tatar-inform.ru: **В РТ более 14 тыс. операторов персональных данных включено в реестр ОПД в этом году**

С начала 2016 года Управлением Роскомнадзора по РТ зарегистрировано и внесено в единую информационную систему Роскомнадзора 78 уведомлений и 540 информационных писем о внесении изменений в сведения об операторе в реестре ОПД.

По состоянию на 1 апреля 2016 года в реестр операторов персональных данных всего включено 14 тыс. 840 операторов, осуществляющих обработку персональных данных физических лиц на территории республики.

В адрес 240 операторов направлены официальные письма-запросы с напоминанием об обязанности предоставления в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) сведений: 100 писем-запросов о предоставлении уведомления об обработке персональных данных, 140 писем-запросов о предоставлении информационных писем о внесении изменений в сведения об операторе в реестре ОПД.

За 3 месяца 2016 года управлением составлено 16 протоколов о нарушениях за непредставление или несвоевременное представление в управление сведений, представление которых предусмотрено законом и необходимо для осуществления управлением его законной деятельности, а также за представление таких сведений в неполном объеме или в искаженном виде.

По 15 протоколам, составленным в 2015 году, судами в 2016 году вынесено 15 постановлений о признании операторов виновными в совершении административного правонарушения, предусмотренного ст. 19.7 КоАП РФ: 9 оператором назначено наказание в виде административного штрафа в размере 3 тыс. руб. – на сумму 27 тыс. рублей, 6 операторам назначено наказание в виде предупреждения.

В 1-м квартале 2016 года зарегистрировано 178 обращений физических и юридических лиц. Из них 167 обращений с жалобами на деятельность операторов (150 поступило от граждан и 17 - от юридических лиц) и 11 обращений по разъяснению законодательства в области персональных данных (8 поступило от граждан и 3 – от юридических лиц).

Факты нарушений законодательства не подтвердились при рассмотрении 122 из 150 обращений граждан с жалобами и 17 обращений юридических лиц. Заявителям направлены ответные письма с разъяснениями.

В одностороннем порядке операторами приняты меры по восстановлению нарушенных прав и законных интересов 2 заявителей, нарушения устранены в установленный законом срок в процессе рассмотрения обращений управлением.

По результатам рассмотрения 5 обращений приняты меры по направлению материалов с признаками нарушений законодательства для рассмотрения и принятия мер по подведомственности в органы прокуратуры. По одному обращению управлением составлено и направлено в суд исковое заявление в защиту прав субъектов персональных данных, по решению суда иск управления удовлетворен.

Для рассмотрения и принятия мер по подведомственности 3 обращения переадресованы в МВД, для рассмотрения по территориальной принадлежности 4 обращения направлены в территориальные органы Роскомнадзора, 1 обращение переадресовано в УФАС по РТ.

По состоянию на 31 марта 2016 года на рассмотрении в управлении находятся 20 обращений граждан с жалобами на деятельность операторов и 1 обращение граждан по разъяснению законодательства в области персональных данных.

С начала года управлением проведены плановые выездные проверки в отношении 2 операторов, осуществляющих обработку персональных данных. По результатам проверок нарушения требований законодательства Российской Федерации в области персональных данных не выявлены, сообщает Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по РТ.

Обзор: Проверки в ЮФО

15.03.2016, Россия, ФО Южный, rkn.gov.ru: **По материалам Управления Роскомнадзора по ЮФО прокурором внесено представление об устранении районной администрацией нарушений законодательства о персональных данных**

По материалам Управления Роскомнадзора по Южному федеральному округу прокуратурой Усть-Лабинского района Краснодарского края внесено представление об устранении администрацией муниципального образования Усть-Лабинский район нарушений законодательства о персональных данных.

Ранее Управлением в результате мониторинга официальных интернет-сайтов государственных и муниципальных органов было выявлено нарушение законодательства администрацией муниципального образования Усть-Лабинский район в части неопубликования документов, определяющих политику в отношении обработки персональных данных и (или) сведений о реализуемых требованиях к защите персональных данных, на интернет-сайте администрации www.adminustlabinsk.ru.

В адрес администрации было направлено требование об устранении выявленного нарушения с последующим информированием Управления об исполнении требования, материалы по нарушению также были направлены в прокуратуру.

05.04.2016, Россия, Астраханская обл., astrahan.bezformata.ru: **В Астраханской области в деятельности четырех учреждений здравоохранения выявлены нарушения требований законодательства в области персональных данных**

Управлением Роскомнадзора по Астраханской области проведено мероприятие систематического наблюдения в отношении ООО «Клиника», ООО Центр Стоматологии «Голливуд», ООО «Клиника доктора Калининой», ООО «Стоматолог плюс».

Выявлены нарушения ч. 4 ст. 9 и п. 2 ст. 18.1 Федерального закона «О персональных данных»: несоответствие требованиям закона заявления о согласии на обработку персональных данных и отсутствие документов, определяющих политику Оператора в отношении обработки персональных данных, и (или) сведений о реализуемых требованиях к защите персональных данных.

В учреждения здравоохранения направлены требования об устранении выявленных нарушений, материалы проверки направлены в органы прокуратуры г. Астрахани для принятия мер прокурорского реагирования.

05.04.2016, Россия, Астраханская обл., rkn.gov.ru: **В Астраханской области по результатам проверки туристической фирмы выявлены нарушения законодательства в области персональных данных**

Управлением Роскомнадзора по Астраханской области проведена плановая выездная проверка ООО Туристическая фирма «АРТЕЗ-ТУР», которое осуществляет деятельность по оказанию туристических услуг и является оператором, обрабатывающим персональные данные граждан.

По результатам проверки в деятельности туристической компании выявлены нарушения ст. 7, ч. 4 ст. 9, ч. 1 ст. 18.1, ч. 3 ст. 6 и ч. 2 ст. 18.1 Федерального закона «О персональных данных»:

- передача персональных данных туристов третьим лицам без их согласия;

- несоответствие формы согласия на обработку персональных данных;

- непринятие оператором мер, необходимых и достаточных для обеспечения обязанностей, предусмотренных законом в части несоответствия обработки персональных данных граждан заявленной цели обработки персональных данных;

- отсутствие в поручении лицу, которому Оператором поручается обработка персональных данных, обязанности по обеспечению безопасности лица, перечня действий (операций) с персональными данными, а также требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона;

- необеспечение неограниченного доступа к документу, определяющему политику Оператора в отношении персональных данных.

ООО Туристической фирме «АРТЕЗ-ТУР» выдано предписание об устранении нарушений, материалы проверки направлены в прокуратуру Кировского района г. Астрахани для принятия мер прокурорского реагирования.

Утечки информации. Инциденты

Соответствие стандарту PCI DSS не спасает от риска утечки данных платежных карт

15 марта 2016, США, pcidss.ru. В 2014 году примерно 31,8 млн американцев стали жертвами утечки данных платежных карт.

В начале марта Федеральная торговая комиссия США поручила девяти компаниям в сфере крупного и малого бизнеса в течение 45 дней предоставить подробные отчеты о проверке соответствия стандарту безопасности данных индустрии платежных карт PCI DSS.

Согласно статистике NASDAQ, в 2014 году примерно 31,8 млн американцев стали жертвами утечки данных платежных карт. Данные результат втрое превышает показатель 2013 года, пишет эксперт компании High-Tech Bridge Илья Колошенко в статье на портале CSO.

Стандарт PCI DSS описывает требования к защите данных о держателях карт, сгруппированные в двенадцать тематических разделов. Основной акцент PCI DSS делает на обеспечении безопасности сетевой инфраструктуры и защите хранимых данных о держателях платежных карт, как наиболее уязвимых с точки зрения угроз конфиденциальности. Также стандарт регламентирует правила безопасной разработки, поддержки и эксплуатации платежных систем, в том числе процедуры их мониторинга.

Многочисленные инциденты, связанные с утечкой данных в соответствующих PCI DSS компаниях, ставят под сомнение эффективность стандарта. Однако дело не только в эффективности, но и отношении предприятий к собственной безопасности. К примеру, большинство из пострадавших компаний не в полной мере выполняли требования PCI DSS или неверно определяли сферу охвата среды данных о держателях карт (Cardholder Data Environment, CDE). Некоторые организации реализовывали временные меры по контролю за безопасностью исключительно с целью прохождения аудита на соответствие PCI DSS.

Если исключить утечки данных, связанных с третьей стороной, физическими атаками (скимминг, атаки на PoS-терминалы и т.д.) и инсайдерскими угрозами, значительное количество подобных инцидентов является следствием использования уязвимых web-приложений.

Согласно пункту 6 требований стандарта PCI DSS, «организации обязаны разрабатывать и поддерживать безопасные системы и приложения». Это одно из наиболее важных требований для web-приложений в сфере CDE.

Однако многие предприятия часто неверно трактуют данную норму, так же, как и ее реализацию.

КОМПЕТЕНТНО: Ян Шредер, PwC Switzerland, эксперт

<<< Соответствие стандарту PCI DSS – только один элемент в рамках подхода к управлению рисками безопасности. Нередко компании используют подход «для галочки» в отношении стандарта PCI DSS без полного понимания и оценки киберугроз, а также их возможных последствий для бизнеса. >>>

Android-устройства на базе процессоров Snapdragon представляют угрозу безопасности данных

16 марта 2016, США, securitylab.ru. Уязвимости в устройствах позволяют получить над ними полный контроль.

Исследователи Trend Micro обнаружили серьезные ошибки в коде ядра Snapdragon от компании Qualcomm, позволяющие получить права суперпользователя на Android-устройствах. С помощью вредоносного ПО злоумышленник может проэксплуатировать уязвимости (CVE-2016-0805 и CVE-2016-0819) и получить над смартфоном или планшетом полный контроль с целью похищения учетных данных, фотографий и другой информации.

По данным Qualcomm, в настоящее время на базе процессоров и модемов Snapdragon работают свыше миллиарда устройств. Компания выпустила исправления, однако проблема заключается в их доставке пользователям. Сначала патчи получает Google. Затем компания передает их производителям устройств, отправляющим обновления операторам связи, и только потом они становятся доступными для пользователей. Иногда обновления не поддерживаются более старыми устройствами, из-за чего пользователи подвергаются большому риску.

Nexus 5X, Nexus 6P, Nexus 6, Nexus 5, Nexus 4, Nexus 7, Nexus 9 и Nexus 10 автоматически получают исправления уязвимостей непосредственно от Google, поэтому их владельцы могут не беспокоиться.

По словам исследователей Trend Micro, уязвимым является каждое Android-устройство, работающее на базе процессора Snapdragon с версией ядра 3.10. Большинство из них либо перестали получать обновления, либо никогда не получали их в первую очередь. Подобные устройства представляют потенциальную угрозу безопасности пользовательской информации. Как сообщают эксперты, уязвимые процессоры используются в Nexus 5, 6 и 6P, а также в Samsung Galaxy Note Edge. Поскольку исследователи не могут проверить абсолютно каждое устройство, данный список является далеко не полным.

В Шелехове менеджер офиса сотовой связи передавал мошенникам персональные данные клиентов

17 марта 2016, Россия, Иркутская обл., baikal-info.ru. В Шелехове будут судить менеджера офиса продаж компании сотовой связи, который передал мошенникам персональные данные клиентов. Как 17 марта 2016 года сообщила пресс-служба ГУ МВД России по Иркутской области, сведения, которые 25-летний мужчина передал мошенникам, позволили воспользоваться сбережениями владельцев сим-карт. В результате преступных действий пострадали 10 человек, с банковских счетов которых было списано более ста тыс. рублей. «За незаконное получение и разглашение сведений, составляющих коммерческую тайну, в отношении работника магазина было возбуждено уголовное дело по статье 183 УК РФ», – рассказывает старший следователь отдела МВД России по Шелеховскому району майор юстиции Виктор Шагдуров.

Как установлено следствием, к мужчине обратился знакомый и попросил предоставить личные сведения – паспортные данные, адреса, ФИО владельцев определенных телефонных номеров. Имея доступ к базе данных, менеджер воспользовался своим служебным положением и передал персональные данные клиентов, которые впоследствии были использованы в мошеннических действиях на территории России.

Получив эти сведения, мошенники по поддельным доверенностям от имени владельцев в офисах диллеров оператора связи сим-карта блокировалась как утерянная, а взамен выпускалась новая с тем же номером. Так мошенники получали доступ к деньгам абонентов и через мобильный банк списывали их. Материалы уголовного дела в отношении уже бывшего сотрудника компании сотовой связи были переданы в суд.

Приложение для iOS дает возможность получить персональные данные о пользователях

19 марта 2016, США, vistanews.ru. Независимый эксперт в области информационной безопасности обнаружил в открытом доступе базу данных MongoDB. Открытой для всех оказалась персональная информация 198 тыс. пользователей.

Независимый эксперт Крис Викери, который занимается вопросами информационной безопасности, обнаружил базу данных, находящуюся в открытом доступе. Персональные данные пользователей приложения Kinotopic хранятся в хранилище под названием MongoDB, которая содержит около 198 тыс. записей.

Видеоредактор для iOS уже длительное время не поддерживается разработчиками, однако имеет обширное число пользователей, данные которых оказались в свободном доступе. Викери утверждает, что «мертвые» приложения, которые не получают обновлений, так же опасны, как и те, которые активно используются пользователями.

