ДОЛМАТОВ Е.А., ДОЛМАТОВ Д.А.

ПРОБЛЕМЫ ПРАВОВОЙ И ТЕХНОЛОГИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Актуальность проблемы правового регулирования защиты персональных данных определяется многими факторами, в частности достаточно быстрым развитием электронного документооборота, автоматизированных систем обработки информации, баз данных, различных сетевых сервисов и платежных систем.

Организационные моменты, связанные с безопасностью персональных данных, контролирует Роскомнадзор, а технические – Федеральная служба технического и экспертного контроля (ФСТЭК) – федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области технической защиты и безопасности информации.

Основная цель предпринимаемых мер по обеспечению безопасности персональных данных – пресечение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении данного вида информации[1].

Обеспечение безопасности персональных данных сотрудников в любом учреждении, организации является не её правом, а прямой обязанностью. Несоблюдение требований ведет к нарушению конституционных прав граждан, может повлечь за собой череду гражданско-правовых исков со стороны физических лиц, чьи права могут оказаться нарушенными, и даже привлечение к административной или уголовной ответственности, а также может повлечь и ущерб для самой организации.

В каждом отдельном случае перечень мероприятий и документов может варьироваться в зависимости от специфики обработки персональных данных, организационной структуры и других особенностей конкретного предприятия.

Организационные меры защиты информации осуществляются в зависимости от категории персональных данных – чем выше категория, тем выше соответствующие требования защиты[2].

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) от 27.07.2006 № 152-ФЗ (действующая редакция от 21.07.2014) // Консультант плюс: http://www.consultant.ru/popular/o-personalnyh-dannyh/ (дата обращения: 16.01.2014).

[2] Шнайдер, С. Новое в законодательстве о персональных данных / С. Шнайдер // Кадровик.ру. – 2012. – № 1. – С. 12.

Репозиторий БГУ

Технические меры является обязательным условием и предполагают использование программно-аппаратных средств защиты информации, а их количество и степень защиты определяется исходя из класса системы персональных данных.

В отличие от организационных мер техническая защита информации является сложным и трудоемким делом, при выполнении которого требуется соблюдать определенные условия, например, наличие соответствующих лицензий, обследование информационных систем в соответствии с методическими рекомендациями ФСТЭК и т.д.

Технические средства защиты персональных данных подразделяют на несколько групп:

- системы защиты от несанкционированного доступа;
- антивирусные программы;
- межсетевые экраны;
- криптографические средства.

Важно, чтобы все применяемые технические средства были сертифицированы, данные об этом можно получить в Реестре сертифицированных средств защиты информации на сайте ФСТЭК России.

Сертификация по требованиям безопасности информации представляет собой деятельность по подтверждению характеристик продукта, услуги или системы требованиям стандартов или иных нормативных документов по защите информации. В нашей стране действуют четыре федеральных органа по сертификации, однако в области защиты персональных данных сферы ответственности поделены между Федеральной службой безопасности (ФСБ) и ФСТЭК. Традиционно сфера компетенции ФСБ лежит в области криптографической защиты, а сфера ФСТЭК – в области некриптографической защиты информации от несанкционированного доступа, а также от утечек по техническим каналам связи.

Обязательной сертификации подлежат системы, продукты и услуги.

Система – это объект информатизации, где обрабатывается реальная информация. По этой причине к системам предъявляются дополнительные требования, касающиеся, в том числе, организационных мер и физической защиты.

Информационные системы защиты персональных данных поделены на 4 класса по степени возможных последствий для субъектов вследствие возникновения инцидентов в этих системах (табл. 1)[1]:

К1 (значительные последствия).

К2 (последствия).

К3 (незначительные последствия).

[1] Сертификация средств защиты персональных данных: революция или эволюция? // Защита информации. – INSIDE – 2008. – № 5– С. 32.

Репозиторий ВГУ

К4 (не приводят к последствиям).

Таблица 1

Классификация информационных систем персональных данных (ПД)

Число субъектов персональных данных (объединение)	Менее 1000	1000 – 100000	Более 100000
Категория ПД	Класс системы персональных данных		
4 – Обезличенные ПД	К 4	К 4	К 4
3 – ФИО, адрес, день рождения	К 3	К 3	К 2
2 – дополнительные данные: образование, должность, финансы	К 3	К 2	К 1
1 – особенности здоровья, политические взгляды, интимная жизнь и т.п.	К 1	К 1	К 1

В нормативных документах ФСТЭК России декларирована обязательность сертификации средств защиты как государственного, так и негосударственного информационного ресурса в тех случаях, когда речь идет об информации содержащей государственную тайну и конфиденциальной информации, размещенной на государственных ресурсах.

