Керим Даев
магистрант,
Московский государственный университет им. М.В. Ломоносова
(г. Москва, Россия);
бизнес-аналитик ПАО Сбербанк (г. Москва, Россия)
(e-mail: Kerim.daev@icloud.com)

ОПАСНОСТИ И РИСКИ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Успешная деятельность любой компании зависит от ее отношения к персональным данным, с которыми осуществляется работа. Нарушение системы защиты персональных данных может привести к непоправимым последствиям. В статье описаны основные опасности и риски утечки персональных данных как для их собственников, так и для компаний, а также даны рекомендации по работе с персональными данными.

Ключевые слова: персональные данные, утечка данных, защита персональных данных, риски утечки персональных данных.

DOI: 10.31857/S020736760019880-7

С момента широкого распространения цифровых технологий во всем мире мы живем в период, когда персональные данные занимают чрезвычайно важное место в деятельности компаний. При этом рост цифровой активности в сочетании с пристрастием к новым технологиям и увеличением объема данных, хранящихся в виртуальной среде, поставил вопрос об утечке и конфиденциальности личных данных. Однако эти данные, которые маркетологи считают ценнейшим ресурсом, сложно защитить. Многие компании признают, что испытывают трудности с их надлежащей защитой, а недавнее исследование *Dell* под названием «*Global Data Protection Index*» показывает, что «27% компаний не смогли восстановить свои данные с помощью своего решения для защиты» [3].

Любая информация, относящаяся к физическому лицу, идентифицированному или идентифицируемому, является персональными данными. Человек может быть идентифицирован:

– напрямую: например, по фамилии и имени;

– косвенно: по идентификатору (номер клиента, номер телефона, номер социального страхования), биометрическим данным или элементам, характерным для их физической или генетической идентичности и т.д.

Данные лежат в основе трансформации бизнеса, и их безопасность очень важна для сохранения текущих процессов и развития новых. Если данные в исходном состоянии имеют ограниченную ценность, то их преобразование

Статья подготовлена под научным руководством доктора экономических наук, профессора кафедры политической экономии экономического факультета Московского государственного университета им. М.В. Ломоносова **Молчанова И.Н.**

позволяет провести анализ и достичь целей компании оптимальным путем. Потенциал данных раскрывается, когда они используются для перепроектирования существующих процессов или для определения новых.

Для компании защита персональных данных – это не только соблюдение Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (далее – Закон о персональных данных) [1], но и защита нематериальных активов. Этот актив состоит из информации о собственных сотрудниках, а также о клиентах. Эти данные стали орудием конкурентной борьбы, особенно в области электронной коммерции. Но, помимо риска потери важных данных, отсутствие безопасности персональных данных также подвергает компании риску судебного разбирательства.

Это касается как злонамеренных атак, так и случайных действий, включая неосторожность. Таким образом, с точки зрения уровней риска и типов нарушений, существует несколько типологий. В документации, существующей по этой теме, выделяются три типологии: (1) нарушение конфиденциальности, что является наиболее распространенным. Оно состоит из несанкционированного или случайного раскрытого доступа к персональным данным. Например, потеря USB-ключа, на котором появляются личные данные, или злонамеренный доступ к информационной системе, плохая конфигурация, позволяющая при взаимодействии с URL-адресом получить доступ к конфиденциальным данным; отправка данных не тому получателю; (2) нарушение целостности: несанкционированное или случайное изменение персональных данных. Выявлен случай, когда ученик, войдя в информационную систему, изменил свои оценки; (3) доступность: случайное или несанкционированное уничтожение или потеря персональных данных.

В то время как некоторые поломки могут быть устранены непосредственно внутри компании, другие требуют вмешательства специализированных поставщиков услуг. Вирус или вредоносное программное обеспечение (ПО) также могут привести к потере данных.

Прежде чем обеспечить безопасность персональных данных, которыми владеет компания, она обязана их квалифицировать, а затем количественно оценить. Процесс квалифицирования персональных данных предполагает их инвентаризацию. Для обычной компании это, как правило, данные, касающиеся сотрудников, клиентов, поставщиков. Это имена, контакты и многое другое, включая отзывы. Нередко компании используют так называемые «конфиденциальные» данные, то есть те, которые могут прямо или косвенно раскрыть этническое или расовое происхождение, политические, философские, религиозные взгляды, членство отдельных лиц в профсоюзах или касаются их здоровья, что требует особых мер предосторожности.

Количественная оценка, которую легче выполнить, представляет интерес только для технического управления этими данными.

После проведения инвентаризации сохраненных персональных данных рекомендуется удостовериться в том, что хранение этих данных осуществляется безопасным образом.

Озабоченность безопасным хранением персональных данных связана не только с их ценностью, но, прежде всего, с юридическим императивом, предусмотренным ст. 19 Закона о персональных данных. Эта статья предполагает, что «оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных» [1]. Таким образом, защита персональных данных будет соответствовать двум требованиям: 1) гарантировать, что эти данные не могут быть повреждены; 2) ограничить доступ к ним только уполномоченными лицами.

Компании должны принять необходимые меры для обеспечения того, чтобы хранящиеся персональные данные не могли быть изменены. Эти меры предосторожности предназначены для защиты персональных данных от искажения или повреждения, преднамеренного или непреднамеренного. Помимо достаточной защиты персональных данных, последние не должны быть никому доступны.

Доступ к различным категориям данных должен быть предоставлен только тем службам, которым они требуются для выполнения рабочих задач. Так, например, сотрудникам отдела кадров не нужны данные о клиентах, и поэтому они не должны иметь к ним доступа. И наоборот, отдел продаж должен иметь доступ к данным о клиентах, но не к данным о персонале компании.