Для Криса Викери данная база является не первой крупной находкой. Ранее он обнаружил в свободном доступе базу данных избирателей США (191 млн), участников официального сайта Hello Kitty (3,3 млн), а также данные пользователей программного продукта MacKeeper (13 млн).

USB Thief крадет данные через зараженные USB-носители

23 марта 2016, Россия, Москва, comss.info. Вирусная лаборатория Eset обнаружила новую вредоносную программу для кражи данных. Троян USB Thief использует для распространения съемные USB-носители и не оставляет следов деятельности на скомпрометированных машинах.

USB Thief запускается только со съемного USB-устройства (флэшки, внешнего жесткого диска и пр.). Это означает, что троян не оставляет следов в скомпрометированной системе, а жертва не замечает, что данные с ПК перемещаются на внешний носитель, подчеркнули в компании. Троян привязан только к одному USB-устройству, что предотвращает его утечку из системы, на которую нацелена атака.

По словам представителей Eset, в USB Thief реализована сложная многоступенчатая система шифрования, связанная с особенностями размещения на съемных носителях.

Благодаря этому троян крайне сложно обнаружить и анализировать. Специальные механизмы защиты от копирования и воспроизводства дополнительно затрудняют детектирование вредоносной программы.

Большинство троянов убеждает пользователя запустить вредоносный файл при помощи традиционных «аргументов»: поддельный ярлык легитимной программы, файл Autorun и пр. В отличие от них, USB Thief использует распространенную практику хранения на USB-носителях портативных версий популярных программ: Firefox, NotePad++, TrueCrypt и пр. Вредоносная программа вставляет свой код в цепочку команд в формате плагина или динамически подключаемой библиотеки (DLL). Когда запускается приложение, троян будет действовать вместе с ним в фоновом режиме, пояснили в компании.

USB Thief нацелен на кражу файлов заданных форматов. Так, образец USB Thief, изученный вирусными аналитиками Eset, записывал изображения, документы и данные, собранные с использованием импортированного приложения WinAudit. Украденные файлы шифруются с использованием криптографии. После удаления USB-носителя с данными, записанными на него трояном, никто не сможет узнать о компрометации системы.

По мнению вирусного аналитика Eset Томаша Гардона, USB Thief создан для таргетированных атак на системы, изолированные от интернета из соображений безопасности. Это не самый распространенный способ кражи данных, но крайне опасный — возможности USB Thief можно расширить любым деструктивным функционалом.

Антивирусные продукты Eset NOD32 детектируют новый троян как Win32/PSW.Stealer.NAI.

Google оштрафована во Франции на 100 тысяч евро, но будет обжаловать

25 марта 2016, Франция, rosbalt.ru. Французский регулятор оштрафовал американскую Alphabet Inc., материнскую компанию интернет-гиганта Google Inc., на 100 тыс. евро за нарушение предписания о применении так называемого «права на забвение» ко всем доменам компании по всему миру.

По данным The Wall Street Journal, французская Комиссия по делам информационных технологий и правам человека (CNIL), главный орган страны в области защиты персональных данных, отметила, что Google нарушила предписание удалять информацию о гражданах по их требованию в отношении «всех доменных имен» поисковика, включая глобальный домен google.com, сообщает «Интерфакс».

Google намерена обжаловать решение регулятора. «Мы не согласны с мнением CNIL, что у него есть полномочия контролировать доступ к контенту людей, проживающих за пределами Франции», — отметили представители компании.

В прошлом году Европейский суд предоставил всем гражданам ЕС «право на забвение», обязав интернет-поисковики удалять ссылки на информацию о гражданах по их требованию, если такая информация устарела, является ложной или нарушает их право на неприкосновенность личной жизни.

Франция считается родоначальницей концепции «права на забвение». В 2010 году страна приняла Хартию о праве на забвение — свод правил, регулирующих отношения государства и интернет-компаний в области защиты персональных данных граждан. В то время как Microsoft подписала хартию, Facebook и Google отказались поставить под ней свои подписи.

Полиция Токио обнаружила утечку 18 млн паролей интернет-пользователей

25 марта 2016, Япония, it-digital.ru. Сотрудники правоохранительных органов Токио смогли обнаружить утечку восемнадцати миллионов логинов, паролей и других персональных данных интернет-пользователей не серверах «серого» провайдера-посредника.

Отмечается, что арестованы были сервера, на них, кроме персональной информации, удалось обнаружить 97 хакерских программ.

Таким образом, в период с июня по ноябрь прошлого года при помощи данного программного обеспечения и с использованием персональной информации пользователей неизвестные лица неоднократно пытались подключаться к серверам популярного в Японии интернет-магазина Rakuten, Yahoo, Twitter и еще 28 компаний.

«Яндекс» впервые попал под суд за отказ разглашать данные пользователей

25 марта 2016, Россия, Москва, therunet.com. Интернет-компанию «Яндекс» впервые попытались осудить за отказ предоставлять персональные данные клиентов. Иск с требованием раскрыть переписку одного из пользователей «Яндекс. Почты» в Хамовнический суд Москвы подала Федеральная таможенная служба (ФТС). Об этом сообщает газета «Коммерсантъ» со ссылкой на собственные источники.

По данным издания, 22 марта Хамовнический районный суд Москвы в законном порядке разрешил «Яндекс. Почте» сохранить тайну личной переписки пользователя.

Судебное дело «Яндекса» началось с запроса Находкинской таможни о предоставлении почтовой переписки одного из пользователей за период с 1 января 2014 года по 1 октября 2015 года. По мнению таможенников, через почтовый ящик «Яндекса» некий «правонарушитель» обсуждал схемы уклонения от таможенных платежей.

Когда интернет-компания отказалась предоставить требуемые данные, таможня обратилась к мировому судье участка N425 города Москвы. Мировой судья признал «Яндекс» виновным и назначил штраф в размере трёх тысяч рублей. Но интернет-компания оспорила это решение в Хамовническом суде, так как в постановлении не указали на ограничение тайны переписки пользователя. Об этом «Коммерсанту» сообщила представитель «Яндекса» Ася Мелкумова.

Когда интернет-компания отказалась предоставить требуемые данные, таможня обратилась к мировому судье участка N425 города Москвы

Между тем юридическая служба компании заявила, что ни один интернет-ресурс не обязан разглашать личные данные пользователей без соответствующего судебного постановления.

Юридическая служба «Яндекса»:

«Согласно Конституции, ограничение права на тайну переписки допускается только на основании судебного решения. „Яндекс“, как и Google, Facebook, Twitter и многие другие международные сервисы, предоставляет информацию о пользователях правоохранительным органам в том порядке и тех случаях, которые предусмотрены законодательством»

Отметим, в 2015 году по данному поводу власти РФ обращались к Google, Facebook и Twitter около 300 раз. В итоге Google удовлетворила около 5 процентов из 207 полученных запросов. Twitter отклонил все 82 требования в отношении ресурса. Facebook за тот же период получил и отклонил всего один запрос на раскрытие персональных данных пользователей.

По данным «Коммерсанта», отечественные IT-компании получают такие запросы ещё чаще, однако, требования властей далеко не всегда бывают законны.

Аппаратно-программные комплексы системы «НИТ-Школьное питание» в школах Серова установлены не будут

26 марта 2016, Россия, Свердловская обл., serovglobus.ru. Управление образования в лице его бывшего руководителя Дмитрия Егорова говорило родителям, что никаких нарушений при попытке внедрить аппаратно-программные комплексы в школах города, не было. В свою очередь, прокуратура нарушения нашла не только в действиях персонала школы № 1, но и ООО «НИТ-Электронная карта».

Напомним, что скандал разразился в начале февраля, когда родители узнали, что их детей кто-то фотографировал для каких-то электронных карт. «В школе будут вводить систему пропуска по картам. Для этого будет проводиться фотографирование учащихся. Фотографировать будут представители организации, выпускающей данные карты. Также для выпуска карты нужно будет предоставить представителям фирмы свои личные данные. Мы были удивлены и ошарашены, поскольку какого-либо родительского собрания не проводилось. До нас, родителей, как законных представителей своих несовершеннолетних детей, данная информация не была доведена», – писали тогда в своей жалобе на имя серовского городского прокурора Андрея Аржаховского возмущенные родители.

Сейчас же к родителям пришли две бумаги с ответами из прокуратуры и Управления образования. К слову, в ответе на редакционный запрос, управление образования утверждало, что в их адрес жалоб от родителей не поступало.

Нарушений нет?

Основные претензии родителей сводились к тому, что детей без разрешения фотографировали на телефоны представители компании. Учителя же, по словам родителей, довели детей отказывающихся фотографироваться, до слез угрозами, что «придется сменить школу».

Вот что ответили в управлении образования: «Информацию для сбора, хранения и обработки персональных данных обучающихся 5 класса для заключения договоров с ООО «НИТ-Электронная карта» школа не запрашивала, и в ООО «НИТ-Электронная карта» не предоставляла; сотрудники школы не обязывали родителей и обучающихся предоставлять какие-либо данные. Форма договора с регистрационной формой (заявкой) ООО «НИТ-Электронная карта» были предоставлены родителям 4 февраля 2016 г. с ознакомительной целью и с последующим заключением данного договора на добровольной основе. В регистрационной форме (заявке) публичной оферты по заключению указанного договора родителем (законным представителем) с ООО «НИТ-Электронная карта» содержится информация о согласии на обработку персональных данных (родители рассказывают о фактах, когда фотографирование было осуществлено до подписания договора).

4 февраля 2016 г. фотографирование обучающихся проводилось сотрудниками ООО «НИТ-Электронная карта» с целью изготовления электронной карты для внедрения в МАОУ СОШ №1 «Полифорум» аппаратно-программного комплекса системы «НИТ-Школьное питание» в режиме тестовой апробации. Фотографирование проводилось в учебном кабинете в присутствии учителя-предметника и в присутствии всего ученического коллектива класса.

По поводу истерии обучающихся к администрации школы и к медицинским работникам обращений не поступало. Среди обучающихся имел место отказ детей от фотографирования. Данные обучающиеся сфотографированы не были.

Предварительно 22 января 2016, 29 января 2016 и 02 февраля 2016, на оперативных совещаниях педагогического коллектива МАОУ СОШ №1 «Полифорум» и совещании педагогического коллектива МАОУ СОШ №1 «Полифорум» информация о внедрении аппаратно-программного комплекса системы «НИТ-Школьное питание» и соответственно о фотографировании обучающихся была доведена до педагогического коллектива, в том числе и о необходимости проведении общешкольного родительского собрания с целью информирования родителей (законных представителей) по внедрению данной системы. Обязанность уведомления родителей (законных представителей) по данному вопросу была возложена на классных руководителей МАОУ СОШ №1 «Полифорум».

Нарушения есть!

– В ходе проверки были выявлены нарушения по защите персональных данных детей, их фотографирование без разрешения законных представителей, то есть родителей. Исполняющему обязанности директора школы № 1 вынесено представление, которое в данный момент находится на рассмотрении. Компания «НИТ-Электронная карта» также не получила согласия на фотографирование детей, – рассказала «Глобусу» Ольга Беляева, помощник прокурора.

Прокуратура выяснила, что фирма фотографировала детей 4 февраля без согласия родителей, между школой и фирмой существовала только предварительна устная договоренность, а собрания родителей не проводилось до 4 февраля (день, когда осуществлялась фотосъемка).

Прокуратура выяснила, что фирма фотографировала детей 4 февраля без согласия родителей

В действиях сотрудников школы прокуратура выявила нарушение требований закона «Об образовании» и о защите персональных данных.

– Мы работали по представлениям, давали информацию и в прокуратуру, и отвечали родителям. Те нарушения, которые были допущены, устранены. Ответы в соответствующие инстанции мы выдали, – прокомментировал работу по выявленным нарушениям начальник Управления образования Александр Колганов.

«Такие системы внедряться будут»?!

Новый начальник управления образования Александр Колганов рассказал о своем видении ситуации по поводу внедрении в школах города аппаратно-программного комплекса системы «НИТ-Школьное питание».

– Вопрос, на мой взгляд, о правильном начинании – переходе оплаты в школах города за питание на карточную систему, и в перспективе – на проход в школу по карточной системе, – прокомментировал Александр Александрович. – Это программа комплексной безопасности. Что эта программа давала? Автоматизированный учет прохода и автоматизированный учет питания детей. Какие плюсы для детей и для родителей? Система предполагает, что родитель деньги ребенку кладет на карточку (обычная банковская карта, только немного другого вида). Ребенок ходит с картой.

Эта карта является единой для входа в школу и для оплаты питания. Родитель каждый день может видеть, что ребенок кушает, на какую сумму, во сколько он пришел в школу, во сколько ушел. И сколько раз в процессе нахождения в школе он вышел. То есть, это определенный контроль и информация о ребенке. К сожалению, эта инициатива вызвала почему-то очень бурное сопротивление родительской общественности. И в настоящее время эти проекты работают только в трех классах одной из школ города. Это пилотный этап. Рассчитан на два месяца. После истечения двух месяцев, этот проект, скорее всего, будет закрыт.

Однако Александр Александрович оговорился, что Управление образования не окончательно отказывается от идеи, по оснащению школ города новой пропускной системой.

