Автор:

Шкидина Анастасия Александровна

студентка

Научный руководитель:

Павлова Галина Юрьевна

канд. культурологии, доцент, преподаватель

НАН ЧОУ ВО «Академия маркетинга и

социально-информационных технологий – ИМСИТ»

г. Краснодар, Краснодарский край

СТАТИСТИКА УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ЕЁ ПРАВОВАЯ ЗАЩИТА

Аннотация*: в статье приведена статистика утечек конфиденциальной информации за 2016–2017 гг. в разных областях деятельности, обусловленных внутренними нарушениями и внешними вмешательствами. Для устранения противоречий в различных Законах, так или иначе затрагивающих тему защиты информации, предложено дополнить формулировку понятия конфиденциальной информации в тексте Федерального закона «Об информации, информатизации и защите информации», распространив её информацию вообще, то есть не только на документированную информацию, но и на сведения в недокументированной форме.*

Ключевые слова*: экономическая безопасность, информационная безопасность, целостность информации, конфиденциальная информация, общедоступная информация, информация ограниченного доступа, секретная информация.*

В современной рыночной экономике России, как и в экономике всего мира, успех предпринимателя в бизнесе не в последнюю очередь обеспечивается экономической безопасностью его деятельности. Составной частью экономической безопасности является информационная безопасность, которая достигается за счёт использования комплекса защитных мер от действий злоумышленников с целью сохранения целостности и конфиденциальности информации.

Проблема защиты информации от постороннего доступа и нежелательных воздействий на неё возникла давно, а именно с той поры, когда человек по каким-либо причинам не захотел делиться информацией, либо ограничил доступ к ней определённому кругу лиц. С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности, информация приобретает цену. Ценной становится та информация, обладание которой позволяет её существующему и потенциальному владельцу получить какую-либо выгоду.

Несмотря на высокую цену информации, многие владельцы конфиденциальной и иной ценной информации пренебрегают элементарными мерами безопасности, и это ещё раз подтверждает статистика утечек информации.

Например, за 2017 год количество утечек конфиденциальной информации в мире возросло в 8 раз по сравнению с предыдущим годом. Только за первое полугодие 2017 года произошло 925 инцидентов, связанных с потерей конфиденциальной информации, что на 10% больше, чем за тот же период 2016 года. Из-за внешнего вмешательства, например по вине хакеров, произошли 384 таких инцидента. Из-за внутренних нарушений (например, по вине сотрудников компаний, случайно или намеренно обнародовавших конфиденциальную информацию) – 520 утечек. Причины оставшихся 21 утечки выяснить не удалось.

Однако объем скомпрометированных данных в результате атак извне оказался значительнее (5,23 млрд записей), чем из-за внутренних нарушений (2,32 млрд). В то же время, по мнению InfoWatch, отчет охватывает не более 1% всех случаев утечки данных, так как основан на анализе публичной информации, а случаи компрометации конфиденциальных данных часто скрываются компаниями.

По количеству инцидентов, связанных с утечкой данных, за рассматриваемый период лидируют медучреждения (17,4%), госорганы (15,2%) и организации из торговой отрасли (12,2%). По количеству скомпрометированных записей – ИТ-компании (33,9%), торговые предприятия (20,2%) и госорганы (15,8%).

Например, на правительственном портале gov.spb.ru в январе были обнародованы паспортные данные, адреса и номера телефонов 1627 человек, включенных в реестр обманутых дольщиков Санкт-Петербурга. В первом полугодии 2017 года резко возросло количество случаев утечки платежной информации. На такие случаи пришлось 26,8% от общего количества, тогда как в первом полугодии 2016 года было 6,2%. Наиболее популярные сценарии утечки платежных данных – через облачные хранилища (45,3% инцидентов) и электронную почту (44,1%).

По итогам 2017 года убытки компаний от потери конфиденциальной информации могут превысить $50 млрд, сообщил РБК руководитель аналитического центра Zecurion Владимир Ульянов. Согласно исследованию Zecurion, лишь 7% компаний – представителей среднего и крупного бизнеса сталкиваются с утечками реже, чем один раз в год.

Необходимо учитывать, что на статические данные больше всего влияют крупные инциденты, например, такие, как атака на «Yahoo!», в результате которой были скомпрометированы данные нескольких миллиардов пользователей. При этом надо учитывать, что крупные утечки влияют не только на количественные показатели, но и на профиль угроз (преобладание того или иного их вида).

В законодательстве РФ информация подразделяется на общедоступную и информацию, доступ к которой ограничен (см. Федеральный закон №149-ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006).

