

Секция «10. Современное российское общество: политическое, социальное и культурное измерение»

Социальные последствия утечки информации в госучреждениях России.

Тимохина Ж.А.¹, Краснослободцева М.В.²

*1 - Финансовый университет при Правительстве РФ, Факультет государственного управления, 2 - Финансовый университет при Правительстве РФ, Факультет государственного управления, Москва, Россия
E-mail: Kirillovazhanna@mail.ru*

Утечки информации – это случайные потери или намеренное хищение информации, представляющей собой персональные данные граждан, важную информацию для бизнеса (коммерческая тайна) или государства (государственная тайна). Как видно из определения, утечки информации несут в себе серьезные угрозы, как для коммерческой деятельности, так и для общества в целом.

Информационная безопасность – это главная проблема и задача современного мира. Так как эффективность бизнеса и безопасность общества зависит от сохранения конфиденциальности, целостности и доступности информации.

Принято разделять утечки информации на умышленную, неумышленную и информацию, в которой невозможно определить природу утечки, когда не возможно определить был умысел или это произошло случайно (например, потеря мобильных носителей – смартфоны, ноутбуки, планшеты, флешки). Процентное соотношения этих видов утечки информации разнятся по странам мира, что касается России, то умышленная утечка информации составляют около 77% всех утечек информации, когда доля таких утечек в мире – 46%.

Происходит утечка информации через следующие каналы : Веб-каналы сети Интернет, атаки со стороны злоумышленников, потери съемных носителей и внутренние утечки информации за счет сотрудников организации. Часто сотрудники сами не осознают, что разглашают корпоративную или государственную конфиденциальную информацию. Например, при разговоре со знакомыми или родственниками, при пользовании портативных и мобильных устройств, принадлежащих организации совместно с посторонними людьми, при пользовании корпоративной почтой и Интернета в личных целях, а также вынос за пределы организации бумажных и электронных носителей информации.

По данным отчета аналитического центра InfoWatch за 2012 год было скомпрометировано более 1,8 млрд. записей. В СМИ было обнародовано 934 случая утечки конфиденциальной информации, что на 16% превышает данные 2011 года.

Россия заняла третье место по количеству случаев утечки информации в 2012 году, обогнав Канаду. Как уже было сказано, в СМИ за 2012 год было зафиксировано 934 случая утечки информации, из них в России – 74 случая.

На сегодняшний день случаи утечек растут в государственном секторе. По данным Zecurion Analytics в 2012 году в России значительно изменился отраслевой профиль утечек. Следует отметить, что в настоящее время из общего числа утечек лидирующие места занимают образование (20,1%) и госорганизации (16,9%).

Доля утечек в государственном секторе уже на протяжении многих лет держится на стабильно высоком уровне, чаще всего утечки случаются из-за халатного отноше-

ния сотрудников госорганизаций. Рассмотрим примеры самых громких случаев утечек информации в госорганизациях за 2012-2013 года.

Например, в апреле 2012 года близ Казани инспекторы Центрального территориального управления министерства экологии обнаружили несанкционированную свалку. Среди мусора оказались и личные дела военнослужащих расквартированной неподалёку воинской части МВД специального назначения. Её бойцы — участники контртеррористических операций на Северном Кавказе. Никаких претензий в части раскрытия персональных данных инспекторы военным не предъявили, зато пообещали привлечь к ответственности за загрязнение окружающей среды.

Еще один случай произошел в декабре 2012 года. На сайте Следственного комитета России в открытом доступе появились тексты обращений граждан через интернет-приёмную. Всего около 30 тыс. сообщений, оставленных за 2,5 года, оказалось в разделе «Новости». Наиболее вероятные причины инцидента — ошибки при разработке сайта или халатность обслуживающих его технических специалистов.

Как мы видим, исходя из приведенных выше примеров, в госорганизациях преобладает неумышленная утечка информации, связанная с халатностью работников. Следует отметить, что самый главный ущерб от обнародования персональных данных, конечно, получают те, чьи данные были скомпрометированы. Следовательно, от утечки информации из госучреждений основной ущерб наносится гражданам России.

Уже известны данные за I полугодие 2013 года и полученные показатели свидетельствуют о том, что все чаще стали выявлять случаи раскрытия утечек информации. Это говорит о растущей самосознательности общества и интереса корпораций к проблеме утечки информации. Только 6 месяцев 2013 года было зафиксировано 496 случаев утечки информации — это на 18% больше, чем в первое полугодие 2012 года. Если такая динамика сохранится, то в этом году число утечек информации может достичь рекордного значения (1000 случаев). Россия уже успела обогнать Великобританию по количеству опубликованных утечек информации и теперь стоит на втором месте в этом списке. Доля утечек в госорганах и муниципальных учреждениях остается высокой (30% по всему миру). Процент утечек персональных данных также является лидирующим по сравнению с другими типами видов утечек информации - 93,8% .

Из всего вышеперечисленного можно сделать вывод, что утечка информации является актуальной проблемой на сегодняшний день и ее последствия носят не только материальные и моральные потери как для коммерческих организации, так и для госучреждений, но и общественно опасный характер. утечек из госорганов и муниципальных организаций продолжается. Причем утекают персональные данные граждан. Защита такой информации — прямая обязанность госорганов, однако справляются они с этой задачей плохо, причем по всему миру. Новый рост доли утечек персональных данных в общей картине утечек объясняется именно слабостью госорганов в деле защиты персональных данных. Однако, для решения данной проблемы применяются все возможные компьютерные программы, но исключить человеческий фактор просто не под силу современным технологиям. В связи с этим необходимо проводить профилактическую работу на местах, то есть разъяснять и подчеркивать для сотрудников предприятия важность конфиденциальности информации и ее сохранности внутри организации.

Литература

1. 1. Аналитический центр InfoWatch: «Глобальное исследование утечек корпоративной информации и конфиденциальных данных 2012» - <http://www.infowatch.ru/analytics>.
2. 2. Аналитический центр InfoWatch: «Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России 2012» - <http://www.infowatch.ru/analytics>.
3. 3. Аналитический центр InfoWatch: «Глобальное исследование утечек конфиденциальной информации в I полугодии 2013 года» - <http://www.infowatch.ru/analytics>.
4. 4. Аналитический центр Anti-Malware.ru - <http://www.anti-malware.ru/leaks>.
5. 5. Zecurion Analytics «Утечки конфеденциальной информации», 2012 год - http://www.zecurion.ru/upload/iblock/f8b/Zecurion_Data_leaks_2013.pdf