– Не удалось убедить всех родителей. А когда три класса ходят по карточкам и питаются по карточкам, а все остальные проходят просто так, то особого смысла смысла в такой организации нет. Хотя, если мы берем школы областные, берем школы в других городах, там это все работает. В школах, в которых планировалось ввести, такое оборудование установлено не было. Была инициатива, но на этом, к сожалению, все закончилось. Но направление правильное, направление в котором необходимо будет работать. Не получилось сейчас, но закон требует, требует время. Думаю, что в ближайшее время этим вопросом заниматься мы будем, и, все-таки, такие системы внедряться будут, – пояснил Александр Колганов.

Стоит отметить, что первыми свое недовольство высказали родители школы № 1 «Полифорум», и впервые узнали они об этом аппаратно-программном комплексе в то время, когда Александр Колганов занимал пост директора той самой школы № 1.

Персональные данные 100 млн пользователей TrueCaller в опасности

28 марта 2016, США, internetua.com. Уязвимость в приложении позволяет злоумышленникам похитить персональные данные более чем 100 млн пользователей.

ИБ-эксперты из исследовательской лаборатории Cheetah Mobile Security обнаружили уязвимость в приложении TrueCaller. Ошибка позволяет злоумышленникам похитить конфиденциальную информацию более чем 100 млн пользователей программы.

Как было обнаружено исследователями, приложение использует лишь IMEI номер для идентификации абонента. Любой человек, имеющий серийный номер устройства, может получить личную информацию пользователя (номер телефона, домашний адрес, почтовый ящик и т.д.), а также изменить настройки приложений (отключить спам-блокаторы, добавить и удалить пользователей из черного списка).

Команда экспертов уведомила разработчика TrueCaller об уязвимости и предложила свою помощь в решении проблемы. 22 марта текущего года создатель выпустил обновленную версию программы. Большинство пользователей по-прежнему не обновили приложение до последней версии, поэтому гарантировать безопасность их данных невозможно.

Truecaller - интеллектуальное приложение, находящее любой номер по всему миру и определяющее неизвестные входящие вызовы с помощью технологии Caller ID. Приложение блокирует звонки, подтвержденные пользователями как спам.

Данные тысячи иностранцев слили в сеть в Таиланде

28 марта 2016, Таиланд, oxpaha.ru. Интернет-безопасность пользователей не всегда зависит от целенаправленных действий злоумышленников или хакеров. Иногда всему виной становится пресловутая халатность и невнимательность должностных лиц, в результате которой дискредитированными оказываются множество людей, чьи персональные данные попадают в сеть. Совсем недавно крупная утечка конфиденциальной информации произошла в Таиланде.

Так, Интернет-портал Security Week сообщил, что 27 марта в свободном доступе оказались данные о более 2000 тыс. иностранцев, проживающих в южных провинциях Таиланда. Открытая информационная база содержала имена, адреса проживания, род деятельности и паспортные данные граждан других государств, пребывающих в настоящее время в «стране улыбок». Несмотря на то, что сайт, предоставивший личную информацию об иностранцах, был заблокирован уже на следующий день, история успела наделать много шума.

Выяснилось, что утечка произошла по вине Интернет-разработчика, который тестировал новую систему для иммиграционной полиции Таиланда. Напомним, что власти страны, имеющие тесную связь с военными структурами, начали активную кампанию «Good guys in, bad guys out» («хорошие парни остаются, плохие уезжают») по выявлению экспатов, граждан иностранных государств, а также международных преступников, находящихся в Таиланде с просроченными или недействительными визами, и их выдворению за пределы королевства.

Хотя доменное имя сайта не имело никаких связей с официальными структурами тайских властей, местной активистской группе Интернет – пользователей Thai Netizens, выступающей за соблюдение прав и свобод в сети, удалось выяснить владельца ресурса. Оказалось, что разработчик тестировал сервис для туристической полиции, собирающей данные об иностранных нелегалах, когда по случайности и произошла утечка конфиденциальных данных.

Хотя иммиграционные власти Таиланда отказались от комментариев, IT-компания Akram Aleeming, замешанная в скандале, сделала официальное заявление в Facebook, сообщив о своей ошибке в ходе тестирования демо-версии Интернет-ресурса.

У коллекторов оказались персональные данные клиентов брянских банков

28 марта 2016, Россия, Брянская обл., bryansknovosti.ru. Активисты Общероссийского народного фронта проводят в Брянской области мониторинг финансового рынка, в частности, взаимодействия банков с коллекторскими агентствами. В регионе участились случаи, когда коллекторы звонят должникам с угрозами. Зачастую клиентов банка даже не предупреждают, что их долг передан третьим лицам.

В ходе мониторинга выявлены случаи, когда сотрудники брянских отделений банков для выполнения планов открывали кредитные карты для своих клиентов. Гражданам звонили и говорили, что им нужно приехать и забрать уже готовую кредитную карту. Клиенты получали карту и даже не активировали ее. Через год в дело вступали коллекторы, которые требовали погасить долг в 300 рублей, угрожая жизни и здоровью. Обратившись в отделение банка, клиент узнавал, что долг за обслуживание навязанной услуги составляет одну тысячу рублей, а 300 рублей – это плата за услуги коллекторскому агентству.

За разъяснением данных фактов активисты ОНФ обратились к управляющему одного из банков, на который поступали жалобы. Руководитель брянского филиала банка не смог внятно объяснить, на каких основаниях за неактивированную карту нужно платить и как персональные данные клиента попали к коллекторскому агентству.

Активисты ОНФ подготовили запрос в отделение по Брянской области Главного управления Центрального банка РФ по ЦФО с просьбой урегулировать работу коммерческих организаций в части правомерности передачи персональных данных коллекторским агентствам без должного предварительного урегулирования.

«Никто не в праве принимать решения за клиента банка. В связи с участившимися фактами различного рода уловок финансовых организаций эксперты ОНФ начали работу по обучению населения финансовой грамотности», – сказал руководитель региональной рабочей группы ОНФ «Честная и эффективная экономика» Алексей Изотенков.

Неизвестные опубликовали персональную информацию 50 млн граждан Турции

05 апреля 2016, Турция, в-деталях.рф. Утекшая база данных предположительно содержит личные данные президента Турции Реджепа Тайипа Эрдогана.

Неизвестные заявили о публикации в Сети персональной информации порядка 50 млн граждан Турции, в том числе президента страны Реджепа Тайипа Эрдогана и премьер-министра Ахмета Давутоглу. В результате инцидента произошла утечка имен, дат и мест рождения, адресов проживания и прописки, сведений о половой принадлежности и родителях, а также данных удостоверений личности (TC Kimlik No). В распакованном виде объем документов составляет 6,6 ГБ. По всем файлам можно без труда осуществлять поиск.

Как отметил немецкий независимый исследователь Якоб Аппельбаум (Jacob Appelbaum), если опубликованная информация подлинная, данный инцидент является одной из самых масштабных утечек персонально идентифицируемой информации со времен атаки на Управление кадровой службы США. Отметим, по состоянию на 2015 год население Турции составляло 79 млн человек.

По данным компании Cybersecurity Help s.r.o., торрент-файл с утекшей базой была создана в воскресенье, 3 апреля, и тогда же в турецких СМИ появились первые упоминания об инциденте. Днем позже ссылка на БД была опубликована на сайте Reddit. Утечка затрагивает граждан, рожденных до 30 марта 1991 года. Не исключено, что опубликованные неизвестными данные были похищены в результате масштабной утечки информации турецих граждан, имевшей место еще в 2009 году.

ИНДИКАТОРЫ РАЗВИТИЯ
Российская практика

Вопрос утечки личных данных больше беспокоит мужчин, чем женщин

07 марта 2016, Россия, Москва, 3dnews.ru. «Лаборатория Касперского» обнародовала результаты исследования на тему того, кто откровеннее в Интернете — мужчины или женщины. В опросе приняли участие почти 12 000 веб-пользователей из 27 стран, в том числе из России.

Оказалось, что представительницы прекрасной половины человечества любят рассказывать в Интернете о себе и своих знакомых при помощи фотографий. Так, своими изображениями делятся 66 % женщин, а еще 30 % публикуют снимки, на которых присутствуют их друзья и близкие. Среди мужчин оба показателя ниже — 54 % и 28 % соответственно.

В то же время видеоролики с собой в главной роли выкладывали в Сеть 20 % российских мужчин, а видео со своими знакомыми — 15 %. И в этом они опережают женщин, для которых аналогичные показатели составляют 16 % и 12 %.

В целом женщины в России в два раза реже мужчин делятся излишне личными фотографиями и видеороликами в Интернете — 11 % против 20 %. Вместе с тем дамы гораздо охотнее делятся в Сети информацией о своих увлечениях и личных отношениях (32 % женщин против 25 % мужчин), а также контактными данными (55 % и 51 %). При этом дату своего рождения в равной степени легко раскрывают 37 % мужчин и женщин.

Что касается вопроса утечки личных данных, то он больше беспокоит сильный пол. Так, мужчины чаще женщин проверяют, не содержит ли готовый к публикации пост или сообщение конфиденциальной информации (32 % против 29 %), отказываются от использования соцсетей или мессенджеров, если их работа угрожает безопасности персональных данных (26 % против 21 %), и предпочитают не откровенничать в Сети во время праздничных застолий с алкоголем (22 % против 15 %). При этом, впрочем, женщины стремятся разделять личную и рабочую коммуникацию и делятся частной информацией только в кругу семьи и близких друзей (50 % против 39 % мужчин).

Банковская тайна не защитит ипотечных должников

17 марта 2016, Россия, Москва, gazeta.bn.ru. Адвокаты должников неоднократно выдвигали в судах тезис, что передача данных должника коллектору является нарушением банковской тайны. Но очень редко находили у судей понимание.

Что есть банковская тайна

Вопросы раскрытия банковской тайны регулируются статьями ФЗ «О банках и банковской деятельности», Гражданского кодекса РФ и Уголовного кодекса РФ. Банк гарантирует тайну счета и вклада, операций по счету и сведений о клиенте.

В реальности уголовные сроки при нарушениях прав физлиц не назначаются: нарушившего права физлиц банковского сотрудника обычно ждет штраф и, возможно, увольнение.

Например, по сообщению пресс-службы прокуратуры Ленинградской области, в позапрошлом году в городе Сосновый Бор за разглашение банковской тайны был вынесен приговор бывшему служащему банка. Сотрудник злоупотребил служебным положением и собрал сведения о состоянии счета должника, после чего предоставил их местному ОМВД.

Впоследствии банковский служащий был признан виновным в совершении преступления, предусмотренного частью 2 статьи 183 УК РФ (разглашение банковской тайны), и оштрафован на 15 тыс. руб. Отметим, что наказанное лицо преследовало личные интересы, а не интересы работодателя. То есть ситуация не являлась типичной для российского долгового рынка.

ВАЖНО

Уголовная ответственность за нарушение банковской тайны предусмотрена в части 1 статьи 183 УК РФ. Последний раз данная статья пересматривалась 2 июля 2015 года. Тогда был подписан федеральный закон № 193-ФЗ, который, кроме прочего, усиливал ответственность за «незаконное получение и разглашение сведений, составляющих коммерческую, банковскую и налоговую тайну»

Банковская тайна и ипотечные долги

Между тем на долговом рынке наблюдается повышенный интерес к данному разделу отечественного права. В последние годы взявшие ипотеку россияне все чаще пытаются использовать нормы о банковской тайне, когда не справляются с долговым бременем. Аргументация следующая. Банк не имеет права передавать информацию о кредите третьим лицам. Если к сведениям о долгах был допущен кто-либо посторонний, например коллектор, это следует считать нарушением законодательства.

Впрочем, гендиректор «Агентства Судебного Взыскания» Максим Богомолов поясняет, что на практике понятие банковской тайны в судах используется, лишь когда речь идет о банковском счете и движении средств на нем. Кредитные отношения остаются в стороне. «Центробанк и суды высшей инстанции не склонны находить нарушения банковских тайн в сложившихся на практике кредитных отношениях, – рассказывает эксперт. – Иначе мы бы давно получили соответствующие постановления, определения и инструкции».

Руководитель антиколлекторского агентства STOP collection Елена Карышева рассказывает о другом «стандартном» поводе для обращений должников в суды. По ее словам, нередки случаи, когда представители кредитора начинают беспокоить звонками ближайшее окружение должника, прежде всего созаемщиков и поручителей. «Здесь действительно есть факт нарушения банковской тайны», – констатирует антиколлектор. Но законодательно не прописан механизм санкций за такие действия.

По сути, законодательство о банковской тайне для защиты должников не подходит.

Время давать согласие и его отзывать

Правда, в правовом поле присутствует еще ряд законов и нормативных актов, «закрывающих» часть личной информации о россиянах. В частности, защиту информации об ипотечных заемщиках в теории мог бы обеспечить закон № 152-ФЗ «О персональных данных». Именно он заставляет банкиров собирать с потенциальных заемщиков подписи под согласиями на обработку персональных данных. Ведь подпись в дальнейшем позволит распоряжаться данными по своему усмотрению. То есть, в принципе, разглашать информацию о заемщике третьим лицам сотрудник банка права не имеет. Но в поисках должника вполне может звонить по телефонным номерам, указанным в подписанной клиентом анкете. При условии, что заемщик подписал согласие на обработку персональных данных.

