УДК 004.056.53

ПРОБЛЕМАТИКА ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В БОЛЬШИХ КОМПАНИЯХ

© 2022 Н. О. Лохина

студентка, направление подготовки Информационная безопасность
e-mail: natasha.lohina@gmail.com

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет»

В статье проанализированы произошедшие утечки информации в двух крупных компаниях, приведена статистика и предложено решение для увеличения степени защиты конфиденциальной информации.

Ключевые слова: информационная безопасность, конфиденциальная информация, персональные данные, защита информации, утечка информации.

PROBLEMS OF LEGAL SUPPORT FOR THE PROTECTION OF CONFIDENTIAL INFORMATION IN LARGE COMPANIES

© 2022 N. O. Lokhina

Student of the Direction of training Information Security
e-mail: natasha.lohina@gmail.com

Federal State Budgetary Educational Institution of Higher Education "MIREA – Russian Technological University"

The article analyzes the information leaks that have occurred in two large companies, provides statistics and suggests a solution to increase the degree of protection of confidential information.

Keywords: Information security, confidential information, personal data, information protection, information leakage.

Почти любая компания в настоящий момент прикладывает огромное количество усилий для цифровизации своей отрасли. Медицинские организации, компании, предоставляющие покупку товаров и услуг, банковский сектор – все отрасли переводят хранение данных и обслуживание клиентов в электронный формат. Это напрямую связано с увеличением количества клиентов компании, так как цифровая трансформация предоставляет пользователю удобство и комфорт при выборе услуг и товаров.

При использовании сервисов крупных компаний среднестатистический человек не задумывается о сохранности своих персональных данных, так как если компания крупная, значит стабильная и ей можно доверять. Персональными данными являются фамилия, имя, отчество, мобильный телефон – и это далеко не полный список.

В феврале 2022 г. появилась информация о свободном размещении в сети Интернет базы данных компании ООО «Яндекс.Еда» [1], насчитывающая 6 миллионов 882 тысячи 230 уникальных номеров телефона людей из стран СНГ. Со слов

представителей компании, утечка произошла из-за халатности сотрудника, имевшего доступ к данным. Также в апреле 2022 г. появилась информация о более масштабной утечке персональных данных компании ООО «Лаборатория Гемотест» [2], которая насчитывает около 30 миллионов персональных данных клиентов медицинской организации. Причины утечки не были озвучены компанией, но о наличии хакерских атак не упоминается, из чего можно сделать вывод, что утечка могла произойти по вине сотрудников самой компании.

На основании вышесказанного можно утверждать, что необходимо преобразовать правовое обеспечение защиты конфиденциальной информации и персональных данных в больших компаниях Российской Федерации. В данной статье проанализируем произошедшие утечки информации в двух крупных компаниях, посмотрим на статистику и попробуем предложить решение для увеличения степени защиты конфиденциальной информации.

Рассматриваемые в данной статье компании ООО «Яндекс.Еда» и ООО «Лаборатория Гемотест» принадлежат отрасли предоставления услуг (доставка еды и медицинские услуги соответственно). Для начала углубимся в терминологию. Разберем отличия конфиденциальной информации от персональных данных. В Российской Федерации в 152-ФЗ [3] под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В 149-ФЗ [4] определено понятие конфиденциальной информации как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Защитой данных внутри компании занимаются департаменты информационной безопасности, составляя политику безопасности организации. Политикой безопасности принято считать совокупность мер, процедур, практических методов и руководящих принципов в области информационной безопасности, используемых организациями в своей деятельности.

В случаях, рассмотренных в данной статье, подразумевается нарушение компаниями ч. 1 ст. 31.11 КоАП РФ, по которой ООО «Яндекс.Еда» уже получила максимальный штраф по этой статье в размере 60 тысяч рублей, а компания ООО «Гемотест» проходит проверку на соответствие информации об утечке персональных данных регулирующим органом «Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций». Роскомнадзор [5] занимается обеспечением выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

Компания ООО «Яндекс.Еда» публично извинилась перед пострадавшей стороной и признала, что утечка произошла из-за недобросовестной и халатной работы одного из сотрудников, имевшего доступ к персональным данным, а именно: к истории заказов (адрес места доставки с указанием города, улицы, номера дома, подъезда, этажа и квартиры) и информации из личного кабинета (ФИО, номера телефонов, адрес электронной почты). Эта ситуация побудила компанию провести внутреннюю масштабную проверку и ужесточить подход к хранению такой информации. Учитывая, что утечка не коснулась данных платежной системы, логинов и паролей пользователей, компания решила обеспечить уровень защиты персональный информации наряду с сопоставимыми данными, а также исключить ручную обработку таких данных и сократить до минимума число сотрудников, которые имеют доступ к персональным данным.