В свою очередь информация ограниченного доступа делится на две группы, одной из которых является конфиденциальная информация (конфиденциальная информация – это информация, представляющая собой коммерческую, служебную, профессиональную или личную тайну, охраняющуюся ее владельцем). В законе определено, что конфиденциальность информации – это требование, обязательное для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия ее обладателя.

Для того чтобы отнести информацию к конфиденциальной, она должна соответсвовать критериям охраноспособности, а именно должен быть известен круг лиц, обладающих этой информацией; итогом разглашения информации должен наступать какой-либо ущерб; доступ к носителям данной информации должен быть ограничен, причём на законных основаниях.

Однако, в отличие от секретной информации, конфиденциальная информация может быть передана другим лицам, но только с разрешения и на условиях обладателя этой информации.

Виды конфиденциальной информации установлены Указом Президента Российской Федерации от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера».

Перечень сведений конфиденциального характера дополняют другие нормативно-правовые акты: основы законодательства РФ «Об охране здоровья граждан», законы РФ «О психиатрической помощи и гарантиях прав граждан при ее оказании», «О нотариате», «Об адвокатуре», «Об основных гарантиях избирательных прав граждан РФ», «О банках и банковской деятельности», а также Налоговый кодекс РФ, Семейный кодекс РФ и др.

По моему мнению, существует необходимость внесения изменений в Федеральный закон «Об информации, информатизации и защите информации», а именно сфера действия Закона была определена, по сути, как отношения в сфере документированной информации (ст. 1). Однако в самом Законе не удалось удержаться в рамках заявленной в начале его текста сферы действия. Грань между документированной информацией и информацией вообще в Законе оказалась размытой. Вопросы регулирования отношений по поводу информации затрагиваются так или иначе в пункте 2 статьи 4, пункте 2 статьи 8, пункте 4 статьи 10, статьях 11–13, 21 и др. В результате указанной нечёткости несмотря на то, что в Конституции РФ, её статьях 29, 41 и 42 речь идёт о свободе информации и достоверной информации об окружающей среде, в Законе эти права и свободы в ряде статей ограничены только предоставлением информации из информационных ресурсов, т.е. документированной информацией. В случае, например,

выброса вредных веществ в море, чиновники, руководствуясь Законом, могут попытаться не представлять общественности информацию, пока не будет документов – скажем, заключения экспертизы или результатов работы комиссии, которые могут быть подготовлены и подписаны через столько времени, сколько потребуется для соблюдения внутриведомственных интересов. Вместе с тем в статье 24 Закона говорится о возможности судебного обжалования отказа в доступе к информации, поэтому указание в предыдущих статьях на право доступа к информационному ресурсу (документированной информации), видимо, объясняется нечёткостью применения при разработке Закона терминов «информационный ресурс», «документированная информация» и «информация». Однако следует отметить, что негативные следствия применения данной нормы Закона частично устраняются ст. 237 Уголовного кодекса РФ, в которой установлена ответственность за сокрытие информации об обстоятельствах, создающих угрозу для жизни или здоровья людей, либо для окружающей среды. В отличие от Закона, УК, не ограничивает форму представления информации только документированной.

Определение конфиденциальной информации в Законе (ст. 2) как документированной также неоправданно сужает сферу защиты охраняемых законом сведений, которые могут выступать и в недокументированной форме (например, государственная, коммерческая, банковская тайны). Несмотря на частичную компенсацию указанных существенных недоработок Закона нормами других нормативно-правовых актов, все же для устранения противоречий непротиворечивости законодательства крайне желательно привести эти нормы в соответствие с конституционными положениями и общепризнанными международными нормами, установив право доступа и защиты информации независимо от формы её представления. Изложенное позволяет сделать вывод о необходимости повышения качества разработки проектов федеральных законов, регулирующих отношения по поводу информации и информационных технологий. Что в настоящее время становится все более важным в связи с ростом утечек информации и

ущерба, наносимого ими, о чем свидетельствует статистика, приведенная в начале статьи.

Список литературы

1. Конституция Российской Федерации: Официальный текст с поправками. Историко-правовой комментарий / Авт. коммент. Б.А. Страшун. – 3-е изд., перераб. – М.: Норма: НИЦ Инфра-М, 2013.

2. Уголовный кодекс Российской Федерации. – М.: Инфра-М, 2013.

3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: Инфра-М, 2012.

4. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – 2-е изд., доп. – М.: Форум: НИЦ Инфра-М, 2015.

5. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – М.: Форум: НИЦ Инфра-М, 2014.