Часть юристов, обещающих должникам быстрое освобождение от долгов, рекомендуют первым же шагом подать в банк заявление о запрете обработки персональных данных. Дескать, как дал разрешение, так и отзываю. Но, скорее всего, должник получит отрицательный ответ. «Согласно п. 5 ч. 1 ст. 6 ФЗ № 152-ФЗ от 27.07.2006 “О персональных данных” согласие субъекта персональных данных не требуется в случае, если обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных», – говорится в типичной отписке одного из банков. Проще говоря, пока не расплатишься с долгами, отозвать разрешение на обработку нельзя. Так что просрочивший выплаты заемщик вряд ли сможет обернуть себе на пользу и 152-ФЗ.

Другое дело, что забрать разрешение будет разумным сразу после погашения кредита. Ведь впоследствии может произойти утечка клиентской базы, и бывшему заемщику станут по десять раз на дню названивать продавцы различных товаров. Кроме того, сам банк в перспективе может попытаться воспользоваться базой для навязывания непопулярных услуг.

Какие персональные данные банк вправе запросить у клиента

22 марта 2016, Россия, Самарская обл., gid.volga.news. Какой бы ни была цель вашего визита в банк, первое, о чем вас просят, - заполнить анкету. Таким образом мы передаем кредитной организации множество информации о себе: от паспортных данных до контактов своих ближайших родственников и знакомых. Но что потом с ними происходит, где все это хранится и отвечает ли банк за утечку ваших персональных данных? Выясним в сегодняшнем обзоре.

На вес золота

Сегодня любая информация о человеке приобретает особую ценность. Поэтому защита персональных данных граждан становится не только важным направлением в работе всех без исключения крупных компаний, но и требованием российского законодательства. Ведь в руках мошенника информация о человеке может превратиться в орудие преступления, а в руках уволенного сотрудника - товаром для продажи конкуренту и даже инструментом мести.

Стоит отметить, что пристальное внимание к этому вопросу в обществе начали проявлять только в последние годы, да и сам закон "О персональных данных", регламентирующий порядок действий с подобной информацией, появился всего 10 лет назад. Он гласит, что под понятием "персональные данные" подразумевается любая информация, прямо или косвенно относящаяся к определенному или определяемому физическому лицу (например, сведения о профессии, доходах, социальном положении, а также любая другая информация).

Однако обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается - за редкими исключениями, также указанными в законе.

На добровольных условиях

Что же из вышеперечисленного кредитная организация может потребовать от клиента? Как поясняет заместитель председателя правления "Ренессанс Кредит" Сергей Королев, банк запрашивает только те персональные данные, которые необходимы для проверки его платежеспособности как заемщика, а также для заключения с ним договора. К таким сведениям относятся ФИО, адрес, номер телефона, паспортные данные.

"Но банк может попросить предоставить не только прямые контакты, но также телефоны знакомых или родственников, - продолжает эксперт. - Данная информация запрашивается с целью проверки клиента, а также для связи с ним в случае, если по предоставленным прямым номерам банк не сможет до него дозвониться. При этом отказ клиента в предоставлении контактов родственников или знакомых не влияет на решение финансовой организации о выдаче кредита или оказании иных услуг".

Добавим к этому, что в последнее время банки довольно часто при заключении договора (будь то открытие счета или оформление потребкредита) делают фотографию клиента. Согласно закону, такой снимок, привязанный к анкете конкретного человека, будет тоже представлять собой персональные данные.

Как сообщили в пресс-службе ВТБ24, это дополнительный элемент идентификации клиента. "Делается это, прежде всего, в целях предотвращения мошеннических действий, - поясняют в банке. - Представим ситуацию, что у вас украли паспорт и преступники попытаются получить по нему кредит. В этом случае сотрудник банка обязательно сверит фото клиента в анкете, хранящейся в базе, и в предоставленном паспорте, с лицом человека, подающего заявку. Конечно, несоответствия не останутся без внимания со стороны службы безопасности банка".

Эти требования вполне законны. "Банки имеют право запросить любую информацию у клиента, в том числе о составе семьи, доходах, иных кредитах и счетах, - комментирует партнер Адвокатского бюро RBL Илья Мунаев. - Банкам необходима информация, которая тем или иным образом отражает финансовое состояние клиента, его платежеспособность и благонадежность. Кроме того, сами банки в ходе проверки со стороны контролирующих органов обязаны предоставлять информацию о своих клиентах, например, на основании федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" или на основании федерального закона "О защите прав и законных интересов инвесторов на рынке ценных бумаг". Но никакого специального закона, который обязывал бы гражданина предоставлять такие данные, не существует, все предоставляется добровольно".

Когда клиент дает добро

Наряду с предоставлением персональных данных кредитные организации просят клиентов дать согласие на их обработку. Это означает, что клиент согласен на любые действия, предусмотренные законодательством, которые будут производиться с информацией о нем. Обработка включает в себя сбор данных, запись, систематизацию, накопление и хранение, а также уточнение (обновление и изменение), извлечение, использование, обезличивание, блокирование, удаление и уничтожение.

Банк обращается к этим сведениям, если необходимо предоставить клиенту какую-то информацию - как по просьбе самого клиента, так и по инициативе банка. В том случае, если клиент не заинтересован в дальнейшем сотрудничестве с кредитной организацией, он может попросить удалить свои персональные данные. "Для этого необходимо направить в банк заявление об отзыве своего согласия на обработку персональных данных, - советует Сергей Королев. - Кредитная организация в течение 30 дней рассматривает это заявление и прекращает обработку персональных данных - удаляет их из базы".

Что касается опасения клиентов по поводу, что отказ от согласия на обработку персональных может стать основанием для отказа, допустим, в выдаче кредита, эксперт поясняет: "Каждый банк это решает индивидуально в соответствии со своими внутренними политиками. Но отказ в предоставлении кредита в этом случае будет правомерен, так как, в соответствии с законодательством, банк не обязан предоставлять кредиты абсолютно всем, кто за ними обращается".

Как долго хранится информация

По умолчанию банк хранит персональные данные клиентов до истечения срока, установленного законодательством. Максимальный срок законом не ограничен, однако ст. 5 закона "О персональных данных" говорит, что хранение персональных данных осуществляется не дольше, чем того требуют цели их обработки. Как правило, персональные данные хранятся в течение пяти лет с момента исполнения обязательств по договорам или до отзыва клиентом своего согласия на обработку персональных данных.

"Также возможны минимальные сроки хранения персональных данных, - поясняет Илья Мунаев. - Например, в отношении кредитного договора данные хранятся до истечения срока действия кредитного договора плюс срок исковой давности на случай, если возникнут проблемы по исполненному договору".

Информация под защитой

По закону, все операторы, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

В случае нарушения наступает ответственность, например, в виде возмещения морального вреда, причиненного субъекту персональных данных вследствие нарушения его прав или по причине нарушения правил обработки персональных данных.

При этом, по словам Сергея Королева, передача информации судебным приставам, в суд или другим органам осуществляется в соответствии с законодательством, и на такую передачу согласие клиента не требуется. Если же клиент считает передачу данных незаконной, то он может направить жалобу в надзорный орган Роскомнадзор, и банк будет привлечен к ответственности.

Кстати, по информации Роскомнадзора, наибольшее количество жалоб на банковскую сферу поступает от граждан именно в части нарушения прав субъектов персональных данных. Так, с 2014 по 2015 гг. их число увеличилось вдвое, при этом количество подтвержденных доводов граждан идет на спад.

В 2015 году Роскомнадзором проведено 14 контрольно-надзорных мероприятий в отношении кредитных организаций, при проведении 35% проверок были выявлены нарушения законодательства. Что характерно, подавляющее количество жалоб традиционно касается передачи персональных данных коллекторским агентствам. В этой связи в 2016 году в отношении кредитных организаций Роскомнадзором запланировано 65 контрольно-надзорных мероприятий.

Персональные данные детей теперь защищены законом

22 марта 2016, Россия, Москва, kr-gazeta.ru. Персональные данные детей, которые еще не достигли совершеннолетия, теперь находятся под защитой официального законодательства России. Официальное ведомство Российской Федерации Роскомнадзор в ходе запланированной проверки обнаружило ряд грубых нарушений законодательства, касающихся размещения персональных данных детей на сайтах.

Прежде всего под прицелом оказались такие данные детей, как их адреса, телефоны, а также места работы родителей. Кроме того, некоторые сайты имели в открытом доступе информацию о том, к какой социальной группе относятся семьи учеников.

Что касается фотографий, существует закон «О защите персональных данных», согласно которому без разрешения человека публиковать его фото запрещено. В случае фотографий детей разрешение необходимо со стороны его родителей или законных представителей. Такая же ситуация и с фамилией и именем ребенка.

Однако законодатели признают, что единой формы решения этой проблемы пока нет. В частности, недоразумения в этом плане могут случаться в детском саду или школе. В общем виде формулировки закона сводятся к тому, что без разрешения публиковать фотографии и персональные данные (Ф.И.О., номер телефона, адрес) нельзя, а значит, имея разрешение — можно. Соответственно, все, что нужно сделать педагогам, это взять письменное разрешение родителей или законных представителей о возможности использования персональных данных детей с уточнением, каких именно персональных данных. Такое разрешение можно спросить у родителей сразу при поступлении в образовательное учреждение либо каждый год, либо для каждого мероприятия.

Впрочем, о мероприятиях разговор отдельный. Статья 152.1 Гражданского кодекса РФ говорит, что согласие не требуется в случаях, если:

— использование изображения осуществляется в государственных, общественных или иных публичных интересах;

— изображение гражданина (в том числе несовершеннолетнего гражданина) получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и тому подобном), за исключением случаев, когда такое изображение является основным объектом использования;

— гражданин (в этом случае, безусловно, речь уже идет о совершеннолетнем) позировал за плату.

Вывод: руководствуясь Гражданским кодексом РФ, фотографии детей с публичных мероприятий можно публиковать без проблем и опасений, а фотографии, где отдельно взятый ребенок, например, сидит за партой и решает задачу, — нельзя.

Подобные проблемы говорят в пользу того, что в любом случае лучше взять разрешение на публикацию фотографий и персональных данных (Ф.И.О.) и уведомлять родителей о публикации тех или иных информаций в сети. Ведь, публикуя что-либо в Интернете, вы публикуете это навсегда. И ребенок даже через много лет может иметь последствия от публикации, сделанной, когда он был в детском саду. Без крайней необходимости не публикуйте в сети ФИО детей, сведения о них (а это — персональные данные) и их фотографии.

Надо знать, что за публикацию фотографий детей в Интернете без согласия их родителей предусмотрена ответственность по статье 137 Уголовного кодекса РФ. В случае, если суд признает вину, лицо, опубликовавшее фотографию, будет наказано штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода за период до 18 месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 4 месяцев.

А вы за личные данные переживаете?

24 марта 2016, Россия, Алтайский край, altapress.ru. Мировую общественность всколыхнула история с отказом компании Apple взломать смартфон террориста по требованию ФБР.

Люди разделились на две стороны: одни выходят на улицы с плакатами, скандируя, что неприкосновенность личной информации превыше всего, другие считают, что в таких случаях о неприкосновенности не может идти и речи. Россию дела ФБР мало заботят, но новостей про хакерские атаки, воровство сим-карт и банковских данных с каждым днем все больше.

Недавно скандал с утечкой персональных данных разгорелся в Барнауле. На сайте краевого медучреждения были опубликованы имена, места прописки и сведения о поставленном диагнозе несовершеннолетним пациентам. Любой желающий мог прочесть эту информацию. В настоящее время база данных закрыта, а следователи ищут компанию, по вине которой это произошло. Мы решили узнать, боятся ли жители Алтая распространения своих личных данных.

Алена Бородулина, сотрудник компании МТС:

Я отношусь к защите своих персональных данных достаточно трепетно. Не указываю в соцсетях лишней информации, никогда не афиширую свое местоположение, не рассказываю о личной жизни. Потому что любая информация может быть использована против меня. Недавно мою знакомую обокрал приятель, который воспользовался тем, что она уехала на отдых и стала выкладывать фотографии с моря. Не могла удержаться от хвастовства. Кражу раскрыли, вещи вернули, но сколько неприятностей девушке в итоге пришлось вытерпеть из-за своей беспечности.

Марина Осипова, повар:

Мне абсолютно все равно. Я не предпринимаю никаких действий для сокрытия информации обо мне. Не понимаю, как может мне навредить информация о моем возрасте, месте проживания или работы. Понятно, что я не выкладываю во всеобщий доступ информацию о моем домашнем адресе, зарегистрированном на мое имя имуществе и так далее. Но ведь держать подобные сведения в тайне будет любой здравомыслящий человек, и это совсем не значит, что он хотя бы раз задумался о своих персональных данных.

Дмитрий Маричев, IT-специалист:

Я очень скрытный человек, и стараюсь максимально оградить себя от внешнего влияния и обезопасить. В интернете нельзя найти ни одной моей фотографии, я не зарегистрирован в соцсетях под своим именем и фамилией — сижу через фейковые страницы. В интернете я не нахожусь без действующей спецпрограммы, которая скрывает мой настоящий IP-адрес. Так что, чтобы найти меня, нужно очень постараться. И я не боюсь утечки моих персональных данных, потому что делаю все для того, чтобы они были в безопасности.