Именно для того, чтобы определить, кто и к какому типу данных должен иметь доступ, необходимо проводить инвентаризацию этих данных. Ограничение доступа только к релевантным персональным данным требует установления строгой политики управления. Эта политика предполагает выделение ролей и назначение уникального идентификатора каждому лицу, которому необходимо получить доступ к персональным данным; такому лицу также должен предоставляться пароль, достаточно надежный, чтобы его нельзя было взломать. Взаимодействие должно завершаться путем блокировки сеансов учетных записей пользователей после кратковременного бездействия. Необходимо также запланировать регулярную смену паролей.

В дополнение к риску потери такого важного актива, как персональные данные, несоблюдение правил безопасности несет для компании риски других существенных потерь.

Компании, управляющие файлами персональных данных (в частности, интернет-магазины, сервисные компании, медицинские работники), должны проявлять особую бдительность и принимать необходимые превентивные меры для

обеспечения безопасности обработки персональных данных, особенно конфиденциальных личных данных. В случае нарушения конфиденциальности корпоративная социальная ответственность компании может быть поставлена под сомнение.

Возможными последствиями для заинтересованных лиц, риск которых должен быть оценен, могут быть, в частности, потеря контроля над своими личными данными, ограничение их прав, риск дискриминации, кражи личных данных, финансовые потери, несанкционированная отмена процедуры псевдонимизации, ущерб репутации или утрата конфиденциальности (включая, например, нарушение профессиональной тайны) или значительный экономический или социальный ущерб.

Основными рисками для компаний являются необратимая потеря данных, финансовый и репутационный ущерб. Утечка персональных данных может не только поставить под сомнение гражданско-правовую ответственность, но и нанести серьезный удар по имиджу компании. Такая небрежность может навсегда подорвать ее репутацию в глазах реальных и потенциальных клиентов.

Плохое управление данными может иметь также серьезные финансовые последствия для организации. Обычно компании, пострадавшие от утечек данных, несут финансовые потери в следующих областях: падение цены акций, снижение оборота, потеря клиентов, потеря конкурентоспособности, штрафы, затраты на кампанию по восстановлению репутации. Значительная потеря оборота и серьезный экономический ущерб вследствие утечки персональных данных повышают риск дефолта и могут привести к полному прекращению деятельности компании.

Одни компании теряют прибыль на том, что украденная информация попадает в руки конкурентов, а те отбирают часть рынка; у других бизнес-субъектов падает стоимость активов. Вдобавок к этому, утечка данных может вылиться в штрафы и выплаты компенсаций пользователям, которые пострадали из-за утечки. Любое лицо, понесшее материальный ущерб, финансовые убытки и/или моральный ущерб в результате утечки его персональных данных (сотрудники, клиенты и т.д.), может потребовать компенсации в рамках своей гражданской ответственности. Эти суммы могут достигать огромных размеров. Например, в 2019 году *Equifax* заплатили не менее 575 млн долларов [4].

Оценка риска имеет центральное значение, поскольку уровень риска определяет действия, которые должны быть предприняты в результате нарушения. Способность оператора данных выявлять утечку персональных данных и оценивать риски, которые она создает для заинтересованных лиц, имеет важное значение, поэтому необходимо заранее внедрить процедуру управления утечкой данных.

Итак, необходимо уделять много внимания безопасности и проводить анализ рисков; организационные меры должны включать повышение осведомленности персонала компании по вопросам защиты и безопасности данных; формализации процедур, проведению тестов, аудита безопасности. Кроме того,

компании могут обращаться к определенному специализированному программному обеспечению или сервисам, позволяющим выявлять инциденты безопасности или выявлять утечки информации в Интернете и в «даркнете», где развиваются соответствующие рынки. Учреждения должны обеспечивать безопасность, обучать свой персонал, проверять свои системы и обучать своих сотрудников противодействию атакам на определенных векторах. Планы действий должны разрабатываться до, во время и после утечки данных.

При этом важно учитывать, что создание сильного чувства безопасности повышает лояльность и доверие клиентов. Клиенты ценят безопасность данных при покупке продуктов и услуг для предотвращения кражи данных, сокращения обмена личными данными, лучшего управления безопасностью данных и большего внимания к потребителю.

Литература

1. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (ред. От 02.07.2021) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.
2. *Дадалко В.А., Тимофеев Е.А.* Основы формирования комплаенс-контроля в области системы обеспечения безопасности персональных данных // Национальные интересы: приоритеты и безопасность. 2020. № 2. С. 339-350.
3. Dell Technologies Global Data Protection Index // URL: https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm
4. Equifax обязали выплатить несколько миллионов долларов из-за утечки данных // URL: https://securenews.ru/equifax-ordered-to-pay-several-million-dollars-due-to-data-breach/

Kerim Daev (e-mail: Kerim.daev@icloud.com)
Master's Degree student,
Lomonosov Moscow State University (Moscow, Russia);
Business analyst PJSC Sberbank (Moscow, Russia)

DANGERS AND RISKS OF PERSONAL DATA LOSS

The success of a company depends in many ways on its attitude to the personal data being handled. A failure in the personal data protection system can lead to irreparable consequences. The article describes the main dangers and risks of personal data loss, both for individuals and for companies, and provides recommendations for employees dealing with clients' personal data.

Keywords: personal data, data loss, personal data protection, risks of personal data loss.

DOI: 10.31857/S020736760019880-7

The article was prepared under the supervision of Doctor of Economics, Professor of the Department of Political Economy, Faculty of Economics, Lomonosov Moscow State University **Molchanov I.N.**