Компания ООО «Лаборатория Гемотест» публично призналась о факте утечки данных и пошла по тому же пути, что и компания ООО «Яндекс.Еда», – проведение внутренней проверки и ужесточение мер защиты информации внутри компании.

Каждый год федеральным аппаратом Роскомнадзор выявляются и расследуются утечки данных больших компаний. Таким образом, в период 2020–2021 гг. были выявлены более 100 миллионов конфиденциальных данных, попавших в свободное размещение в сети Интернет. По данным экспертного аналитического центра «InfoWatch» [6], являющейся ведущим российским разработчиком решений для обеспечения информационной безопасности организаций, статистика утечек информации в этот период выглядит так:

- за 2020 г. в Российской Федерации было зарегистрировано на 2,2 % больше утечек данных, чем в 2019 г.;
- за 2020–2021 гг. выявлено более 100 миллионов персональных данных и платежной информации граждан страны, попавших в свободный доступ;
- в мировом распределении утечек персональных данных доля Российской Федерации составляет почти 17 %;
- самыми незащищенными сферами деятельности в Российской Федерации являются сфера высоких технологий и финансовый сектор – там было зарегистрировано более 40 % утечек персональных данных;
- почти 80 % утечек персональных данных произошло в результате умышленных и халатных действий сотрудников компаний. К примеру, доля таких случаев в 2019 г. составляла 38,7 %.

Можно сделать вывод, что количество утечек растет преимущественно по вине сотрудников компании и процент опубликованной информации растет с каждым годом.

Юридические меры, применяемые к большим компаниям при осуществленной угрозы распространения персональных данных (административное нарушение), не создают для компании большой риск потерять часть прибыли за год, но определенно могут вызвать потерю репутации и доверия клиентов, что ведет к снижению числа потребителей товаров и услуг больших компаний. Таким образом, из-за утечки данных компании теряют не только денежные средства в момент судебного постановления, но и перспективу зарабатывать то же количество прибыли, что и раньше, из-за снижения доверия клиентов.

Совокупность проблем с защитой персональных данных и конфиденциальной информации можно разделить на три основные проблемы:

1) нормативно-правовые акты не подразумевают серьезного наказания для утечек персональных данных;
2) в российских компаниях недостаточно проработана политика безопасности и руководство по работе с персональными данными, что ведет к краже и утечке персональных данных;
3) из-за большого количества сотрудников внутренним департаментам безопасности тяжело отследить и выявить конкретного нарушителя.

Отталкиваясь от всего вышесказанного, можно сделать выводы о том, какие основные моменты помогут повысить уровень защиты конфиденциальной информации в больших компаниях:

- корректировка законов и нормативно-правовых актов на государственном уровне в сфере защиты конфиденциальной информации;
- проработка и ужесточение мер безопасности при работе сотрудников внутри компании с конфиденциальной информацией;
- снижение количества сотрудников, имеющих доступ к конфиденциальной информации;
- ужесточение наказания за невыполнение требований политики безопасности организации;

- документирование и отслеживание поведения сотрудников, имеющих доступ к конфиденциальным данным для быстрого выявления и урегулирования проблем департаментами безопасности внутри компании.

В заключение акцентируем внимание на рассматриваемых проблемах в данной статье. Стремительная цифровая трансформация всех сфер и отраслей экономики прямо пропорционально связана с желанием злоумышленников похитить с конфиденциальную информацию и осуществлять с нею манипуляции. При достаточно низком пороге входа в организацию сотрудник получает доступ к персональным данным и конфиденциальной информации, что может натолкнуть его на мысль о краже и последующей продаже данной информации с целью получения собственной выгоды. При этом расследования могут не вывести департамент безопасности организации и Роскомнадзор на конкретного виновного человека, что усугубляет проблему и увеличивает количество утечек информации. Нет сомнений, что в будущем все сферы деятельности будут перенесены в цифровой формат для удобства и быстроты использования. Поэтому сейчас необходимо придумать решения о защите конфиденциальной информации граждан страны, например путями, описанными в данной статье, чтобы упорядочить и заложить фундамент для дальнейшего развития безопасного хранения персональных данных и конфиденциальной информации.

(дата обращения: 13.05.2022).

---

1. Официальный сайт «Яндекс.Еда» [Электронный ресурс]. – URL: https://eda.yandex.ru/moscow?shippingType=delivery (дата обращения: 13.05.2022).
2. Официальный сайт «Лаборатория Гемотест» [Электронный ресурс]. – URL: https://gemotest.ru/ (дата обращения: 13.05.2022).
3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 13.05.2022).
4. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.05.2022).
5. Официальный сайт «Роскомнадзор» [Электронный ресурс]. – URL: https://rkn.gov.ru/ (дата обращения: 13.05.2022).
6. Аналитические отчеты с официального сайта «InfoWatch» [Электронный ресурс]. – URL: https://www.infowatch.ru/analytics/analitika (дата обращения: 13.05.2022).