Анна Караваева, пенсионерка:

Не боюсь. Я не владею никакой важной информацией, красть у меня нечего, банковскими картами не пользуюсь. Да, я счастливый человек, завидуйте.

Виктор Павлов, банковский служащий:

Буквально на днях моя личная информация из одного онлайн-магазина утекла в "Яндекс". Теперь любой может увидеть номер моего телефона и адрес, а также то, что за 1,5 года я купил в том магазине монитор, блок питания и звуковую карту. Подаю в суд.

Павел Андреев: «Работодатель вправе контролировать переписку сотрудников и увольнять за «лайки»

25 марта 2016, Россия, Москва, up74.ru. Прецедент был создан румынским инженером, который был уволен за нарушение правил внутреннего распорядка организации. Тот использовал учетную запись в Yahoo Messenger не только для общения с клиентами, но и при личной переписке.

Европейский суд по правам человека отклонил жалобу заявителя, признав тем самым право работодателя контролировать переписку сотрудников в рабочее время. Ситуацию комментирует адвокат по трудовым спорам Павел Андреев.

— Вполне типичная картина для нашей действительности, когда в рабочее время, используя оплаченный интернет-трафик предприятия, сотрудники «пропадают» в социальных сетях, посещают всевозможные сайты, связанные с продажей, в личных целях, — отметил Павел Викторович. — Моя позиция однозначна: работодатель вправе за это привлекать к дисциплинарной ответственности. Пока еще не сложилась судебная практика компенсации работодателю затраченных средств, хотя очевидно, что вы свое рабочее время потратили на личные цели с использованием имущества работодателя. Запрет на такие действия необходимо фиксировать в трудовом договоре. Если вы используете собственный мобильный Интернет, то о компенсации речь не идет. Но после череды дисциплинарных взысканий за «лайки» на работе вполне логичным может быть увольнение.

Вопрос: Судя по примеру с румынским инженером, это мировая практика. И создан прецедент увольнения.

Павел Андреев: Принятое Европейским судом по правам человека решение распространяется на все государства, которые ратифицировали Европейскую конвенцию по правам человека, включая Россию. Стоит добавить, что, помимо Интернета, любое отвлечение от работы, не связанное с производственной деятельностью, является нарушением трудовой дисциплины. И, повторюсь, наказанием может стать и увольнение.

Вопрос: Но встает вопрос о правомерности контроля за личной перепиской со стороны работодателя. Насколько это законно?

Павел Андреев: Работодатель, на мой взгляд, с точки зрения защиты персональных данных, не вправе осуществлять просмотр личных аккаунтов своих сотрудников. Но в случае с инженером речь идет об использовании в личных целях служебных аккаунтов.

Кроме того, работодатель вправе ограничить доступ к социальным сетям и сайтам, не связанным с трудовой деятельностью. Это законно и обоснованно. К слову сказать, многие компании так и делают. А если будет установлено, что вы с личных девайсов на работе ведет личную переписку, продажи, то это влечет дисциплинарное взыскание. Прецедент, созданный Страсбургским судом, позволяет работодателю знать, чем занимается его сотрудник в рабочее время, и контролировать деятельность работников по использованию Интернета только для осуществления профессиональной деятельности.

«Лаборатория Касперского»: беспечность при установке программы открывает путь киберпреступникам

28 марта 2016, Россия, Москва, kaspersky.ru. Российские пользователи беспечно относятся к процессу установки новых программ на компьютеры и мобильные устройства, тем самым подвергая свой цифровой мир серьезному риску. К такому выводу пришла «Лаборатория Касперского» в результате исследования активных пользователей Интернета по всему миру*.

Так, 35% россиян не ограничивают права приложений при их установке на мобильные гаджеты. Более того, 10% ошибочно уверены, что никак не могут повлиять на список прав, доступных приложениям. Беспечность и неосведомленность пользователей приводят к тому, что приложения на совершенно законных основаниях могут получить доступ к конфиденциальной информации на устройстве — контактам, фотографиям и геолокационным данным.

Важной мерой безопасности является внимательное чтение лицензионного соглашения. Однако при установке программы на ПК или мобильное устройство его игнорируют 65% пользователей, а каждый пятый владелец компьютера (22%) даже не вчитывается в содержание установочных окон, просто нажимая «далее, далее, согласен, далее».

В результате приложения получают слишком широкие права, что может угрожать безопасности пользователя. Владельцы гаджетов, сами того не подозревая, могут разрешить выложить в общий доступ свои личные данные, установить дополнительные, например, платные, приложения или даже внести серьезные изменения в настройки операционной системы.

«Мало кто задумывается, что установленные приложения могут способствовать утечке конфиденциальных данных, хранящихся на устройстве. Игнорирование таких мер безопасности как контроль прав доступа, запрашиваемых программой при установке и первом запуске, дают злоумышленникам возможность обойти встроенные механизмы защиты и в конечном итоге получить доступ к персональной, а в некоторых случаях и финансовой информации. Чтобы этого избежать, нужно, как минимум, быть очень внимательным и не лениться читать все предложенные программой пункты при ее установке», — напоминает Юрий Наместников, антивирусный эксперт «Лаборатории Касперского».

«Лаборатория Касперского» рекомендует внимательно относиться к выбору приложений и источников их загрузки, обязательно читать условия лицензионного соглашения, отслеживать список прав, доступных новому приложению, и использовать надежное защитное решение, например, Kaspersky Internet Security для всех устройств. Продукт позволяет настроить режим безопасных программ, который разрешает запуск только доверенных приложений и ограничивает работу всех подозрительных программ.

*Данные исследования поведения пользователей в Сети, проведенного «Лабораторией Касперского» в 2015 году среди более 18 тысяч интернет-пользователей старше 18 лет из 16 стран по всему миру, в том числе 1056 человек из России.

Защита персональных данных граждан – одна из главных задач государства

29 марта 2016, Россия, Вологодская обл., severinfo.ru. Перед руководителями 26 муниципальных районов области, городов Вологды и Череповца, руководителями бюджетных учреждений области были поставлены задачи по повышению эффективности мер по обеспечению безопасности персональных данных в условиях изменения законодательства Российской Федерации и сокращению количества основных ошибок в данной работе. Сегодня в Правительстве области под руководством первого заместителя Губернатора области Алексея Шерлыгина состоялась научно-практическая конференция «Обеспечение безопасности персональных данных».

По итогам 2015 года положительно оценена работа администрации Вологды, мэрии Череповца, администрации Шекснинского муниципального района по организации взаимодействия с подведомственными учреждениями в части оказания методической и консультационной помощи в сфере защиты персональных данных.

«В эпоху глобализации, когда информационное пространство увеличивается, охватывая все сферы человеческой деятельности, необходимость защиты прав субъектов персональных данных очень велика. Мы обязаны на своем уровне обеспечить максимальную защиту данных граждан. Следует отметить, что в органах исполнительной государственной власти и органах местного самоуправления проведена работа по совершенствованию системы информационной безопасности, по разработке организационно-распорядительных документов по обеспечению безопасности персональных данных с учетом требований законов», - отметил Алексей Шерлыгин.

С каждым годом тематика конференции становится все более актуальной, особенно учитывая постоянное совершенствование законодательства о защите персональных данных в РФ.

На конференции шла речь о новой системе учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам, о защите информации в муниципальных информационных системах и технических вопросах работы учреждений в сфере защиты персональных данных.

Acronis анонсирует результаты глобального исследования по хранению данных

31 марта 2016, Россия, Москва, acronis.com. По мере того, как количество ПК и мобильных устройств в семьях возрастает, люди начинают ценить свои личные данные больше, чем сами устройства

Международное исследование компании Acronis, приуроченное к Всемирному дню резервного копирования 31 марта показало, что пользователи стали больше ценить свои данные и меняют свое отношение к вопросам их защиты. Более половины респондентов отметили, что в их семьях имеется более четырех цифровых устройств, информация на которых нуждается в защите. При этом 45% участников исследования ответили, что больше всего боятся потерять личные фотографии и видеозаписи.

Новые поводы для беспокойства о сохранности своих персональных данных

Количество угроз безопасности персональных данных постоянно растет. К такими типичными причинам потери данных, как неисправности техники или удаление файлов по ошибке, добавляются новые - «программы-вымогатели». Это вредоносные программы, которые блокируют доступ к компьютерным системам и их данным до тех пор, пока жертвы не заплатят выкуп.

Согласно данным Центра жалоб на преступления в Интернете (Internet Crime Complaint Center), в период с апреля 2014 года по июнь 2015 года поступило 992 жалобы на преступления с использованием «программ-вымогателей» и их общий ущерб составил 18 миллионов долларов. Наиболее эффективным средством борьбы с последствиями подобных преступлений является регулярное резервное копирование.

Исследование, проведенное Google по заказу компании Acronis, позволило получить представление об отношении к цифровой безопасности и способах защиты данных в таких странах, как Россия, Германия, Франция, Испания, Великобритания, США, Канада, Япония и Австралия. Результаты исследования подводят к следующим выводам:

- 30% респондентов назвало «Простоту использования» в качестве основного требования в системе резервного копирования, а «Безопасность» и «Конфиденциальность» волновали 36% и 26% участников опроса соответственно.

- 46% опрошенных человек пользуются 4-я и более девайсами (компьютерами, ноутбуками, смартфонами), находясь дома.

- Облачное резервное копирование выбирали 30% респондентов, а внешними носителями пользуются 38% опрощенных.

- 58% пользователей создают резервные копии ночью, а 27% — «фоново» (как правило, во время просмотра телевизора).

Поведение российских пользователей во многом совпадает с поведением респондентов из других стран. Однако можно выделить несколько особенностей, характерных именно для пользователей в России:

- Российские пользователи склонны хранить всю информацию на локальных дисках и на личном компьютере, так поступают 23% и 32% респондентов из России соответственно, хотя в остальном мире локальный бэкап делают 38% респондентов;

- Облачными сервисами для хранения резервных копий в России пользуются лишь 5% респондентов, хотя показатель для остальных стран составляет 30%.

Сохранность данных всех членов семьи

В современной среднестатистической семье имеется как минимум четыре электронных устройства, данные которых нуждаются в защите и резервном копировании. Все чаще в семьях появляется человек, ответственный за сохранность данных всех членов семьи. Объемы данных, которые создают люди, постоянно растут, количество фотографий и видео, аудио-файлов с музыкой и отсканированных документов неуклонно увеличивается. Долг «хранителя» состоит в защите данных, которые хранятся на электронных устройствах родственников.

Милонов: Windows в госорганах необходимо запретить

05 апреля 2016, Россия, Москва, riafan.ru. Операционная система нового поколения Windows 10 вызывает у пользователей множество вопросов. Многих смущает тотальная слежка, создание своей закрытой экосистемы и даже, по некоторой информации, принудительная установка новой версии операционки вместо предыдущих версий.

Корреспондент Федерального агентства новостей пообщался с российским политиком о необходимости защиты государственных органов от Windows 10.

Как известно, последняя операционная система от Microsoft собирает персональные данные пользователя. Windows 10 считает всё — запросы поиска, личные переписки, файлы, которые находятся на жестком диске. Так, например, как сообщают эксперты издания ARS Technica, проведшие соответствующее исследование, последняя версия Windows отсылает на сервера Microsoft информацию пользователей даже в том случае, если было произведено отключение функций, которые связаны со сбором и хранением персональных данных пользователя.

В то же время в прошлом месяце на известном сайте Reddit была опубликована информация, согласно которой пользователи операционной системы Windows 7 столкнулись с очень неприятной ситуацией — в результате очередного обновления операционной системы на компьютер без предупреждения и разрешения пользователя была установлена Windows 10.

Сообщается, что обновление произошло достаточно быстро, некоторые компьютеры потратили на это не более 15 минут.

Российский политик, член партии «Единая Россия», депутат Законодательного собрания Санкт-Петербурга Виталий Милонов в беседе с корреспондентом ФАН рассказал, что в этом нет ничего необычного. По его словам, не нужно думать о том, что Windows 10 чем-то отличается от других операционных систем.

«Там также все тоже самое. Windows 10 также осуществляет слежку за пользователями, как это делает Windows 7, 8 и Vista. Windows XP и 2000 меньше следили, потому что технологии тогда были не того уровня, как сейчас. В этом плане Windows 10 ничем не отличается от прошлых версий. Просто «десятка» это делает, менее стесняясь, остальные стесняясь. Все операционные системы позволяют следить за пользователями в полной степени», — пояснил политик.

Что же касается того, что Windows 10 может сама себя установить внезапно и без разрешения, то, по мнению Милонова, точно также делали прошлые версии Windows. Здесь, повторился он, нет абсолютно ничего удивительного.

«Является ли это законным со стороны Microsoft? Нет, это абсолютно незаконная деятельность. Давно незаконная, с самого начала. Я давно говорил, что Windows надо запретить использовать в государственных органах. Особенно, когда там есть вопросы, связанные с конфиденциальной государственной информацией. Я не говорю даже про государственные секреты — там особый протокол. Но в принципе есть информация, которая нежелательная для легкого доступа другим, так сказать, сторонам. И Windows не обеспечивает эту защиту. Я давно поднимал этот вопрос. У нас же есть целый Сколково — там фонарики изобретают, недвижимость строят.