Документы, подтверждающие реализацию предпринятых мер:

- перечень средств защиты персональных данных;
- журнал учета и хранения носителей персональных данных;
- акт установки средств защиты информации;
- утвержденная форма акта списания и уничтожения электронных носителей информации;
- утвержденная форма акта уничтожения документов;
- подписанные соглашения о неразглашении персональных данных с третьими лицами (организациями) или соответствующие оговорки в контрактах и соглашениях (в особенности при трансграничной передаче данных).

В каждой организации решения по обеспечению безопасности опираются прежде всего на средства анализа и интеллектуальные технологии обнаружения угроз в реальном времени.

Ключевой элемент защиты информации – наглядное представление о текущем состоянии среды и угрозах, создание стратегии обеспечения устойчивости к киберугрозам, основанной на оперативной информации о безопасности, для защиты организации от направленных атак и сложных устойчивых угроз.

Важный шаг – повышение информированности сотрудников по вопросам безопасности на основе комплексной стратегии, охватывающей персонал, процессы и технологии. Ознакомление сотрудников с новейшими политиками и процедурами обеспечения безопасности, методиками атак и инструментами, с целью обеспечения надежной защиты всей информации, где бы она ни находилась.

Репозиторий ВГУ

Современные интеллектуальные решения в области безопасности предоставляют следующие возможности:

Защита бренда и дохода за счет быстрого обнаружения атак и противодействия им. Благодаря наглядному представлению и оперативной информации можно быстрее и увереннее принимать решения.

Готовность к отражению атак злоумышленников существует благодаря интеллектуальным решениям для обеспечения безопасности, основанным на анализе больших объемов данных. В данном случае, информация – ключевой элемент защиты информации. Анализируются первоначальные предупреждения, оперативная информация о внешних угрозах и характеристики сетевого трафика на наличие вредоносного кода, сопоставляются и обнаруживаются тенденции, что способствует повышению устойчивости и готовности организации к угрозам.

Международная служба, объединяющая специалистов по обеспечению безопасности, аналитиков и исследователей, занимающихся разработкой материалов в области последних угроз для организаций и конечных пользователей – Symantec Security Response – в ежегодном отчете об угрозах безопасности в Интернете (ISTR) дает общее описание и анализ угроз, с которыми приходилось сталкиваться в 2013 году в разных странах.

Отчет основывается на данных из сети Symantec Global Intelligence Network, которые помогают аналитикам Symantec идентифицировать, анализировать и обоснованно комментировать новые тенденции угроз.

Названы основные факты в отчете об угрозах безопасности в Интернете в 2013 г.:

- число направленных атак, которое возросло на 91%;
- число обнаруженных брешей в системах безопасности возросло на 62%;
- обнаружено 23 уязвимости «нулевого дня»;
- через уязвимости в 2013 году были похищены данные 552 миллионов учетных записей;
- за последние 12 месяцев 2013 года 38% пользователей мобильных устройств сталкивались с киберпреступностью в мобильной среде;
- количество Интернет-атак возросло на 23%;
- из каждых 392 сообщений электронной почты одно отправлено с целью фишинга;
- на каждом восьмом зарегистрированном Интернет-сайте имеются критические уязвимости[1].

[1] Отчет об угрозах безопасности в Интернете за 2014 год, том 19 // Публикации службы Security Response: http://www.symantec.com/ru/ru/security_response/publications/threatreport.jsp (дата обращения: 16.01.2014).

Репозиторий БГУ

Российское законодательство о защите персональных данных является относительно новым, и существует множество нерешенных вопросов, что зачастую препятствует выполнению работодателем необходимых требований действующего законодательства о персональных данных.

Складывающаяся практика применения федерального закона «О персональных данных» и существующих нормативных документов данной сфере выявила несколько групп проблем, требующих оперативного решения.

Проблемы правового характера возникли в связи с неоднозначными положениями закона, которые по-разному трактуются государственными регуляторами и операторами, требуют конкретизации, уточнений и разъяснений.

Не менее важной проблемой является достаточно быстрое развитие технологической основы обработки персональных данных, электронного документооборота, автоматизированных систем обработки, информационных баз и сетевых технологий. Существующая законодательная база не всегда адекватно, оперативно и своевременно отражает происходящие изменения.

Конфликт этот развивается, но активные поиски оптимальных решений в рамках существующей законодательной базы продолжаются. Наиболее перспективными направлениями в данной сфере законотворчества, с одной стороны, попытки экстраполяции существующих тенденций и направлений развития технологических систем и реализация опережающего развития законодательной базы в рамочной форме, с другой – закрепление существующих наиболее успешных практик в законодательных актах.

Представляет интерес направление дальнейшего исследования возможностей внедрения интеллектуальных информационных систем анализа взаимосвязей и взаимозависимости нормативных актов в данной области.

Репозиторий БГУ