Грубо говоря, есть множество талантливых и молодых ребят-компьютерщиков из России, которые на основе Linux предлагают действительно более защищенные операционные системы. Предлагают более эффективную систему защиты данных. К тому же они — бесплатны, а мы платим за операционные системы от Microsoft. У Windows 10 сейчас бесплатное обновление, а так мы платим огромные деньги за платную версию, которая ко всему этому еще ворует наши данные», — резюмировал Виталий Милонов.

Опрос: 20% пользователей сталкивались с проблемой безопасности в соцсетях

05 апреля 2016, Россия, Москва, newkaliningrad.ru. Каждый пятый пользователь в России сталкивался с проблемой безопасности социальных сетей. Об этом свидетельствуют итоги опроса, проведенного Региональным общественным центром интернет технологий (РОЦИТ).

Социальными сетями пользуется около 60% россиян. В тройку самых популярных входят «ВКонтакте» (70,4% опрошенных), Instagram (43,6%) и Facebook (29,1%). Незначительно отстают «Одноклассники» (27,9%). Аудитория Twitter и Linkedin гораздо меньше — 10,3% и 3,2%, соответственно.

Каждый пятый пользователь (около 20%) сталкивался с проблемами безопасности в соцсетях. Речь чаще всего идет о краже пароля (26%) и взломе аккаунта (69,2%). При этом чуть более 23% опрошенных отметили, что при взломе мошенник выдавал себя за них и пытался выманить деньги у их друзей.

Также пользователи часто сталкиваются с кражей пароля от электронной почты, к которой привязан аккаунт в социальной сети (15,6%), и кражей денежных средств с банковской карты, привязанной к аккаунту (3,5%). При этом около 5% пользователей, у которых возникали проблемы, не смогли понять, куда им обращаться с жалобами на мошенников. По мнению 28% опрошенных, многие пользователи, попавшие в беду, просто не могут разобраться с техникой подачи заявления.

Зная об этом, мошенники пользуются ситуацией, создавая «фейковые» службы поддержки, стараясь завладеть персональными данными пользователей. Поэтому многие предпочитают решать проблемы самостоятельно, опасаясь кражи (15,9%) и разглашения своих персональных данных (19%).

В связи с этим авторитет служб поддержки в глазах пользователей невысок. За помощью к ним обращались около 32% опрошенных, решить проблему самостоятельно старался практически каждый второй. При этом около 63% обратившихся сумели устранить проблему.

Алина Кабаева ответила на открытое письмо журналистки Znak.com

05 апреля 2016, Россия, Москва, jourdom.ru. Бывший депутат госдумы, гимнастка Алина Кабаева ответила на открытое письмо журналиста Znak.com Лёли Мингалевой. Ответ поступил в редакцию по электронной почте от пресс-секретаря Кабаевой.

«Уважаемая редакция Znak.com!

В открытом письме, опубликованном на страницах вашего издания, прозвучал упрек в адрес инициированного мною закона N 50-ФЗ от 5 апреля 2013 года, который запрещает распространять в СМИ информацию о несовершеннолетних, пострадавших от противоправных действий. В письме говорится о том, что действующее законодательство, в том числе и закона N 50-ФЗ, не позволяет журналистам помочь ребенку, который попал в беду и теперь страдает по вине соцработников и чиновников.

Автор полагает, что «закон, некогда принятый для того, чтобы защитить детей от жестокости преступников, делает их жертвами преступного равнодушия тех, кому государство доверило заботу о наших маленьких согражданах» и «обеспечивает режим замалчивания того, мимо чего не должны проходить порядочные люди».

Это утверждение свидетельствует о том, что автор либо не разобрался, либо вообще не знаком с содержанием закона. Поэтому считаю необходимым дать разъяснения его сути.

Прежде всего, закон направлен не на то, чтобы защитить детей от жестокости преступников (это прерогатива других законов), а на то, чтобы защитить их от СМИ, для которых трагедии детей и подростков стали источником наживы, рабочим материалом для публикаций и ток-шоу, которые тиражируются на всю страну. Другими словами, защитить от журналистов, которых не волнует, как их «деятельность» скажется на психическом здоровье и без того травмированных детей.

Напомню, закон N 50-ФЗ принимался на основе многочисленных обращений граждан и представителей аппарата Уполномоченного по правам ребенка при Президенте РФ, которые указывали на фактическое отсутствие каких-либо ограничений для СМИ на распространение такого рода информации. В тот период СМИ, особенно телевидение, были переполнены сюжетами о детях, пострадавших от насилия.

Травмированных детей и подростков приводили в студию, расспрашивали и рассказывали об их беде на всю страну, и никого из авторов публикаций и передач не интересовало, что будет с детьми потом, как они будут себя чувствовать завтра, когда придут в свою школу, встретятся со своими сверстниками, с соседями по дому. Все попытки ограничить этот беспредел, недопустимый в цивилизованном обществе, сопровождались возмущенными заявлениями со стороны ряда СМИ о том, что это покушение на свободу слова. Справедливости ради замечу: часть журналистов, для которых понятие о журналистской этике не пустой звук, поддержала нас, признав, что беспринципность среди ряда СМИ в погоне за рейтингами просто зашкаливает.

Работая над законом, я и мои коллеги учитывали, какое влияние СМИ имеют на общество, поэтому я со всей ответственностью могу сказать, что закон не мешает инициировать общественный интерес к любому вопросу, в том числе и вопросу, связанному с насилием над детьми. Закон не препятствует также и публично обсуждать эти вопросы. При этом нет никакой необходимости показывать детей, называть их имена, адреса проживания. О фактах противоправных действий можно распространять информацию в обезличенном виде.

Закон N 50-ФЗ запрещает средствам массовой информации травмировать ребенка, устраивать из беды, в которую он попал, публичное зрелище, наживаться на этом, обеспечивая себе высокие рейтинги. Вместе с тем, закон не мешает журналистам реально помогать попавшим в беду детям. СМИ имеют право запрашивать у любого органа власти, в том числе и у правоохранительных органов, любую информацию, анализировать ее и распространять, не упоминая персональные данные детей.

Также хочу отметить, что зачастую практика применения закона искажает его смысл и напрямую противоречит намерениям его авторов. Нередко даже самые совершенные законодательные акты, направленные на помощь людям, не достигают своей цели из-за неграмотного, а иногда и намеренно искаженного правоприменения. Таким образом, некоторые ответственные лица пытаются оправдать свое бездействие, прикрыть недобросовестное исполнение обязанностей рамками закона. Искренне надеюсь, что в вашем случае мы не имеем дело с подобным пренебрежением законом со стороны представителей региональных органов власти.

Хочу поблагодарить вас за то, что не остаетесь безразличными к данной теме. Ее актуальность не вызывает сомнений, и я со своей стороны поддерживаю идею о продолжении публичной дискуссии о том, каким образом законодательное регулирование может помочь защитить детей от жестокого обращения, создать максимально благоприятные условия для их роста и развития.

С уважением, Алина Кабаева».

В «Национальной медиагруппе», председателем совета директоров которой работает Алина Кабаева, Znak.com подтвердили, что ответ готовила именно она.

Напомним, открытое письмо касалось закона о запрете на публикацию данных детей, ставших жертвами преступлений. Журналистка Znak.com обращала внимание, что законодательная норма в ряде случаев мешает защищать интересы детей, в частности собирать для них помощь и следить за их судьбой.

Закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части ограничения распространения информации о несовершеннолетних, пострадавших в результате противоправных действий (бездействия)" был принят в Государственной думе 22 марта 2013 года.

Главной целью закона было обеспечить безопасность пострадавших детей посредством нераскрытия персональных данных. Инициаторами выступили депутаты Алина Кабаева, Валентина Терешкова и Марина Мукабенова.

Зарубежная практика

Суд Гамбурга разрешил социальной сети Facebook требовать настоящие имена пользователей

06 марта 2016, Германия, b-online.ru. Согласно решению, принятому 3 марта административным судом Гамбурга, социальная сеть Facebook имеет все права требовать у пользователей указывать их настоящие имена. После данного судового постановления деятельность американской компании на территории Европы будет регулироваться нормами законодательства Ирландии, а не Германии.

Принятое судовое решение базируется на заявлении одного из пользователей, чей счет в социальной сети Facebook был заблокирован. Основанием для подобного решения стал факт использования псевдонима данным субъектом. Немецкое законодательство разрешает пользователям использовать псевдонимы при регистрации в социальных сетях.

Тем не менее суд Гамбурга при оглашении решения отметил, что отделение Facebook, которое руководит деятельностью соцсети за пределами США, располагается в Дублине, а значит, должно руководствоваться законодательством не Германии, а той страны, где производится обработка данных пользователей.

Это означает, что в Германии компания Facebook одержала юридическую победу.

Не так давно началось следствие в отношении возможных нарушений Facebook среди социальных сетей. Инициатором расследований стало антимонопольное ведомство ФРГ. Указывается, что со стороны Facebook замечены злоупотребления: компания разрабатывает свои договорные положения о использовании персональных данных таким образом, что в будущем это может повлечь за собой условия для того, чтобы занять доминирующее положение. Юристы отмечают, что предложенные положения нарушают нормы закона о защите персональных данных. В Facebook данное заявление опровергают.

В пользовательском соглашении Facebook обозначается, что при регистрации пользователи должны указывать личную информацию, которая соответствует паспортным данным. В случае несоблюдения настоящих правил, администрация соцсети имеет право ограничить доступ к страницам ресурса и заблокировать аккаунт.

ForgeRock: У компаний до сих пор нет надежных средств защиты конфиденциальности данных

18 марта 2016, США, securitylab.ru. Корпорация ForgeRock провела исследование, направленное на изучение надежности защиты конфиденциальности личных данных. В данном проекте принимали участие 300 IT-специалистов из 38 стран мира.

93% профессионалов согласны, обеспечение конфиденциальности данных клиентов компаний является большой проблемой для топ-менеджеров. Только 9% экспертов считают надежной нынешнюю защиту данных и доступные методы ее обеспечения. 96% респондентов признали необходимость динамичных и гибких средств обеспечения конфиденциальности.

93% профессионалов согласны, обеспечение конфиденциальности данных клиентов компаний является большой проблемой для топ-менеджеров

Данные инструменты должны адаптироваться к будущим нормативным требованиям и ожиданиям потребителей.

Исследование корпорации ForgeRock показало различия во мнениях специалистов из США и Европы. 84% американских экспертов уверены, Америка примет аналогичные европейским правила защиты персональной информации. С данным утверждением согласились только 66% европейских специалистов.

Нормативно-правовая база для обеспечения конфиденциальности данных беспрецедентно растет. Появляется все больше документов, подобных рамочному соглашению между США и Европой, именуемому «Безопасной гаванью» (Safe Harbor). В 2015 году Европейский суд отклонил данный документ, регулирующий передачу и хранение личных данных между странами ЕС и США. Впоследствии была объявлена замена соглашения Safe Harbor на «Щит приватности» (Privacy Shield). До сих пор неизвестно, утвердит ли суд новый образец.

Пользователи все более обеспокоены защитой конфиденциальности личных данных. Также важным фактором является способность контролировать, обрабатывать и обмениваться информацией о себе в сети.

SailPoint: Каждый пятый сотрудник компании готов продать учетные данные

21 марта 2016, США, security.dirty.ru. Работники склонны халатно относиться к безопасности корпоративных данных, однако беспокоятся по поводу своих собственных.

Согласно исследованию экспертов SailPoint, каждый пятый сотрудник компаний готов продать свой пароль, в 40% случаев даже менее, чем за $1 тыс. Некоторые также согласны выдать хакерам корпоративные учетные данные всего лишь за $100 и даже меньше.

В опросе SailPoint приняли участие 1 тыс. работников различных предприятий в США, Европе и Австралии со штатом, насчитывающим не менее 50 тыс. человек. Как показало исследование, сотрудники компаний не относятся должным образом к безопасности данных.

По словам 65% опрошенных, они используют один и тот же пароль для разных учетных записей, а почти треть из них обменивается своими учетными данными с сослуживцами. Таким образом, продать учетные данные готовы 10 тыс. человек, 32,5 тыс. используют одинаковые пароли для разных приложений и порядка 17 тыс. обмениваются ими с коллегами по работе.

Как оказалось, каждый третий сотрудник без ведома IT-отдела приобретает приложения, распространяемые по модели SaaS (программное обеспечение как услуга). По словам работников, они действуют в обход ИБ-специалистов, поскольку последние склонны чрезмерно усложнять процесс. Четверть респондентов загружают конфиденциальные документы в облачные хранилища с целью дальнейшего распространения за пределами компании. У 40% опрошенных до сих сохраняется доступ к учетным записям на прежних местах работы.

Сотрудники компаний склонны весьма халатно относиться к безопасности корпоративных данных, однако выражают обеспокоенность по поводу конфиденциальности собственной информации. 40% работников намерены уволиться с работы, если в их компании произойдет утечка.

Эдвард Сноуден прокомментировал слова главы Apple о защите персональных данных

21 марта 2016, Россия, Москва, rns.online. Бывший сотрудник американских спецслужб Эдвард Сноуден прокомментировал высказывание главы корпорации Apple Тима Кука о защите персональных данных.

«2016 год — это когда общество вынуждено отдать одной корпорации защиту своих прав. Это опасный сигнал», — написал он в Twitter. Комментарий он сопроводил хештегом #AppleEvent и ссылкой на заявление Тима Кука.

Ранее на презентации в штаб-квартире компании Тим Кук заявил, что компания не ожидала, что «вступит в противоречие с собственным правительством». «Мы обязаны защитить ваши персональные данные», — заявил Кук. По его словам, история с требованиями ФБР взломать iPhone террориста еще не завершена, она может создать опасный прецедент.

Калифорнийский суд 16 февраля предписал американской корпорации Apple изменить программное обеспечение на смартфоне модели iPhone 5c таким образом, чтобы следователи ФБР могли подобрать пароль к смартфону одного из двух террористов, которые в декабре 2015 года расстреляли в Сан-Бернардино 14 человек и ранили 21. Apple должна была исполнить предписание суда до 26 февраля 2016 года.

В ответ глава Apple Тим Кук заявил, что решение суда угрожает безопасности клиентов Apple. «Правительство США просит от Apple взломать устройства собственных пользователей и подорвать достигнутые за десятилетия успехи в сфере безопасности, которые защищают наших клиентов, в том числе десятки миллионов американских граждан, от хакеров и киберпреступников», — заявил глава корпорации в открытом письме.

В поддержку Apple уже высказались такие корпорации, как Facebook, Twitter, Microsoft, Google.

Как Telegram позволяет обойти закон американским чиновникам

23 марта 2016, США, rusbase.com. Новый поворот в споре между правительством США и технологическими компаниями на тему защиты персональных данных: законодатели в Сан-Франциско стали использовать мессенджер Telegram, чтобы уклоняться от выполнения законов о раскрытии публичных записей.

Как сообщает издание The Information, несколько членов наблюдательного совета Сан-Франциско вместе со своими советниками и помощниками активно пользуются мессенджером. При желании пользователи Telegram могут общаться через зашифрованные «секретные чаты», в которых можно настроить автоматическое удаление сообщений на устройствах отправителя и адресата.

Пока мессенджеры с функцией шифрования фигурируют в обсуждениях о том, как соблюдать баланс между обеспечением правопорядка и соблюдением кибербезопасности, политики также могут использовать такие программы для тайных переговоров. К примеру, чиновники в Сан-Франциско пользуются приложением Telegram с опцией автоматического удаления шифрованных сообщений.

Сотрудник администрации Сан-Франциско рассказал в интервью, что опыт использования Telegram он и его сослуживцы переняли у коллег из городского совета, которые отзывались о приложении как о способе обхода законов о публичных документах. «Приложение используют именно для этого, — сказал чиновник — все так делают».

Как гласит руководство, составленное прокуратурой Сан-Франциско, по закону о публичных записях штата Калифорния, текстовые сообщения и электронные письма, отправляемые представителями городской власти, считаются документами публичного характера в том случае, если в них помимо личной информации содержатся сведения, «представляющие интерес для общества». Прокурор города также отмечает, что письменную корреспонденцию, хранящуюся на личных устройствах госслужащих, тоже стоит считать публичными документами. Тем не менее, в руководстве написано, что суд еще не вынес решение о том, считается ли переписка на личных устройствах документами, представляющими общественный интерес.

В законе о публичных записях ничего не говорится о новых способах электронной коммуникации, таких как мессенджеры с функцией шифрования или удаления данных, но, как сказал руководитель рабочей группы по выполнению закона об открытости правительства Виктор Янг, «этот вопрос стал актуальной темой для обсуждения».

Предпочтения

Сообщения, зашифрованные в режиме «секретного чата» Telegram, могут быть стерты с устройств отправителя и адресата, так что пользователи, заинтересованные в том, чтобы информация была удалена, предпочитают это приложение конкурентам — WhatsApp и iMessage. На сайте Telegram, набравшего уже более 100 млн. ежемесячных активных пользователей по всему миру, говорится, что на серверах компании не сохраняются сообщения, отправленные в секретных чатах. Это значит, что даже при наличии судебного постановления сообщения нельзя будет прочитать, если пользователи включат опцию их удаления.

Несмотря на то, что в WhatsApp и iMessage переписка шифруется по умолчанию, у пользователей нет возможности удалять сообщения на устройстве получателя.

Эйприл Венерасьон, старший помощник наблюдателя Джейн Ким и пользователь Telegram, рассказала, что чиновники пользуются им в первую очередь из-за наличия опции «самоуничтожения». Она также отметила, что благодаря функции группового чата можно «связаться с нужным человеком практически мгновенно».

Венерасьон сказала, что не знала о том, что эти функции нарушают законы города или штата, касающиеся публичных данных. «Надо бы это уточнить!», — написала она в сообщении.

«Законы должны быть актуальными, — добавила ЛиЭнн Пэлхем, исполнительный директор комитета по вопросам этики Сан-Франциско. — Если эти люди занимаются вопросами, представляющими общественный интерес, тогда законы должны вовремя изменяться, чтобы регулировать все необходимые аспекты».

Привязанность к смартфонам

Еще один работник администрации Сан-Франциско, который зарегистрировался в Telegram после приглашения коллег, сообщил, что приложение понравилось госслужащим еще и потому, что они достаточно молоды, «активно пользуются смартфонами и ценят возможность быть на связи» друг с другом.

Джон Кени, глава правозащитной организации Reinvent Albany, которая базируется в Нью-Йорке и занимается вопросами подотчетности правительства, считает, что возросшая популярность мессенджеров сделала «размытыми» различия между письменной коммуникацией и личными или телефонными разговорами.

«В перспективе это может сделать законы [о свободном доступе к информации] абсолютно бесполезными, — сказал Кени. — Если общаться через защищенные каналы начнут все политики, общество мало что сможет сделать с этим прямо сейчас».

Непонятно, сколько именно сотрудников администрации Сан-Франциско являются пользователями приложения. С Telegram можно синхронизировать список контактов в телефоне. Простой поиск по приложению показал, что несколько наблюдателей и их помощников имеют статус «активен». Эти чиновники, а также помощники и советники регулярно используют Telegram для обсуждения различных вопросов.

«Telegram создан для политики», — сказал Джон Элберлинг, пользователь приложения, активист и советник по землепользованию в Сан-Франциско.

Джон Уандерлих, временный директор по политике фонда Sunlight Foundation, правозащитной организации, выступающей за открытость правительства, сказал, что он ожидает обострения дискуссий о публичных записях по мере того, как мессенджеры с возможностью шифрования сообщений завоевывают популярность. Он рассказал, что раньше для обхода законов о публичных документах чиновники использовали систему поэлементного обмена сообщениями от Blackberry и частные серверы электронной почты.

«Теперь появилось нечто новое, — сказал он о Telegram. — Эта тема активно обсуждается и входит в область наших интересов».

Испанские работодатели могут записывать на видео действия своих сотрудников

23 марта 2016, Испания, espanarusa.com. Конституционный суд Испании вынес постановление, согласно которому работодатели имеют право снимать на видео действия своих сотрудников на их рабочих местах для того, чтобы узнать, как они справляются со служебными обязанностями. Такое решение было принято в ответ на жалобу бывшей сотрудницы магазина Bershka в Леоне, которая в 2012 году была уволена с работы за кражу денег из кассы.

Обнаружив систематические недостачи, служба безопасности торговой точки разместила в помещении записывающее устройство, не оповестив об этом персонал, но вывесив на видном месте соответствующее предупреждение для посетителей. Видеозаписи и послужили документальным доказательством преступления, и после того, как подозреваемая забрала из кассы 187 евро, фирма расторгла с ней трудовое соглашение.

Конституционный суд признал, что действия работодателя не являются нарушением Закона о защите персональных данных, поскольку сбор и обработка этой информации были необходимы для наблюдения за выполнением условий контракта, подписанного обеими сторонами. Иначе говоря, руководители испанских компаний вправе вести съемку на видео действий своих сотрудников без оповещениях последних о целях, ради которых им приходится идти на такой шаг.

Трактовка казахстанских законов об «облаках» вызывает противоречия

25 марта 2016, Казахстан, digital.report. Светлое будущее, которое сулит использование облачных сервисов для хранения и передачи информации, может быть отсрочено из-за несостыковок в казахстанском законодательстве.

Об этом шла речь на круглом столе для юристов и специалистов по информационной безопасности, в рамках ИТ-конференции Profit Cloud Day, которая состоялась в Алматы 16 марта. Главной темой на повестке мероприятия стал вопрос о законности использования облачных хранилищ, расположенных за пределами Казахстана.

По словам старшего юриста Norton Rose Fulbright Жибек Айдымбековой, законодательство часто отстает от уровня развития технологий — и не только в Казахстане, где вопросы стали возникать после вступления в силу в начале текущего года поправок в Закон «О персональных данных». Новая редакция двух его статей — 12 и 16 — привела в замешательство некоторых игроков рынка.

В ней, в частности, говорится, что «… хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, которая хранится на территории Республики Казахстан». Тем самым, государство в императивном порядке установило место хранения персональных данных — Республика Казахстан.

После этого многие компании задались вопросом, законно ли теперь хранить данные на серверах расположенных за пределами Казахстана, какие из этих данных являются персональными, а какие нет, и касается ли вообще данная поправка хранения информации в «облаке», ведь, по сути, законодательство Казахстана не содержит термина «облачные технологии».

Многих представителей индустрии тревожит использование зарубежных публичных «облаков» . А именно, при размещении в облачных сервисах базы данных, часть которой состоит из конфиденциальной информации, по сути, происходит нарушение закона РК — к примеру, если в базе данных клиентов присутствуют их контактные данные, это уже считается персональной и конфиденциальной информацией.

По словам эксперта, теперь, при использовании облачных технологий, особое внимание следует уделять таким понятиям, как передача персональных данных и трансграничная передача данных. По закону, место хранения персональных данных должно физически располагаться в пределах Казахстана. В то же время, закон позволяет трансграничную передачу персональных данных, если страна, куда они передаются, предоставляет их защиту.

«Исходя из принципа нашего законодательства — «что не запрещено, то разрешено» — можно смело говорить, что, в целом, закон не ставит жестких ограничений на использование «облаков» для передачи и хранения данных», — говорит Айдымбекова. Исключение составляют данные с ограниченным доступом, которые находятся под защитой государства — госсекреты и персональные данные.

По словам юриста, теперь, прежде чем отправлять ту или иную информацию в облачное хранилище, центр обработки данных (ЦОД) которого расположен в другой стране, следует отталкиваться от прописанных в законе терминов. Очевидно, лучше всего при выборе облачного хранилища, предварительно выяснить его юрисдикцию, и предоставляет ли государство, законами которого руководствуется данный сервис, защиту персональных данных.

При этом, закон также оставляет возможность трансграничной передачи персональных данных на территорию государств, не обеспечивающих защиту персональных данных, но только при наличии соответствующего согласия субъекта (или законного представителя), а также в случаях, предусмотренных международными договорами, ратифицированными Казахстаном, предусмотренных законами, «если это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека и гражданина, здоровья и нравственности населения» или для «защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно».

Однако, при всем этом, в законе содержится бланкетно-отсылочная норма, которая может поставить в тупик всех, к кому он относится. В статье, посвященной трансграничной передаче персональных данных, последним пунктом стоит следующая формулировка: «Трансграничная передача персональных данных на территорию иностранных государств может быть запрещена или ограничена законами Республики Казахстан». Какими именно законами и на каком основании могут быть введены такие ограничения, остается неясным.

Аналогичный закон в России, принятый больше года назад, содержит более жесткие требования. Ограничения коснулись не только хранения информации, но и сбора, записи, систематизации, аккумулирования, исправления и выборки данных, которые должны производиться только в базах данных, расположенных на территории РФ.

Директор по юридическим вопросам Microsoft в Центральной и Восточной Европе Ребекка Радлофф говорит, что ни в одной стране мира нет ясных и четких законов по сфере облачных вычислений — и ситуация правовой неопределенности в Казахстане неуникальна. По ее словам, перед Microsoft, являющейся провайдером облачных услуг, стоит задача формировать восприятие того, что будет обозначать законодательство для сектора.

Также в законе говорится о недопустимости нахождения персональных данных за пределами страны, если они одновременно не хранятся в базе данных в Казахстане. Таким образом, заметила старший юрист Norton Rose Fulbright, ограничений на параллельное хранение персональных данных в резервной копии, размещенной в облачном хранилище другой страны, нет.

Резюмируя встречу, участники выразили надежду на то, что регулятор в ближайшее время разъяснит вопросы использования персональных данных в облачных сервисах. «Законы принимаются, а инструкций о том, как ими пользоваться, порой приходится ждать годами — в таких условиях нам приходится попросту “импровизировать”», — посетовала Жибек Айдымбекова.

Напомним также, что согласно новым Правилам регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента интернета, введенным с 21 марта текущего года, пользование доменным именем в пространстве .kz может быть приостановлено в случае «нахождения аппаратно-программного комплекса, на котором размещается интернет-ресурс, за пределами территории Республики Казахстан».

В прежней редакции Правил говорилось о недопустимости размещения только серверного оборудования за пределами страны. Новый документ налагает ограничения не только на «железо», но и на «софт», отмечают специалисты — впрочем, затрудняясь однозначно сказать, что именно это означает для собственников и администраторов интернет-ресурсов.

Trend Micro: в 2015 году здравоохранение вышло на первое место по количеству утечек и краж данных

30 марта 2016, США, ria-ami.ru. Компания Trend Micro Incorporated (TYO: 4704; TSE: 4704), мировой лидер в разработке решений для информационной безопасности, опубликовала отчет с анализом наиболее значительных инцидентов в области информационной безопасности за 2015 год «Изменение ландшафта угроз задает новые стандарты стратегий защиты» (Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies).

Согласно результатам данного исследования, в 2015 году на отрасль здравоохранения пришлось самое большое число инцидентов (26,9%), в ходе которых были украдены или оказались под угрозой цифровые данные пациентов. На втором и третьем месте оказались образование и госсектор. Различные инциденты с медицинскими данными затронули данные более 90 млн человек.

В отчете приводятся наиболее значительные инциденты с медицинскими данными за 2015 год:

- В феврале компания Anthem, второй по величине провайдер медицинского страхования США, объявила о целенаправленной атаке, в ходе которой оказались затронуты данные 80 млн ее клиентов и сотрудников.

- В марте крупнейший медицинский провайдер Аляски компания Premera Blue Cross пострадала от инцидента, затронувшего данные 11 млн человек.

- В мае сразу две крупные организации здравоохранения объявили об инцидентах с данными. В начале месяца в ходе кибератаки на больничную сеть Калифорнийского университета (UCLA Health) в Лос-Анджелесе были скомпрометированы данные о 4,5 миллионах ее клиентах. В конце мая федерация компаний, предоставляющих услуги медицинского страхования, CareFirst BlueCross BlueShield объявила, что стала жертвой кибератаки, в результате которой были затронуты данные 1,1 млн текущих и бывших клиентов компании.

- В сентябре 2015 года кибератаке подверглось американское агентство по медицинскому страхованию Excellus BlueCross BlueShield (BCBS), в результате чего были скомпрометированы данные более 10 млн человек. В этом же месяце провайдер облачных решений по работе с клиентами Systema Software объявил о том, что в результате несанкционированного доступа к его системе хранения данных, была затронута медицинская информация 1,5 млн человек.

Информация, которая была скомпроментирована в ходе различных инцидентов, включала в себя персональные данные, номера социального страхования, финансовые данные и медицинские записи. Эта информация потенциально может быть использована злоумышленниками для мошенничества, шантажа и других преступлений, связанных с незаконным использованием чужих персональных данных для получения материальной выгоды.

Несмотря на то, что в течение 2015 года активность киберпреступников в отношении медицинских организаций заметно повысилась, здравоохранение пока еще не входит в число отраслей, активно применяющих самые современные методы информационной безопасности.

Организациям здравоохранения необходимо внедрять передовые методы защиты информации на всех уровнях, включая защиту медицинских порталов и баз данных, обнаружение утечек, целенаправленных атак и защиту конечных устройств.

Видеорегистраторы в такси тайно снимают пассажиров

31 марта 2016, Эстония, rus.postimees.ee. Все чаще в такси устанавливают бортовые видеокамеры, которые фиксируют не только то, что происходит на дороге, но и пассажиров. Если видеорегистратор снимает пассажиров, в салоне должна быть установлена соответствующая табличка.

Корреспондент Tartu Postimees столкнулся с тем, что в такси фирмы Vatex Takso был установлен видеорегистратор с двумя камерами – одна предназначена для съемки дороги, другая направлена в салон автомобиля. Видеорегистратор был укреплен на лобовом стекле, но в салоне не было объявления о том, что одна из камер снимает пассажиров.

Как объяснил таксист, видеорегистратор он использует в целях собственной безопасности, и в Тарту такие же видеорегистраторы с двумя камерами установлены, по меньшей мере, в двадцати такси.

Следует оповещать

«Каждый третий водитель такси использует такие видеокамеры», – заявил таксист. Глава фирмы Vatex Takso Индрек Уус подтвердил, что, насколько ему известно, двое таксистов из его фирмы используют видеорегистраторы с двумя камерами исключительно в целях безопасности. «После инцидента с одним из клиентов таксист установил видеокамеру, чтобы в случае необходимости можно было что-то доказать. Данные записываются на карту памяти. Мы никогда не проверяли эти записи», – сказал Уус, отметив, что все больше таксистов используют видеорегистраторы с двумя камерами.

«После трагического случая в Пярну таксисты стали ставить видеорегистраторы так, чтобы камера снимала салон, – сказал Уус. – В Таллинне такая же ситуация, там видеорегистраторы ставят еще активнее. Камера начинает работать, когда включается таксометр. Никто даже не обращает внимания».

Руководитель Tartu Taksopark Куно Когер, по его словам, не в курсе, что таксисты снимают на камеру видеорегистратора пассажиров.

«Мне известно, что снимают происходящее на дороге, но я не слышал, чтобы таксисты снимали пассажиров. Это возможно только по предварительной договоренности. Наша фирма не устанавливала видеорегистраторы, но я не могу исключать, что кто-то из таксистов сделал это самостоятельно», – сказал Когер, предположив, что недавние события в Европе тоже могли подтолкнуть водителей такси к тому, чтобы установить видеорегистратор.

Как сказала представитель Инспекции по защите данных Кая Пуусепп, Закон о защите персональных данных разрешает использовать камеры для защиты лиц и имущества. В том числе бортовые видеокамеры, но другие лица должны быть оповещены об этом. Если в такси установлен видеорегистратор с камерой, направленной в салон, то на видном месте должен быть значок с символом камеры.

«Наклейка обязательно должна быть, в противном случае это рассматривается как нарушение закона, – сказала Пуусепп, по словам которой инспекция не считает отсутствие соответствующей наклейки серьезным нарушением. – Как правило, мы ограничиваемся предупреждением. Все, кого мы оповестили, наклеили стикеры со значком камеры. Несколько лет назад такое же требование мы предъявили гостиницам».

Более серьезной, чем отсутствие в салоне стикера со значком камеры, Пуусепп считает другую проблему, а именно, как могут быть использованы записи. По ее словам, сейчас пассажир такси не может быть уверен в том, что видеокадры, на которых он запечатлен, не появятся в социальных сетях.

Нет гарантии

«Никто не проверяет, что делают таксисты с этими записями. Надежда только на то, что они не станут злоупотреблять ими. Но в любом случае пассажиры должны знать, что их снимает камера видеорегистратора, этого требует закон», – сказала Пуусепп.

IT-Security Conference 2016: подводим итоги

01 апреля 2016, Беларусь, news.tut.by. 29-30 марта в Минске состоялась 2-я Конференция «Технологии защиты информации и информационная безопасность организаций» (IT-Security Conference 2016).

Инновационная площадка, созданная Академией управления при Президенте Республики Беларусь и Ассоциацией «Инфопарк», собрала почти 350 ведущих специалистов в сфере защиты информации и информационной безопасности более чем из 130 организаций Беларуси и России.

Участники обсудили наиболее актуальные вопросы, связанные с использованием мобильных приложений, Big Data, Cloud Computing, сервисами ЦОД, Open Data, технологиями Blockchain. Наибольший интерес и много вопросов вызвали выступления, связанные с внедрением и функционированием Государственной системы управления открытыми ключами (ГосСУОК), а также с текущим состоянием и перспективами развития сертификации продуктов и аттестации систем защиты информации в Беларуси.

Эксперт в области управления ИТ-рисками Кирилл Домнич и в этом году представил результаты международного исследования EY по информационной безопасности и подробнее остановился на результатах для Беларуси. Одним из интересных фактов стало то, что 59% организаций из Беларуси, принявших участие в международном исследовании EY, имеют стратегию обеспечения информационной безопасности, утвержденную высшим руководством, но лишь у 12% организаций запланированы ключевые мероприятия по реализации стратегии ИБ на следующие 12 месяцев.

Живой интерес вызвала панельная дискуссия «Полковник никому не нужен…или новые ожидания от информации», организованная российским гостем Олегом Седовым, главным редактор журнала BISA. Участники обсуждения – представители государственного регулятора (ОАЦ), белорусского и российского ИТ-бизнеса попытались, опираясь на личный опыт, проанализировать, как же изменилось значение информации в связи с приходом в нашу повседневность современных цифровых технологий.

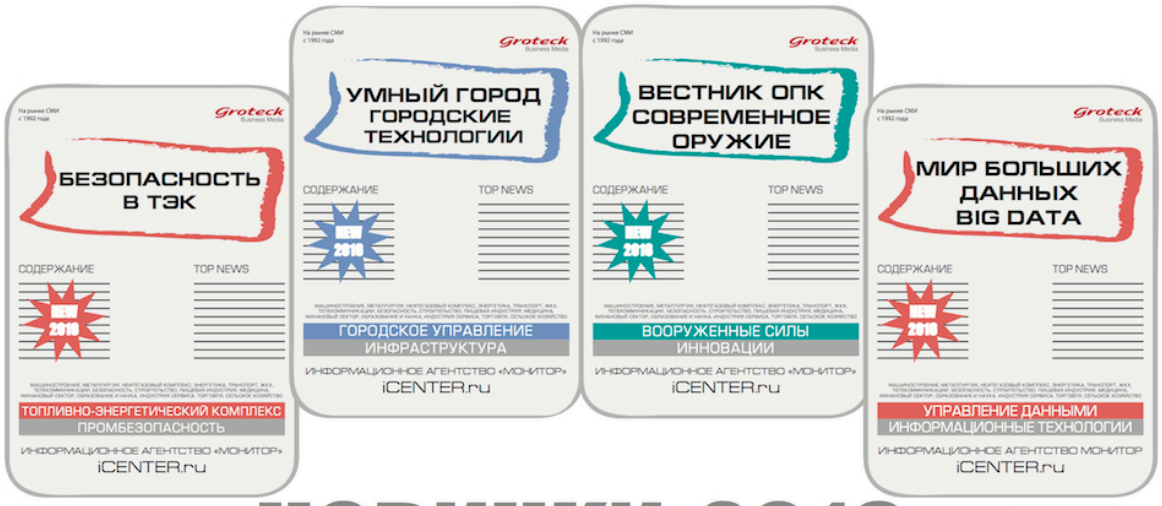
Николай Колоша из ОИПИ НАН Беларуси в ходе семинара по защите персональных данных, на примере эстонской системы интернет-голосования i-Voting объяснил, при помощи каких мер можно снизить организационные и технические риски, а также рассказал про верификацию голосов на разных уровнях.

Второй день IT-Security Conference также представил насыщенную программу, вобравшую в себя вопросы криптографической защиты, ГосСУОК, кибербезопасности, технологий Blockchain и криптовалют.

Технологии Blockchain и криптовалют подробнее обсудили на отдельном семинаре по одноименной теме. Владимир Комисаренко, модератор семинара и эксперт в данной области, рассказал, в чем вся «соль» цифровых наличных денег (digital cash), как они работают, об угрозах, атаках, моделях нарушителя.

Заинтересовал слушателей и мастер-класс по внедрению системы управления информационной безопасностью (СУИБ) – несмотря на усталость в конце второго дня Конференции, участники с удовольствием пообщались с Алексеем Евменковым.

Отзывы участников подтверждают слова Владимира Анищенко, председателя Комитета по ИБ Ассоциации «Инфопарк»: «Особенность конференции – как раз и заключается в том, что она становится местом открытой профессиональной дискуссии между представителями собственников информационных систем, на плечах которых лежит ответственность за защиту информации, с одной стороны, и представителями регулятора с разъяснением его требований и представлением рекомендаций, а также поставщиков ИТ – с их решениями в области защиты информации, с другой стороны».



НОВИНКИ-2016

Выход с 01.01.2016

Выход с 01.07.2016

ЕЖЕМЕСЯЧНЫЙ ОТРАСЛЕВОЙ МОНИТОРИНГ
БОЛЕЕ 60 ТЕМАТИЧЕСКИХ ИЗДАНИЙ
ПОМОГУТ СПЕЦИАЛИСТАМ:

Выявить Вызовы, Угрозы и Риски
ОпределитьТочки Развития
Прогнозировать Темпы Развития
Оценить Деловую Репутацию Партнеров
Принять Взвешенное Решение

iCenter.Ru

13 АПРЕЛЯ 2000

В Канаде вышел закон по защите персональных данных PIPED Act (PIPEDA)

Самое личное о данных... ИА "Монитор"

НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ * ТРЕНДЫ * ЭКСПЕРТИЗА

ТРЕНДЫ * ЭКСПЕРТИЗА * НОВИНКИ * ОБЗОРЫ

НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ

ИСТОРИЧЕСКИЙ КАЛЕНДАРЬ:

Подробнее об «Историческом календаре»
на сайте http://2016.icenter.ru/2

ТРЕНДЫ * ЭКСПЕРТИЗА * НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ

Периодичность выхода	Ежемесячно
Учредитель	ООО «Гротек»
Генеральный директор	Андрей Мирошкин
Издатель	Информационное агентство «Монитор»
Руководитель агентства	Татьяна Никонова
Свидетельство о регистрации	СМИ ИА № 77-1095
Тираж	Менее 1000 экз.

Подписка по каталогам в отделениях Почты России:

Газеты и журналы индекс **47345**
Пресса России индекс **38580**
Почта России индекс **99115**

Почта: 123007, Москва, а/я 82
Телефон: (495) 647-0442 Факс: (495) 221-0862
Подписка: monitor@groteck.ru www.icenter.ru
Редакционное сотрудничество: monitor@groteck.ru

iCenter.Ru